SECRET SOURCES

Whistleblowers, National Security, and Free Expression

PEN AMERICA free expression. literature.

SECRET SOURCES: WHISTLEBLOWERS, NATIONAL SECURITY, AND FREE EXPRESSION

November 10, 2015

PEN American Center is the largest branch of PEN International, the world's leading literary and human rights organization. PEN works in more than 100 countries to protect free expression and to defend writers and journalists who are imprisoned, threatened, persecuted, or attacked in the course of their profession. PEN America's 4,200 members stand together with more than 20,000 PEN writers worldwide in international literary fellowship to carry on the achievements of such past members as James Baldwin, Robert Frost, Allen Ginsberg, Langston Hughes, Arthur Miller, Eugene O'Neill, Susan Sontag, and John Steinbeck. For more information, please visit www.pen.org.

Cover (clockwise): Photograph of Pentagon by David B. Gleason. Photograph of the Central Intelligence Agency New Headquarters Building by the CIA. Photograph of the National Security Agency building by the NSA.

PEN AMERICA free expression. literature.

CONTENTS

INTRODUCTION

Edward Snowden's disclosures regarding mass surveillance programs set in motion a national and international debate over the limits of government power, the measures necessary to protect national security, and what information the public has a right to know about its government's activities. Many changes have resulted, including a federal appellate court ruling in May 2015 that the National Security Agency's (NSA) bulk collection of communications records was illegal, the passage of the USA Freedom Act to introduce crucial reforms to the NSA's bulk collection program, and the adoption of a resolution by the UN General Assembly declaring online privacy to be a fundamental human right.[1]

Within days of the first story's publication in *The Guardian* in June 2013, the government filed criminal charges against Snowden under seal, later leaked, including theft of government property and violating the Espionage Act through unauthorized disclosure of national defense information and willful communication of classified intelligence activities to people who were unauthorized to receive that information.[2]

Since then, government officials from both parties have repeatedly criticized Snowden for failing to raise his concerns through internal channels, implying that by doing so he forfeited any claim to "whistleblower" protection, and called upon him to return home from Russia to make his case in court. In August 2013, President Barack Obama said that if Snowden "believes that what he did was right, then, like every American citizen, he can come here, appear before the court with a lawyer and make his case."[3] In a recent Democratic Presidential debate, former Secretary Hillary Clinton said that Snowden broke the law when he "could have gotten all the protections of being a whistleblower."[4] Secretary of State John F. Kerry has called for Snowden to "man up" and return to "make his case" in the United States.[5] Many Republicans have echoed these statements. The former chairman of the House Intelligence Committee, Representative Mike Rogers (R-Mich) said of Snowden, "All he had to do was raise his hand... under the whistle-blower law, he is protected. Yet he chose to go to China."[6]

However, these characterizations are inaccurate, as PEN American Center's report will demonstrate. As a government contractor, Snowden had few, if any, protections under whistleblower provisions compared to intelligence employees who are hired directly by the U.S. government. In January 2013, shortly before he made his disclosures, Congress significantly weakened existing whistleblower protections for national security contractors by passing a law that removed most of their pre-existing rights. President Obama did issue a directive in 2012 that provided intelligence community contractors who pursue internal channels to raise concerns about misconduct with protection from security clearance retaliation, but the directive didn't go into effect until after Snowden's disclosures and would not have protected him from other forms of retaliation.[7] These confusing procedural developments aside, Snowden's case underscores a far more fundamental issue for intelligence community workers: trying to blow the whistle through internal channels is nearly impossible when it concerns an institutionally accepted program that has been judged lawful by political leaders or Congress.

Under the existing legal framework, intelligence community employees are only considered a "whistleblower" entitled to protection from retaliation if they disclose "a violation of any Federal law, rule, or regulation; or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety," through specific internal channels, such as to an Inspector General's office or a congressional intelligence committee.[8] They are not protected for disclosures made to the public, nor are they are protected when they question judgments of legality or propriety concerning public policy matters through internal channels.[9] It is therefore difficult for an intelligence community whistleblower to draw attention to a controversial program or policy that has been approved by an agency and/or Congress, even if the legality, constitutionality or wisdom of that policy is questionable, and/or the policy touches on a matter of significant public concern. For the purposes of this report, and because not all cases described within meet all definitions of "whistleblower," PEN uses the general term "national security leakers."

PEN's research demonstrates that the gaps in existing protections for intelligence community whistleblowers, coupled with the government's failure to adequately address retaliation against them and the Obama administration's aggressive prosecution of leakers under the Espionage Act, are damaging to freedom of expression, press freedom, and access to

information in the United States. The combined impact of these elements has created a chilling effect on free expression, and affects both the willingness of government workers to publicly expose wrongdoing and the ability of journalists to cover their revelations. This poses risks for the free flow of information and informed public debate that is necessary for a healthy democratic society.

As a candidate in the 2008 election, Barack Obama voiced support for whistleblowers, and pledged to protect them. His pledge seemed like more than political rhetoric, as he had an actual record of assisting whistleblowers: when he was a practicing lawyer he had represented a whistleblower and won the case.[10] During the campaign, Obama acknowledged that "Often the best source of information about waste, fraud and abuse in government is an existing government employee committed to public integrity and willing to speak out," and said "such acts of courage and patriotism, which can sometimes save lives and often save taxpayer dollars, should be encouraged rather than stifled." He vowed to strengthen whistleblower laws if elected and to ensure that whistleblowers would "have full access to courts and due process."[11] At the start of his first term, he also pledged to make his administration "the most open and transparent" in history.[12]

Seven years into President Obama's term, his administration's record on whistleblower protection is decidedly mixed. Whistleblower protections have been significantly strengthened for many federal government employees and contractors. In 2012 Congress passed the Whistleblower Protection Enhancement Act, which strengthened protections for most federal employees. However, the law specifically exempts workers of agencies or units that conduct foreign intelligence or counterintelligence activities, including the Federal Bureau of Investigation, Central Intelligence Agency, National Security Agency, Defense Intelligence Agency, National Geospatial-Intelligence Agency, Office of the Director of National Intelligence, and National Reconnaissance Office.[13] These intelligence community employees are protected by separate, weaker laws and policies, including the Intelligence Community Whistleblower Protection Act of 1998. While the administration has also strengthened protections in some areas for intelligence community employees with the issuance of Presidential Policy Directive 19 in 2012 and the 2014 Intelligence Authorization Act, their rights remain significantly weaker than those provided to other government employees. Furthermore, in important respects, the protections for intelligence contractors (like Snowden) were actually weakened by Congress during Obama's tenure.

All the while, the administration has ramped up criminal prosecutions of government employees responsible for national security leaks. This presidency has prosecuted more than twice as many leakers under the Espionage Act as all previous administrations combined.[14] As former *Washington Post* Executive Editor Leonard Downie wrote, "The administration's war on leaks and other efforts to control information are the most aggressive I've seen since the Nixon administration, when I was one of the editors involved in *The Washington Post*'s investigation of Watergate." Downie added that the administration has repeatedly made a "disturbing distinction" that "exposing 'waste, fraud and abuse' is considered to be whistleblowing. But exposing questionable government policies and actions, even if they could be illegal or unconstitutional, is often considered to be leaking that must be stopped and punished. This greatly reduces the potential for the press to help hold the government accountable to citizens."[15]

Government employees and contractors have repeatedly risked their careers and freedom to inform the public about important national security-related issues that were being concealed from the American people, and have often done so by talking to the press. In 1971 Daniel Ellsberg, a military analyst with the RAND Corporation, released a classified Department of Defense analysis of the Vietnam War to the *New York Times* and the *Washington Post.* These "Pentagon Papers," showed attempts by several presidents to deceive the American public about the progress of the Vietnam War, including the poor prospects for a successful outcome. Ellsberg was subsequently charged under the Espionage Act. The judge declared a mistrial and dropped the charges against Ellsberg after it was revealed that President Nixon authorized a "plumbers" unit to burglarize the office of Ellsberg's psychoanalyst—an early example of the varied forms of retaliation experienced by many national security leakers.[16]

In the following decades, leaks continued to play a significant role in Washington. A mid-1980s Harvard University survey of current and former senior government officials found that 42% of those who responded had, on at least on one occasion, felt "it appropriate to leak information to the press."[17] The researchers concluded that leaks "are a routine and generally accepted part of the policymaking process." Likewise, a review by the Senate Select Committee on Intelligence of eight major U.S. newspapers found 147 instances of classified information leaks over a six-month period in 1986.[18]

Confidential government sources have always served as a vital resource for journalists reporting on national security, and brought to light many major stories. These sources have been of particular importance in the post-9/11 era, as underscored by *Washington Post* journalist Dana Priest:

> The subjects that I have been able to cover, based on information provided by confidential sources, include the existence and conditions of hundreds of prisoners, some later to be found innocent, held at the military prison at Guantánamo Bay, Cuba…the wasteful spending of tens of billions of dollars in taxpayer funds on an outdated and redundant satellite system; the legal opinions supporting the 'enhanced interrogation techniques' of prisoners captured in the war on terror; the specifics of those techniques, including waterboarding; the rendition of multiple suspected terrorists by the CIA in cooperation with foreign intelligence services to third countries …the abuse of prisoners at the Abu Ghraib prison in Iraq …and the existence and evolution of the CIA's secret prisons in the countries of Eastern Europe…All of the revelations in my stories on these subjects were at one point secret from the American public. None of them could have been reported without the help of confidential sources.[19]

The leak cases discussed in this report include numerous examples of intelligence community employees who made a difficult decision resulting in grave personal consequences to expose certain government actions that they felt the American public had a right to know. In parallel, the legislative and executive actions documented here demonstrate the continuing failure to implement strong, meaningful protections for intelligence community whistleblowers. The report begins with a brief overview of relevant U.S. and international legal provisions on free expression, the right to information, and press freedom, outlining the obligations of U.S. public officials. The report then analyzes current protections afforded to intelligence community employees and contractors, including their strengths and weaknesses, and the impact that the Obama administration's use of Espionage Act prosecutions to crack down on leaks to the media has had on free expression. Finally, the report presents PEN's key recommendations to the executive and legislative branches to protect whistleblowing as an important component of government accountability and transparency, and to ensure that journalists are able to report in the public interest and protect their sources without fear of repercussion.

METHODOLOGY

This report is based on interviews with experts on national security, whistleblowing, and free expression, including civil society representatives, lawyers, whistleblowers and leakers, scholars, Congressional staffers, Inspector General representatives, other government representatives and journalists. Some interviewees chose to speak to PEN on background. PEN also requested interviews with Congressman Adam Schiff's office, the Department of Justice (national security and criminal divisions), and the offices of several Inspectors General (including the CIA, DOD and NSA IGs), which either did not respond to the request or declined to be interviewed. This report also includes an extensive review of secondary sources, including books, law review articles, civil society reports, parliamentary and congressional reports, and news articles.

U.S. AND INTERNATIONAL LEGAL PROVISIONS ON FREEDOM OF EXPRESSION AND ACCESS TO INFORMATION

Freedom of expression is protected both by the U.S. Constitution and under international law. The First Amendment provides:

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.[20]

Under international law, the right to freedom of expression is protected by Article 19 of the International Covenant on Civil and Political Rights (ICCPR), to which the United States is a state party:

> Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.[21]

Freedom of Information

Freedom of information refers to the idea that the public has a right to access government and court records. The right is sometimes also referred to as the "public's right to know" about their government's activities. In U.S. law, while there is no general constitutional or statutory right of access to, or disclosure of government information, there are specific constitutional and statutory provisions for public access to such materials.

Statutorily, the right is most prominently reflected in the 1966 Freedom of Information Act (FOIA).[22] At its signing into law on July 4, 1966, President Lyndon B. Johnson said "this legislation springs from one of our most essential principles: a democracy that works best when the people have all the information that the security of the nation permits. No one should be able to pull curtains of secrecy around decisions which can be revealed without injury to the public interest."[23] FOIA establishes that all government reports are accessible to the public unless they fall into an exempted category. There are nine categories of exemptions, with the first and most broadly applied exception being classified information.

The Supreme Court has also recognized a First Amendment right to government information in certain situations. The 1980 case of *Richmond Newspapers Inc. v. Virginia*, in which a plurality ruled that the public had a right of access to information in the course of criminal trials, has been generally understood to articulate a fairly broad First Amendment right of public access to government proceedings.[24] In a concurrence by Justice Stevens, he wrote that "the Court unequivocally holds that an arbitrary interference with access to important information is an abridgment of the freedoms of speech and of the press protected by the First Amendment."[25]

While the scope of these rights is not unlimited, they represent the importance of access to information to promoting government transparency and protecting democratic values. As Judge Damon Keith of the Sixth Circuit wrote in *Detroit Free Press v. Ashcroft*, "democracies die behind closed doors."[26]

Freedom of Information under International Law

Article 19 of the International Covenant on Civil and Political Rights (ICCPR) explicitly protects the right of access to information as a component of freedom of expression.[27] The United Nations Human Rights Committee, the body that provides authoritative interpretations of the ICCPR's provisions, has stated that the right of access to information "includes the expression and receipt of communications of every form of idea and opinion capable of transmission to others," subject to certain limitations described below.[28] It has also affirmed that the right to information "includes records held by a public body, regardless of the form in which the information is stored, its source and the date of production."[29] The U.N. General Assembly declared freedom of information to be a fundamental human right during its first session in 1946.[30] Other international and regional human rights mechanisms have also recognized, to varying degrees, the right of access to information.[31]

David Kaye, the UN Special Rapporteur for the promotion and protection of the right to freedom of opinion and expression, presented a report to the General Assembly in September 2015 that powerfully articulates the important role played by whistleblowers and confidential sources in upholding freedom of expression and the public's right to receive information of public interest. The report reiterates states' obligations under international law to ensure strong legal protections for whistleblowers and for journalists' ability to protect source confidentiality. It notes that "the right to information also requires a bedrock of social and organizational norms that promote the reporting of

wrongdoing or other information in the public interest."[32] The United Nations Convention against Corruption, to which the United States is a state party, also recognizes the importance of access to information in promoting government transparency, and calls upon states party to provide whistleblower protections for "any person who reports in good faith and on reasonable grounds to the competent authorities any facts concerning offenses established in accordance with this Convention."[33]

Additionally, there are several internationally persuasive sources that further contextualize the right of freedom of information in the context of whistleblowing. For example, the Tshwane Principles on National Security and the Right to Information (Tshwane Principles) were developed by the Open Society Justice Initiative in consultation with 22 civil society organizations and more than 500 global experts, based on international and national legal practices. The Tshwane Principles call for states to provide defenses for whistleblowers, enforcement of due process mechanisms, judicial recourse, and protection for a wide range of government-affiliated employees. The Tshwane Principles also state that any leaker or whistleblower who discloses information in the public interest should be protected from retaliation, provided they acted in good faith and followed any available and applicable procedures. [34]

Freedom of the Press

Freedom of the press is protected under the First Amendment and the ICCPR. The Supreme Court has defined "press" in the context of the First Amendment as "every sort of publication which affords a vehicle of information and opinion."[35] The ICCPR uses a similarly broad definition; the Human Rights Committee has recognized that journalism may be engaged in not only by professional full-time reporters, but also "bloggers and others who engage in forms of self-publication in print, on the internet or elsewhere." [36]

Although the Supreme Court has declined to give independent context to the Press Clause, it has nevertheless repeatedly underscored the special role played by the media in protecting freedom of speech and promoting government accountability.[37] In the 1971 "Pentagon Papers" case, the Nixon administration sought to halt the *New York Times*' publication of the documents leaked by Daniel Ellsberg and another defense analyst, and the request for an injunction reached the Supreme Court in a fast-tracked and highly publicized case.[38] In a 6-3 decision, the Supreme Court held that the *New York Times* and other media outlets were free to print the leaked information about the Pentagon Papers. Justice Potter Stewart's concurrence noted:

> The only effective restraint upon executive policy and power in the areas of national defense and international affairs may lie in an enlightened citizenry… For this reason, it is perhaps here that a press that is alert, aware, and free most vitally serves the basic purpose of the First Amendment.[39]

"The only effective restraint upon executive policy and power in the areas of national defense and international affairs may lie in an enlightened citizenry."

The media's right to engage in the process of newsgathering is also protected under the U.S. Constitution and international law. On the heels of the *Pentagon Papers* case, the Supreme Court most famously protected newsgathering in *Branzburg v. Hayes*, a 1972 decision in which Justice Byron White wrote for the majority, "We do not question the significance of free speech, press, or assembly to the country's welfare. Nor is it suggested that news gathering does not qualify for First Amendment protection; without some protection for seeking out the news, freedom of the press could be eviscerated."[40]

Justice Stewart underscored this principle, and the relationship between access to information and press freedom, in his concurrence:

> News must not be unnecessarily cut off at its source, for without freedom to acquire information the right to publish would be impermissibly compromised. Accordingly, a right to gather news, of some dimension, must exist.[41]

Permissible Limitations on Freedom of Expression Under International Law

Under international law, the right to freedom of expression may be restricted in certain specific circumstances.[42] Protection of national security is a legitimate grounds for restriction of free expression, but any limitation imposed must satisfy particular conditions, as the Human Rights Committee has explained:

> It is for the State party to demonstrate the legal basis for any restrictions imposed on freedom of expression . . . When a State party invokes a legitimate ground for restriction of freedom of expression, it must demonstrate in specific and individualized fashion the precise nature of the threat, and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat."[43]

CURRENT LAW AND POLICY RELATING TO THE REPORTING AND DISCLOSURE OF GOVERNMENT PRACTICES

The Obama administration has a complex and inconsistent relationship with national security whistleblowing. On the one hand, the President has taken several significant steps to reform and strengthen protections for intelligence community whistleblowers who make internal disclosures, most significantly by issuing Presidential Policy Directive 19, discussed in this section, and has appointed strong whistleblower advocates to some offices that assist whistleblowers. He has also supported stronger whistleblower protections for non-intelligence community employees, as demonstrated by his unwavering support for the 2012 Whistleblower Protection Enhancement Act (WPEA).[44] On the other hand, the administration has aggressively prosecuted leakers who publicly disclose national security information even on matters of unquestioned public concern while failing to hold accountable those who engaged in the misconduct being disclosed (e.g. those who authorized or participated in torture). This section will analyze the strengths and weaknesses of the laws and policies set up to protect intelligence community whistleblowers, followed by an examination of the laws that the administration has used to prosecute leakers. The report then presents a series of recommendations that highlight reforms necessary to protect whistleblowers, disclosures in the public interest, and press freedom.

Protections Afforded to Intelligence Community Employees and Contractors: An Overview

Contrary to Secretary Clinton's understanding of the protections available to Edward Snowden, intelligence community employees who report wrongdoing through internal channels are afforded very few protections against retaliation. Intelligence community *contractors*, who are employed by a private firm contracted by the government, are even more vulnerable.[45]

Under Executive Order 12,674, which was signed by President George H.W. Bush in 1989, all federal employees are required to report "waste, fraud, abuse, and corruption to the appropriate authorities."[46] This requirement reflects the fact that employees who carry out the government's duties on a day to day basis and observe the internal workings of government in a way those outside cannot, are essentially 'first responders' when it comes to misconduct or wrongdoing: They are generally the first to detect such issues, and are thus in the best position to respond early to raise the alarm and set in motion procedures to rectify the problem.

Yet for many years intelligence community employees were provided little protection from retaliation for reporting misconduct. And retaliation against non-intelligence whistleblowers has apparently increased throughout the federal government, suggesting the protections granted to them have also fallen short. A 2011 report by the U.S. Merit Systems Protection Board based on a survey of federal employees found that perceived reprisals for reporting wrongdoing had significantly increased from 1992 to 2010.[47]

Congress and the executive branch have enacted protections for government whistleblowers in a piecemeal, inconsistent manner. There are at least 16 laws establishing various protections for federal employees and contractors seeking to blow the whistle, though some of these do not apply to intelligence community or other national security employees.[48] The whistleblower laws and executive orders that specifically apply to intelligence community employees, including the Intelligence Community Whistleblower Protection Act of 1998, Presidential Policy Directive 19 and the 2014 Intelligence Authorization Act, are analyzed in detail in this section. These laws and executive orders have numerous weaknesses in common, a summary of which is presented here prior to an examination of each specific law/executive order. It should also be noted that, while a full examination of the laws and policies applicable to military whistleblowers is beyond the scope of this report, there are comparable problems with the protections available to them.[49]

1. The failure to protect whistleblowers from criminal prosecution: None of the laws or executive orders applicable to intelligence community workers seeking to blow the

whistle protects them from retaliatory criminal investigations or prosecution. As the Brennan Center's Elizabeth Goitein commented, "It's bizarre to me that the legal protections out there for whistleblowers who disclose classified information, such as they are, relate only to administrative consequences and not to criminal prosecution, which is obviously the most draconian of government responses. I don't think it's fair to say we want to protect and encourage these kinds of disclosures and therefore we will prohibit some forms of retaliatory actions but not others."[50] Tom Devine, legal director of the Government Accountability Project (GAP) said, "If it's not lawful to fire someone for blowing the whistle, it shouldn't be lawful to put them in jail," further noting that "most nations apply their whistleblower rights in the civil or criminal context," but the U.S. doesn't.[51]

International standards also promote protection from criminal prosecution for certain disclosures. Specifically, the Tshwane Principles state that a person who blows the whistle through the proper channels or who makes a public disclosure of wrongdoing that meets certain standards should not be subject to "criminal proceedings, including but not limited to prosecution for the disclosure of classified or otherwise confidential information."[52]

2. Lack of access to court to challenge alleged retaliation: When Barack Obama was campaigning for president, he promised to ensure that whistleblowers would have "full access to courts and due process."[53] President Obama has fulfilled that promise only provisionally, and only for non-intelligence community employees. The WPEA temporarily provides non-intelligence employees with access to appellate review of retaliation complaints in all circuit courts of appeals while the government conducts a study evaluating the feasibility of full access to courts. Non-intelligence contractors also have temporary access to court through the National Defense Authorization Act for Fiscal Year 2013, which gives them the right to U.S. district court jury trials for civil complaints as part of a four-year pilot program.[54]

In contrast, the current system for enforcing intelligence community whistleblowers' rights against reprisal is entirely internal to the intelligence agencies, though the Congressional Intelligence Committees can intervene to help ensure that the whistleblower is protected. The system has been formalized in recent years and an appeals mechanism has been added, but without access to courts to appeal internal decisions, whistleblowers raising questions about the overarching legality or constitutionality of policies or programs operated under secret law, like the NSA's mass surveillance programs, are unlikely to prevail. As Jesselyn Radack, whistleblower attorney and head of the Whistleblower and Source Protection Program at ExposeFacts, said, "Whistleblowers need recourse outside of the agency and they also need access to jury trials. They need an enforcement mechanism that is not dependent on the agency that is engaged in the wrongdoing and covering-up and retaliating against them."[55]

> ***"If it's not lawful to fire someone for blowing the whistle, it shouldn't be lawful to put them in jail."***

3. Shortcomings in the Inspector General Offices charged with enforcement of whistleblower protections: Each government agency's Inspector General (IG) is authorized to receive and investigate retaliation complaints lodged by would-be whistleblowers, as well as disclosures related to wrongdoing. If the IG finds the claim to be valid, s/he may recommend that the agency take action to address the retaliation.

These IG offices, as currently constituted, have several shortcomings. The recommendations made by an IG are not binding, so agencies can choose not to address the retaliation. IG offices may also lack neutrality and independence, as the IG is often nominated by the President and beholden to his or her respective agency head for budgetary decisions and staff performance reviews.[56] This was a particular problem at the NSA. Until 2014, the NSA Inspector General was appointed directly by the director of the NSA.[57] Finally, on several past occasions IG offices have themselves engaged in allegedly retaliatory conduct towards whistleblowers.

IG offices' lack of power is further demonstrated by the fact that agencies sometimes ignore their requests for documents or information. This is especially a problem at the Department of Justice (DOJ), where the FBI has repeatedly refused the DOJ IG's request for some records in whistleblower cases.[58] IGs also have limited ability to contest legal interpretations adopted by the agency (or by other government entities, such as the Justice Department's Office of Legal Counsel). As Professor at American University Washington College of Law and national security law expert Stephen Vladeck described it, "The problem is that the inspectors general of these agencies are not the chief lawyers of the agencies. So when you have programs that the chief lawyers of the agencies have approved, there's no structure pursuant to which the inspector general can disagree."[59]

As a result, IG offices are unlikely to be an effective venue for whistleblowers whose concerns relate to the broader constitutionality of a program or policy that is nominally operated pursuant to law, like the NSA's mass surveillance programs. NSA IG George Ellard stated publicly that if Snowden had come to him with his concerns about surveillance he would have told him that the NSA acted within the law and explained to Snowden his "misconceptions."[60] This is notwithstanding the fact that Congress took action to address some of Snowden's

concerns through passage of the USA Freedom Act reforming aspects of mass surveillance.[61]

IG offices are further weakened when the Inspector General post remains vacant for long periods. Vacant posts are temporarily filled by acting directors who have less actual and apparent authority than IGs who have been nominated and approved by Congress. According to Senator Ron Johnson, acting directors "are not truly independent, as they can be removed by the agency at any time; they are only temporary and do not drive office policy; and they are at greater risk of compromising their work to appease the agency or the president."[62]

The Obama administration has been particularly slow to fill Inspector General vacancies. According to the Project on Government Oversight, the Obama administration has taken, on average, twice the length of time to fill IG vacancies as President George W. Bush did, and significantly more time than other recent administrations. The State Department IG position, for example, remained vacant for all of Hillary Clinton's four-year tenure as Secretary. As of June 2015, there were seven Inspector General vacancies in federal agencies, including at the CIA.[63]

In some cases, IG offices have been accused of destroying records, violating confidentiality, and failing to conduct adequate investigations.[64] Thomas Drake, a former senior NSA executive who blew the whistle on the failures of several major NSA programs, asserts that during the pre-trial criminal proceedings for his case "it came out that apparently the Department of Defense Inspector General [DoD IG] destroyed most, if not all, of the documentation I had given them…That's destruction of evidence in a criminal investigation at a criminal trial."[65] The DoD IG also allegedly revealed Drake's name to the FBI, while at the same time promising him confidentiality.[66] Also, when Drake submitted a retaliation complaint to the DoD IG, the IG rejected it after reviewing only five months of the alleged ten-year retaliatory period.[67] Notably, some of what is now known of the DoD IG's handling of Drake's case was uncovered by *McClatchy News* through a Freedom of Information Act request and from sources within the Department of Defense who requested anonymity because they feared retaliation.[68] As Drake's attorney, Jesselyn Radack, said, "Given that the DoD IG could not bother to investigate the crux of the reprisal allegations from one of its own witnesses, it is understandable that whistleblowers are disinclined to bring significant disclosures to the DoD IG."[69]

IG offices have, on multiple occasions, launched allegedly retaliatory investigations against whistleblowers.[70] Radack said that several of her clients have been retaliated against by an IG's office, including four of the NSA whistleblowers whom she represents. Radack said she also experienced retaliation by an IG's office when she raised concerns about alleged ethics violations committed by the FBI during the interrogation of "American Taliban" John Walker Lindh, while she was working as a DOJ ethics adviser. In 2003, the Justice Department IG placed her under criminal investigation without telling her why, referred her to the state bars in which she was licensed to practice law, and added her to the No Fly List.[71] Radack believes that these internal channels "at best do nothing and at worst target whistleblowers."[72]

As a candidate in the 2008 election, Barack Obama pledged to protect government whistleblowers.

Finally, according to the DoD IG's own records, the vast majority of reprisal complaints it investigates are found to be unsubstantiated. According to the DoD IG Semiannual Report to Congress, during the first half of fiscal year 2015 the DoD IG received 591 whistleblower reprisal complaints and closed 671. The IG substantiated only 9% of the whistleblower reprisal complaints that it investigated. The rate for intelligence community whistleblowers was even lower: the IG closed 9 intelligence community reprisal cases under PPD-19 and failed to substantiate any of them. The IG also failed to substantiate any of the 52 reprisal complaints it received from defense contractors.[73] These statistics suggest that intelligence community employees and contractors who seek to prove retaliation face long odds.

4. Failure to protect external disclosures: Intelligence community whistleblowers in the United States have no statutory protections for making disclosures to the media, even if they reveal unclassified information.[74] In contrast, other federal government employees are protected from reprisal when they make external disclosures to the media, provided that the disclosure meets certain standards and the information disclosed is not classified.[75] International norms also promote external disclosure. Specifically, Tshwane Principle 40 recommends that national laws should protect external disclosures that meet certain criteria (e.g. that the person only "disclosed the amount of information that was reasonably necessary to bring to light the wrongdoing").[76]

There is, however, one exception to this lack of protection for external disclosures that intelligence community employees could potentially utilize to their advantage. Most employees in the intelligence community sign nondisclosure agreements and are required to go through a prepublication review process before they can externally disclose or publish any information about their experience working for the government.[77] The prepublication review process is subject to judicial review, meaning that if an agency unreasonably denies permission to publish, a judge can override their refusal. Stephen Kohn, who has represented numerous whistleblowers, argues that whistleblowers should avail themselves of the prepublication review process, saying, "I often have a whistleblower write out his disclosure and submit it to prepublication clearance. Then they're fully protected and have a right to judicial review," if the agency denies the request or does not approve it in a timely manner. Kohn says this judicial review of a classification decision is "a very powerful tool," and that "whistleblowers can actually go to the press if they go through this process first. And it's with immunity, they can't be touched." He says that he's used this process effectively in the past, but that many whistleblowers aren't aware of this option and don't use it.[78]

5. Failure to address overclassification: There was a broad consensus among interviewees, including some working in Congress and the executive branch, that overclassification is a pervasive problem throughout the government and that recent national security leaks underscore the need to reform the classification system. As Robert S. Litt, General Counsel for the Office of the Director of National Intelligence said, "One lesson that I have drawn from the recent events—and it is a lesson that others including the Director of National Intelligence have drawn as well—is that we would likely have suffered less damage from the leaks had we been more forthcoming about some of our activities, and particularly about the policies and decisions behind those activities …We need to scrutinize more closely what truly needs to be classified in order to protect what needs to be protected.'[79]

Congress has examined the issue of overclassification on numerous occasions, and consistently found it to be pervasive.[80] Both the Snowden and the Chelsea Manning leaks provided clear, anecdotal examples of government documents that either should never have been, or were improperly, classified.[81] According to John Fitzpatrick, the director of the Information Security Oversight Office (ISOO), the government office responsible for policy and oversight of the classification system, "Overclassification can mean something was classified that shouldn't have been, it was held as classified longer than it needed to have been, or it was classified at a higher level than it needed to have been."[82] Improper classification violates Executive Order 13526, which specifies what information can and cannot be classified. Section 1.7 of the Order specifically prohibits the classification of information in order to "conceal violations of law, inefficiency, or administrative error," or "prevent embarrassment to a person, organization, or agency," among other things.[83]

A full analysis of how to address the government's overclassification problem is beyond the scope of this report, and has already been addressed in detail by several government studies.[84] However, several interviewees suggested that a change in the incentive structure for classification would help. Under current law, there is no consequence for incorrectly classifying a document other than its declassification, whereas there are many potential consequences for failing to classify a document. As ISOO director John Fitzpatrick said, government employees often make "risk-averse decisions," which "leads to a culture where now folks tend to look for the reason to classify rather than the reason not to. I think it's a fair criticism of the system to say that's a line where culturally, more attention could be paid to help individuals and agencies to understand the full implications of decision to classify rather than to fear the one-in-a-thousand chance that if they don't something bad might happen."[85]

Fitzpatrick believes that "there's no clearer incentive for declassification than spending more on it and it's absolutely true that not enough is spent on it. To see more declassification happen, we have to invest in technology that would allow agencies to use their intellectual resources and other resources better and smarter to produce what is required by the policies, which is to declassify information on a time-based schedule."[86]

Many interviewees argued that a leaker should not be prosecuted for exposing information that was improperly classified. As Elizabeth Goitein of the Brennan Center for Justice said, "If you really had a reason to believe that every decision to classify information was justified, then it might make sense to attach criminal sanctions to any unauthorized disclosure of classified information. But we're not even close to that world and I doubt we'll ever be close to that world."[87]

6. Failure to deal with misconduct on an institutional level: Intelligence community whistleblowers are not protected from retaliation if they raise "differences of opinions concerning public policy matters," internally but are protected if they raise violations of laws, rules or regulations.[88] But in situations where the difference of opinion relates to the overall legality or constitutionality of a government action or program that has not been made public, the potential whistleblower is left in a precarious position.

"Internal channels are useless for things like torture, warrantless wiretapping, any of those major systemic abuses, like the ones we saw after 9/11."

As Ben Wizner, Snowden's attorney, said, "there is no place to complain internally about something that has been approved by all of your superiors and is known to all of them and has been briefed to and approved by the official oversight mechanisms," including the congressional intelligence committees. Wizner further noted, "Even if you had a well-functioning internal complaint system, there is nowhere for someone like that to go. What he [Snowden] was confronting was an entire system of global surveillance that had been deployed and deemed legal by the system without consultation with the public. So for him, the only way to solve that problem was to bring in the public in the conversation through the media."[89] Indeed, Dan Meyer, the government's executive director for intelligence community whistleblowing and source protection (ICW&SP) said, "If Snowden could have come to me I would have said 'that's nice you think it's unconstitutional, but staking your career on your hypothetical opinion about constitutionality is very dangerous."[90]

Many of the people whom PEN interviewed thought the recent reforms hadn't done enough to address this problem. As Elizabeth Goitein said:

> The whistleblower laws for intelligence community members pretend that there's no such thing as agency level misconduct and we know that that's not the case… If what you're talking about is official misconduct that has been sanctioned by the agency, then obviously reporting that misconduct to that agency is not going to help. So internal channels are useless for things like torture, warrantless wiretapping, any of those major systemic abuses, like the ones we saw after 9/11.[91]

Specific Legal Mechanisms to Protect National Security Whistleblowers

While the laws intended to protect intelligence community whistleblowers provide many opportunities for the government to circumvent protection, they do exist in some format. These include the Intelligence Community Whistleblower Protection Act, Presidential Policy Directive 19, and certain protections included in the 2014 Intelligence Authorization Act. The protections available to intelligence community contractors are also briefly discussed.

The Intelligence Community Whistleblower Protection Act of 1998 (ICWPA): The ICWPA was passed in 1998 with the goal of providing a secure means of disclosing certain types of classified information to some members of Congress. The law, which applies to both employees and contractors, requires the whistleblower to notify the agency head, through an Inspector General, before they can report an "urgent" concern to a congressional intelligence committee. The law focuses on disclosures to the intelligence committees and not Congress more broadly.[92] In some cases, however, the intelligence committees will already be aware of the issues raised by a whistleblower and may have little interest in addressing the employee's concern. When that happens the Act offers no further recourse. For example, former CIA analyst and case officer John Kiriakou told PEN that he chose not to use internal channels to raise concerns about the agency's use of enhanced interrogation techniques and waterboarding because he believed he "wouldn't have gotten anywhere" as his superiors and the congressional intelligence committees were already aware of the program.[93]

ICWPA doesn't prohibit employment-related retaliation and it provides no mechanism, such as access to a court or administrative body, for challenging retaliation that may occur as a result of having made a disclosure. This lack of protection is exacerbated by the fact that the process outlined in the law is not strictly confidential and may result in the whistleblower's superiors being alerted to his or her disclosure, which may lead to retaliation.[94] As Michael German with the Brennan Center for Justice said, the ICWPA, "provides a right to report internally but no remedy when that right is infringed, which means that there is no right at all."[95]

According to the Office of the Director of National Intelligence, ICWPA has rarely been utilized. From 1999-2009, only 10 complaints/disclosures were filed under this law, four of which were found to be credible by the relevant Inspector General. In three of these ten cases the whistleblower claimed that s/he was retaliated against: two CIA cases and one DOJ case. Subsequent investigations by the CIA and DOJ failed to find evidence of retaliation in any of these cases.[96]

The experiences of NSA whistleblowers William Binney, J. Kirk Wiebe and Ed Loomis may shed light on why few other intelligence community employees have tried to make use of ICWPA. Each attempted to use the ICWPA framework to use internal channels to blow the whistle on mismanagement, fraud and waste of government funds connected to Trailblazer, an

Protesters in Berlin, Germany in June 2013.

PHOTOGRAPH © MIKE HERBST

expensive and invasive NSA intelligence-gathering software program that was designed to sift through digital communications.[97] They contacted Diane Roark, a staffer for the chair of the House Permanent Select Committee on Intelligence, and she helped them file a joint complaint in 2002 with the DoD IG.[98] The three whistleblowers and Roark were subsequently subjected to fierce retaliation: the FBI raided their houses in 2007 (officers put a gun to Binney's head while he was naked in the shower), they were subjected to investigations, and their security clearances were revoked.[99] According to Binney, the government tried to indict them three separate times, but ultimately dropped the charges after the whistleblowers presented exculpatory evidence, as well as evidence of malicious prosecution.[100]

While Binney was ultimately happy with the DoD IG's investigative report on Trailblazer, which was based on the whistleblowers' disclosures, he was frustrated when most of it was redacted in the version made public, which he believes

was done to avoid embarrassing the NSA.[101] Moreover, the DoD IG not only failed to protect him and the other whistleblowers from retaliation, but also provided their names to the Justice Department for potential criminal prosecution under the Espionage Act.[102] Binney said, "This discredits the IG's office for any future reporters of fraud in the DoD. And I would add, says to all government employees that the requirement that they report fraud, corruption and criminal activity is disingenuous."[103]

In Snowden's case, if under ICWPA he had raised his concerns with Congress or the NSA Inspector General, the law would not have protected him from retaliatory employment action for having done so. Moreover, it is unclear whether ICWPA would have applied to Snowden at all, as it creates a process for reporting an "urgent concern" to Congress but excludes from that definition "differences of opinions concerning public policy matters."[104]

Protections available to intelligence community contractors: In the National Defense Authorization Act for Fiscal Year 2008 (NDAA), which was signed by President George W. Bush, Congress enacted protections for DoD and NASA contractors against reprisal for having made disclosures to a member of Congress, an Inspector General, the Government Accountability Office, or responsible DoD employees. The law also created a process through which contractors could request a remedy, initially through agency Inspector General investigations and subsequently through access to district court jury trials for civil complaints.[105] The law covered close to 60 percent of government contractors, including NSA, DIA and other intelligence community whistleblowers working at the Pentagon, but it didn't cover CIA contractors.[106] Although the protections were part of an annual authorization bill, they were permanent, unless repealed by a future Congress.[107] While critics of the law predicted that it would result in a flood of court cases, from 2008 to 2012, only 25 cases were filed in court under the provision. According to the Government Accountability Project, a whistleblower protection organization, the law "was working as intended and did not produce any adverse impacts on national security during its five-year lifespan."[108]

Separately, as part of the stimulus-spending bill in 2009, Congress temporarily extended best practice whistleblower protections to all government contractors who worked for a recipient of stimulus money, including CIA contractors. These protections included the right to jury trials in court to challenge retaliation. However, Congress subsequently stripped intelligence community contractors of these rights, as well as all of the preexisting protections applicable to them (including those under the 2008 NDAA), in the 2013 NDAA.[109] As a result, since 2013 intelligence community contractors like Snowden have had significantly fewer (and weaker) protections than other government contractors, and no statutory protection against retaliation (with the exception of security clearance-related reprisals, from which they are protected from under PPD-19). Furthermore, the shifting landscape with respect to these legal protections itself acts as a constraint on contractors who are aware that protections granted by Congress may be withdrawn at any point.

According to the *Washington Post*, "close to 30 percent of the workforce in the intelligence agencies is contractors," including 265,000 people with top-secret clearances.[110] As Liz Hempowicz, public policy associate at the Project on Government Oversight (POGO) said, because contractors "are a growing part of our intelligence community, it doesn't make sense to leave them out of these protections."[111] When PEN raised the issue of protection for contractors with a staffer for the House Permanent Select Committee on Intelligence, the staff member, who asked not to be named, said that the Committee is "taking a wait and see approach" to make sure the new rights are "going well" for intelligence community employees before taking further action regarding contractors. Such a cautionary approach might make sense if giving contractors stronger whistleblower rights represented an unprecedented step, but is harder to justify given that contractors previously enjoyed much stronger protections than they do at present.

Presidential Policy Directive 19 (PPD-19): In 2012, President Obama issued a directive titled "Protecting Whistleblowers with Access to Classified Information" (PPD-19), after provisions protecting intelligence community whistleblowers were stripped from the proposed Whistleblower Protection Enhancement Act. The order prohibits retaliation against intelligence community employees who make a protected disclosure through the proper internal channels and establishes remedies for substantiated retaliation claims.[112] Whistleblower advocates regard PPD-19 as a firm step forward. As Tom Devine of GAP said, the issuance of PPD-19 was a "paradigm shift" that will "force agencies to work a lot harder to make their reprisals stick."[113] However, advocates have also noted many flaws in the order.

The directive requires each intelligence community agency to establish policies and procedures that prohibit retaliation and to create a process through which the agency's Inspector General can review personnel or security clearance decisions alleged to be retaliatory.[114] This presents a conflict of interest, as the agencies responsible for writing regulations to enforce these protections are ordinarily those who would find themselves named as defendants in potential lawsuits brought by whistleblowers.[115] Moreover, initial review of retaliation claims occurs within the whistleblower's agency rather than by an independent body. Whistleblower attorney Jesselyn Radack said PPD-19 creates a situation in which the "fox is guarding the henhouse."[116]

The directive also creates a process by which a whistleblower can appeal an agency-level decision regarding a retaliation claim to the Inspector General of the Intelligence Community (IC IG), who can then decide whether or not to convene an "External Review Panel" comprised of three Inspectors General, to review it. But the Panel can only make

recommendations back to the head of the original agency where the complaint was first lodged, and cannot actually require agencies to correct it.[117] According to Tom Devine, "this doesn't break the paradigm conflict of interest," as the IGs are still part of the intelligence community, and aren't "qualified to serve the role of an appellate court in any credible due process system." He claims that the "process for enforcement turns the new rights into Trojan Horses for anyone who takes them seriously."[118] Several other interviewees echoed Devine's view. They believe that the framework created by PPD-19 is insufficient and that intelligence community whistleblowers will only have effective, meaningful rights if they are given access to courts to challenge retaliation.

PPD-19 also fails to protect contractors from any form of reprisal except decisions connected to their security clearance, which leaves them open to retaliatory terminations and investigations, not to mention criminal prosecutions.[119] As whistleblower lawyer Mark Zaid said, excluding contractors was "a remarkable and obviously intentional oversight, given the significant number of contractors who now work within the intelligence community. This is a gap that desperately needs to be closed, as I often have contractors coming to me with whistleblower-type concerns and they are the least protected of them all."[120]

Moreover, PPD-19 is not a law, so portions of it that have not been otherwise codified into statutes can be revoked or modified at any time by a future President.[121] In the opinion of Mike German with the Brennan Center for Justice, the government advocated for the removal of intelligence community protections from the WPEA and the issuance of PPD-19 instead because "a directive is much easier to change and harder [for the employee] to enforce."[122]

Implementation of PPD-19: In 2010, Congress created the Inspector General for the Intelligence Community (IC IG). This official answers to Congress and to the Director of National Intelligence.[123] As a result, there are now several layers of Inspectors General available to workers in the intelligence community. For example, an NSA employee could go to the NSA IG, then to the DoD IG, and then to the IC IG.[124] Each agency has its own regulations under PPD-19, so the process for dealing with a whistleblower retaliation complaint varies. In general, the originating agency's IG will usually do the initial review of a retaliation complaint. If the whistleblower does not find the IG's response to be adequate s/he may be able to have the DOD IG review the claim, depending on what agency s/he works for (this option would not, for example, be available to CIA employees). Once that process is exhausted, a whistleblower could go to the IC IG.[125]

In 2013 the Inspector General for the Intelligence Community created the Intelligence Community Whistleblowing & Source Protection (ICW&SP) directorate to help promote whistleblowing as an internal function.[126] Civil society groups have praised the selection of former whistleblower Dan Meyer as the first executive director of ICW&SP.[127] In 2014, Meyer's office, which is part of the IC IG, "executed twenty-eight outreach events, conducted seventeen training sessions, processed three reports of urgent concern to Congress…docketed four requests for PPD-19 review, and referred four reprisal complaints to local inspectors general." ICW&SP is also creating a "community-wide training on the Intelligence Community whistleblowing program," which, according to Meyer, "will begin the culture change necessary to make the accepted mission of whistleblowing into a mission that is integrated into doctrine."[128]

Meyer hopes to reassert whistleblowing as a vital internal function and believes that "the promotion of whistleblowing as an accepted federal mission engaging all supervisors, managers, and employees, enables the federal bureaucracy to curtail domestic, internal corruption."[129] He told PEN that if there is ever another incident similar to that of the Edward Snowden disclosures, "what I'm going to be advising my boss is that we need to find out whether that employee knew how to disclose lawfully, were they trained on that, did the management keep records of the training, why do we have a situation where information is leaving our community improperly or unlawfully…so a lot of what I'm focusing on in the outreach is identifying for supervisors and managers that I fully expect them to be under review if we have another incident the size of *The Guardian* and WikiLeaks."[130] This statement reflects Meyer's commitment to ensuring that employees are informed about the authorized avenues for blowing the whistle, with the aim of deterring and preventing external disclosures.

While civil society organizations have praised the work done by Meyer, they are skeptical about whether his office will be able to remedy the underlying deficiencies in the intelligence community whistleblower protection system. As Tom Devine said, the ICW&SP executive director "has already obtained relief against retaliation in a handful of cases. It has a good faith staff trying to turn those rights into reality, but the challenge is hopelessly unrealistic." He noted, for example, that the ICW&SP had only "token resources" and a "staff of less than half a dozen who police the entire intelligence community."[131] Moreover, the appeals system is still designed with a structural conflict of interest that is likely to prove detrimental to whistleblowers, as previously discussed. Devine argued, "The actual rights look pretty good on paper, but the problem is they're not worth the paper they're written on and [won't be] until there's independent due process."[132]

Intelligence Authorization Act for Fiscal Year 2014: This Act, which was signed into law on July 7, 2014, indefinitely codifies some protections from PPD-19.[133] It strengthens whistleblowing protections for intelligence community workers by prohibiting retaliation against an employee who reports violations to the Director of National Intelligence, the IC IG, the agency's head, the agency's IG, a Congressional intelligence committee, or another designated official.[134] It also offers whistleblowers protection from adverse security

"The real concern we should have from the point of view of democratic government ***is not so much [Snowden's] right to speak, as the public's right to know…"***

clearance and information access determinations and offers additional enforcement mechanisms for challenging these forms of retaliation.[135]

However, the protections established by this law are very weak. The law prohibits judicial review and does not address what forms of remedy would be available to a whistleblower who substantiated a claim of retaliation.[136] Enforcement against non-security clearance-related retaliation appears ultimately to be left to the President, who can choose whether or not to develop enforcement procedures separate from those in PPD-19.[137] The law does not appear to extend to contractors and provides no explicit protection against criminal prosecution. [138] According to Stephen Kohn, the executive director of the National Whistleblowers Center, this law was a "very small step forward," as the protections it created are "weak and essentially unenforceable." He says that the law "could easily morph into a bureaucratic trap leaving whistleblowers vulnerable and unemployed."[139] At the very least, the law further exacerbates, rather than clarifies, the confusing state of authorities regarding which disclosures by which employees to which offices are and are not protected—and what they are or are not protected *from*.

The law also creates some conflicts with PPD-19 that may be counter-productive. For example, the standard that an agency has to meet to prove it wasn't retaliating against the whistleblower is lower in the Act than it is in PPD-19. The Act requires only that an agency establish by a "preponderance of the evidence" that it would have taken the same action absent the whistleblower's disclosures, whereas PPD-19 allowed for the use of the higher "clear and convincing" standard.[140] As ICW&SP Executive Director Dan Meyer noted, "for a whistleblower who is locked out and doesn't have access to the evidence, not having the clear and convincing standard can be very, very difficult... I'm very suspicious of whether a whistleblower can prevail with a preponderance standard unless there's complete buffoonery on the part of management."[141]

In conclusion, there are numerous weaknesses in the laws designed to protect intelligence community whistleblowers, not the least of which is the absence of a clear, coherent, and easily understandable regime. Due to the loopholes in many of the policies and regulations designed to help protect the whistleblowers, they may still face reprisals even after using authorized channels to blow the whistle on genuinely inappropriate or unlawful government conduct. Unless these problems are addressed, potential whistleblowers may continue to resort to external disclosures rather than using unreliable and unclear internal channels. As whistleblower attorney Jesselyn Radack said, "without adequate internal disclosure channels, intelligence whistleblowers are faced with an impossible choice—either risk their careers (and, in Drake's case, his liberty) by making unprotected disclosures, or remain silent about grave national security problems…The best way to prevent both 'leaks' and 'leak prosecutions' is to institute meaningful and effective internal whistleblowing channels."[142]

Laws and Policies Used Against National Security Leakers

The insufficiencies of the current national security whistleblower protection regime are exacerbated by the current administration's aggressive pursuit of criminal liability for national security leakers. The laws pertaining to national security leaks comprise a "dizzying array of overlapping, inconsistent and vague criminal statutes—none of which is specifically addressed to national security leaking, as such," according to national security law expert Professor Stephen Vladeck. Instead, according to Vladeck, "the government has historically been forced to shoehorn national security 'leaking' into criminal laws designed for far more egregious offenses (such as spying), or far more common offenses (such as conversion of government property)."[143] The resulting tangle of laws has created confusion and apprehension surrounding what national security employees may legally say and do to raise concerns over government practices. Former CIA general counsel Anthony Lapham noted, "It is likely that the very obscurity of these laws serves to deter perfectly legitimate expression and debate by persons who must be as unsure of their liabilities as I am unsure of their obligations."[144]

Many interviewees criticized the use of criminal statutes—especially the Espionage Act—to prosecute those who reveal information with the aim of advancing the public interest. For example, Washington University Law Professor Kathleen Clark said, "Our current legal framework is completely inadequate in protecting disclosures in the public interest from an executive branch that has these powerful tools."[145] Many

interviewees also believed that the prosecution of intelligence community leakers has had a chilling effect on free expression and the public's right to know. As Snowden's attorney, Ben Wizner, said, "The real concern we should have from the point of view of democratic government is not so much [Snowden's] right to speak, as the public's right to know… The criminal laws that punish people for providing this information to the media or public without authorization are intended to prevent the public from knowing." [146] Journalist and Chelsea Manning biographer Denver Nicks said he thinks "the intent of the Obama administration's crackdown is to prevent people from speaking out and I think it has done that to some degree." He said that this "has made it harder to be a journalist, in particular a national security reporter in D.C."[147]

There are several criminal laws that the administration has used to prosecute government employees or contractors who leak information to the press claiming that their intent in doing so is to advance the public interest. The most commonly used and punitive is the Espionage Act, which tends to be the focus of these prosecutions, as it is a broad, vague charge not easily defended against. The government will sometimes add charges under other laws as well, including prohibitions on false statements to investigators, conversion of government property, and destruction of evidence.[148] This section will focus primarily on the Espionage Act. This section also explores some recent developments within the executive branch that further limit the public disclosure of national security information.

Espionage Act of 1917: This law was passed just after the United States entered World War I, amid a climate of intense fear of Communism after the Bolshevik Revolution. It was aimed at punishing espionage committed during wartime. The law criminalizes the communication, transmission, gathering and retention of national defense information.[149] It was written before the classification system came into existence and was also drafted before the Supreme Court's modern reinvigoration of the First Amendment and its articulation of Fifth Amendment "vagueness" doctrine.[150] According to Vladeck, the law therefore "lacks the hallmarks of a carefully and precisely defined statutory restriction on speech."[151]

Prior to the current administration, the Espionage Act had only been used on three occasions against national security leakers: in 1973 against Daniel Ellsberg and Anthony Russo in the Pentagon Papers case; in 1984 against National Intelligence Support Center employee Samuel Morison for providing a publication with classified photographs related to a Soviet aircraft carrier; and in 2005 against Pentagon analyst Lawrence Franklin and lobbyists Steven Rosen and Keith Weissman for disclosing information about the Iranian nuclear program (Franklin disclosed it to Rosen and Weissman, who then allegedly leaked it to the press.)[152]

Under the Bush administration, leaks were aggressively investigated, but rarely prosecuted. According to Steven Aftergood, director of the Federation of American Scientists' Project on Government Secrecy, "between 2005 and 2009, U.S. intelligence agencies submitted 183 'referrals' to the Department of Justice reporting unauthorized disclosures of classified intelligence. Based on those referrals or on its own initiative, the FBI opened 26 leak investigations, and the investigations led to the identification of 14 suspects."[153] But the Bush administration only prosecuted one of these leakers: Lawrence Franklin (though it also prosecuted the lobbyists he leaked to).[154]

Prior to the current administration, the Espionage Act had only been used on three occasions against individuals who allegedly leaked classified information to the press.

In contrast, there are eight publicly reported cases in which the Obama administration has charged leakers under the Espionage Act: Shamai Leibowitz, Stephen Jin-Woo Kim, Thomas Drake, Chelsea Manning, Jeffrey Sterling, John Kiriakou, James Hitselberger, and Donald Sachtleben.[155] Criminal charges filed against Edward Snowden were also leaked publicly. The amount of information leaked varies widely from case to case, from the mere discussion of national security information with a journalist in Kim's case, to the disclosure of hundreds of thousands of documents in Manning's case.[156]

According to Obama's first director of national intelligence, Dennis C. Blair, the administration started targeting leakers in June 2009, after an alleged leak to *Fox News* journalist James Rosen revealed information related to an imminent North Korean nuclear test.[157] Blair said that he and then-Attorney General Eric H. Holder Jr. initiated prosecutions because "We were hoping to get somebody and make people realize that there are consequences to this and it needed to stop. It was never a conscious decision to bring more of these cases than we ever had." According to Matthew Miller, Holder's former spokesman, several factors led to the increase in prosecution, including an uptick in the number of crime reports from intelligence agencies and pressure from Capitol Hill to prosecute leakers.[158]

Some may think that technology also played a role in the increase in prosecutions, as it made it easier for potential leakers to obtain and release vast quantities of information, as

Chelsea Manning and Edward Snowden did; but as Harvard Law School Professor Yochai Benkler has written:

> There is, however, no robust evidence that the number of national security leaks has increased in the past decade or so. Moreover, the technological thesis does not fit the fact that of the sixteen national security leak and whistleblowing cases of the past decade, only two—Manning and Snowden—were facilitated by the Internet and computers. What does appear to have increased, however, is the number of national security leaks that purport to expose systemic abuse or a systemic need for accountability… aggressive prosecutions are merely a symptom of the self-same post-9/11 national security overreach that instigated the legitimacy crisis: they manifest the government's need to shield its controversial actions from public scrutiny and debate.[159]

Benkler called such leaks "accountability leaks." He noted that, "Unlike normal leaks, which preserve a space for leaking useful to leaders in the national security system and therefore enjoy a certain laxity in enforcement, accountability leaks that expose systemic illegality, incompetence, error, or malfeasance challenge the system they expose in ways that make the leakers the target of heightened enforcement." He claimed that such accountability leaks, "only occur when the incongruity between what the system is doing and what conscience dictates to individual insiders is so great that they become willing to take that risk."[160]

The difficulties of defending a leaker from Espionage Act charges: Almost all of the non-government representatives whom PEN interviewed—including activists, lawyers, journalists and whistleblowers—thought the Espionage Act had been used inappropriately in leak cases that have a public interest component. Experts described it as "too blunt an instrument," "aggressive, broad and suppressive," a "tool of intimidation," chilling of free speech, and a "poor vehicle for prosecuting leakers and whistleblowers."[161]

U.S. Secretary of State John Kerry has said that, if Snowden wants to argue that his leaks were necessary, he should "come back and make his case. If he cares so much about America and he believes in America, he should trust the American system of justice."[162] However, Kerry's statement is not mindful of the strictures of an Espionage Act prosecution. As whistleblower Daniel Ellsberg said, "The current state of whistleblowing prosecutions under the Espionage Act makes a truly fair trial wholly unavailable to an American who has exposed classified wrongdoing."[163]

It is extremely difficult for a leaker to defend him or herself from Espionage Act charges. There is no public interest defense to the Act, and courts have ruled that a defendant is not allowed to argue that the leaks were in the public interest nor can they mention the reforms that happened as a result. The courts have also found that the leaker's intent is irrelevant—at least until sentencing—and that the government "need not show" that the leaked information "could damage U.S. national security or benefit a foreign power, even potentially."[164] In addition, the courts have rejected the "improper classification" defense, so defendants cannot challenge whether or not documents should have been classified in the first place.[165] In the Drake case, for example, the defense team would have been barred from using both the words "whistleblowing" and "overclassification" if the case had gone to trial.[166] As Trevor Timm, executive director of the Freedom of the Press Foundation, said, "basically any information the whistleblower or source would want to bring up at trial to show that they are not guilty of violating the Espionage Act the jury would never hear. It's almost a

SECTIONS OF THE ESPIONAGE ACT THAT ARE MOST FREQUENTLY USED AGAINST LEAKERS

18 U.S.C. § 793 (d): "Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it;"

18 U.S.C. § 793 (e): "Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it...Shall be fined under this title or imprisoned not more than ten years, or both."

certainty that because the law is so broadly written that they would be convicted no matter what."[167]

In several cases, an intelligence community employee has publicly disclosed non-classified information, only for the government to retroactively classify it.[168] This happened in Jeffrey Sterling's case, in which the government retroactively classified three documents as secret and used these documents as part of the evidence used to convict him under the Espionage Act, and in Thomas Drake's case, in which the government retroactively classified five documents in an apparent attempt to strengthen their case for prosecution.[169]

It is also important to note that under the Espionage Act, it does not matter to whom a leaker discloses information, as the law covers disclosures made to anyone "not entitled to receive" national defense information, not just agents of foreign governments. In 1988 the Fourth Circuit Court of Appeals confirmed in the *Morison* judgment that the audience to which the information is leaked is irrelevant. The court specifically stated that there was no evidence in the legislative record that Congress intended to exempt transmissions "to a representative of the press."[170]

Moreover, it is difficult and expensive for a national security leaker to defend him or herself from Espionage Act charges. Those who are found guilty of violating section 18 U.S.C. § 793 of the Espionage Act—the section most commonly used against leakers—could be imprisoned for up to ten years and fined.[171] Many defendants have chosen to settle rather than go to court.[172] Defending oneself from Espionage Act charges is estimated to cost between $1 million and $3 million should the case proceed to a trial.[173] As Thomas Drake said, "Criminal prosecution completely upends your life… It practically bankrupts you, breaks you and makes you unemployable." He added that, "By virtue of being charged under the Espionage Act you're already guilty… People will usually plead guilty under a lesser charge or a reduced sentence, which may still be many years in prison.[174] Shamai Leibowitz said the government uses this law because it "gives them leverage when it comes to sentencing to really throw the book at people." He believes the government's intention is not to go to trial, but rather to get the leaker to settle.[175]

Applicability to leaks to the press: The Espionage Act's scope is not limited to the initial party who disclosed national defense information; it could conceivably be applied to anyone who redistributes the information, including the press, even if the information is already public.[176] Indeed, some provisions of the Act, including § 794 (b), 797, and 798 (a), explicitly state that they apply to a person who "publishes" information. The George W. Bush administration used the law against two people who redistributed leaked information when it prosecuted American Israeli Public Affairs Committee lobbyists Steven J. Rosen and Keith Weissman under the Act for disclosing to the media and Israeli officials information they received from Pentagon analyst Lawrence Franklin.[177] Moreover, a 2011 study found that the U.S. government had "considered" bringing charges against a member of the media for having published leaked information "on at least four occasions," but none of these cases proceeded to prosecution.[178]

The courts have generally recognized that media outlets have more protection under the First Amendment than whistleblowers do. As attorney Bruce Methven wrote, "The United States Supreme Court's solution to the government information problem has been to uphold subsequent punishment of 'insiders' who leak unauthorized information but to leave the press free to publish virtually anything that falls into its hands."[179] As Professor David Pozen wrote, there is a "source/distributor divide," in which "the First Amendment has been construed to provide so little protection for the leaker and yet so much protection for the journalist who knowingly publishes the fruits of the leaker's illicit conduct... Courts and prosecutors have privileged journalists over leakers, it is said, because of the former's special First Amendment status and the latter's consent to nondisclosure as a condition of employment."[180]

This doesn't mean that publishers and journalists are exempt from the Espionage Act or that the government won't try to prosecute them. The administration is reportedly considering bringing a case against Wikileaks founder Julian Assange.[181] Former *Guardian* journalist Glenn Greenwald was initially hesitant to return to the United States after writing stories based on Snowden's documents because he had "been told by pretty much everybody I have asked, including lawyers for *The Guardian*, my personal lawyer, lawyers I trust, political people who are well connected that…the chances that I would be arrested are something more than trivial."[182] However, if the government were to bring such a case, the courts may be less receptive than they are toward prosecutions of leakers.

But the government has other tools, short of formal prosecution, that it can use to intimidate journalists and chill free speech. For example, in the Stephen Jin-Woo Kim leak case, the government labeled *Fox News* journalist James Rosen as a "criminal co-conspirator" in an application for a search warrant to seize Rosen's telephone and personal email records. In the application, the government claimed that Rosen "asked, solicited and encouraged Mr. Kim to disclose sensitive United States internal documents and intelligence information."[183] This was a significant shift in the Justice Department's approach to journalists who interact with confidential sources who may be disclosing classified information. New Jersey Superior Court Judge Andrew Napolitano noted that the case marked "the first time that the federal government has moved to this level of taking ordinary, reasonable, traditional, lawful reporter skills and claiming they constitute criminal behavior."[184] As Kim's attorney said, naming Rosen as an unindicted co-conspirator in an Espionage Act case "certainly sent a chill through the media as I understood it. It is a dangerous and slippery slope for the government to have the ability to name the media as unindicted aiders and abettors of what they say are illegal leaks, because it has the natural impact of stifling the investigative function of the media and the perfectly appropriate reporting on that which the government often wants to keep secret for improper purposes."[185]

"It is a dangerous and slippery slope for the government to have the ability to name the media as unindicted aiders and abettors of what they say are illegal leaks."

The government can also subpoena a journalist to compel him or her to identify a source. In fact, the Obama administration has subpoenaed more journalists than all former administrations combined.[186] For example, both the Bush and Obama administrations issued subpoenas to *New York Times* journalist James Risen to try to force him to reveal the source who provided him with information about the CIA's "Operation Merlin" program for his book, *State of War*.[187] Although Risen attempted to battle the subpoena in court, he lost that battle. While a federal district court judge held that Risen did not have to reveal his source, an appellate court overturned that decision, finding that reporters are not protected from having to testify "in criminal proceedings about criminal conduct that the reporter personally witnessed or participated in."[188] Risen appealed to the Supreme Court, but the Court rejected his appeal.[189]

After sustained pressure from news organizations and press freedom advocates, then-Attorney General Eric Holder promised in 2014 that "no reporter who is doing his job is going to go to jail," a promise that has since been reaffirmed by Loretta Lynch.[190] Holder also issued new DOJ guidelines outlining the procedures the agency should follow before obtaining information or records from the media or questioning, arresting or charging a journalist. These guidelines make it more difficult for the government to obtain journalists' records through subpoenas, court warrants and other tools, including a requirement that alternative means of identifying a source be pursued before issuing a subpoena.[191] However, the guidelines apparently do not restrict the use of national security letters to obtain transactional data like phone numbers or records of meetings, so the DOJ can still use them to seize records and identify sources.[192] As long as the government is able to do this, journalists will be unable to fully protect the confidentiality of their sources.

In January 2015, Risen took the stand in a federal district court hearing, but refused to answer any questions that could identify his source(s).[193] Shortly thereafter, the Justice Department announced that it would abandon its efforts to force Risen to testify. Ultimately, Sterling was convicted without Risen's testimony, as the prosecution had obtained phone and email records that proved that Sterling had been in contact with Risen.[194]

The Risen case also shows how the government attempts to identify leakers by obtaining a journalist's or media organization's records. The DOJ obtained Risen's credit card and bank records, as well as his credit reports and travel records, in an attempt to identify his source. Risen also believes that the government obtained his phone records without notifying him.[195] In the Donald Sachtleben leak investigation, in which Sachtleben was accused of disclosing national defense information regarding a disrupted terrorist plot in Yemen, the government identified the leaker by secretly subpoenaing two months' worth of *Associated Press* reporters' phone records. It obtained records from more than 20 numbers, including from journalists' home and cell phone numbers.[196] The FBI can also use national security letters—legal orders that are issued to communications service providers without judicial review and usually with gag orders—to secretly obtain the call records of reporters from phone service providers.[197]

These government attempts to identify sources have had a noticeable chilling effect. Associated Press President and CEO Gary Pruitt remarked, following the discovery of the DOJ's secret subpoenas, "some of our long-trusted sources have become nervous and anxious about talking to us—even on stories that aren't about national security." He added that this effect was not limited to the *Associated Press*, as "journalists from other news organizations have personally told me [the DOJ's seizing of the AP's phone records] has intimidated sources from speaking to them."[198] The UN Special Rapporteur on freedom of expression has expressed concern that "government capacity to access the data and footprints that all [digital electronic] devices leave behind has presented serious challenges to confidentiality and anonymity of sources and whistleblowers."[199]

Currently, there is no recognition under federal law of a reporter's privilege that would protect journalists from being forced to identify or testify against confidential sources. While a majority of states have enacted "shield laws" to recognize these protections for journalists, Congress has yet to pass a federal equivalent, though several proposals have been debated.[200] The ability to make a meaningful guarantee of confidentiality to sources is a critical component of investigative journalism, and of the press' ability to fulfill their role as a government watchdog. A wide variety of professional associations of journalists and press freedom organizations have expressed support for a broad, inclusive federal shield law.[201]

Alternatives to the Espionage Act: Because it is intended to punish leaks of information to an enemy and because the courts have determined that a defendant's intent is irrelevant, the Espionage Act is not the only, nor the optimal, legal basis for leak prosecutions. As whistleblower lawyer Jesselyn Radack said, "There are some two dozen other laws that could be used for those kinds of prosecutions, both criminal and

James Risen, Pulitzer Prize-winning reporter for the *New York Times*, fought a seven-year battle against the U.S. government's efforts to force him to reveal the identity of a confidential source.

administrative penalties. Using the Espionage Act is a very deliberate, heavy-handed, draconian way to pursue this."[202] Professor David Pozen has compiled a list of other laws that could be used instead, including 18 U.S.C.§ 1905, which prohibits disclosure of confidential information "not authorized by law," and 18 U.S.C. § 1924, which prohibits "the unauthorized removal and retention of classified documents or materials," both of which carry a maximum sentence of one year in prison, and 18 U.S.C. § 2071, which prohibits the "willful and unlawful concealment, removal, or destruction of government records," and carries a maximum three-year sentence.[203] The government could also seek to enforce employee non-disclosure agreements in court, which could potentially result in the leakers having to pay monetary damages.[204]

Another alternative is to implement administrative remedies, which, according to Pozen, could include "removal, suspension without pay, and denial of access to classified information."[205] The use of administrative penalties was the preferred practice under the Clinton administration. As former Attorney General Janet Reno noted in her 2000 testimony before the U.S. Senate Select Committee on Intelligence, "While we certainly agree that government officials who intentionally leak classified information should be criminally prosecuted where the requisite criminal intent can be established, in general we believe that the better way to address the problem of leaks is to try to prevent them through stricter personnel security practices, including prohibitions on unauthorized contacts with the press, regular security reminders, and through administrative sanctions, such as revocation of clearances."[206] While such sanctions would not apply to leaks by former employees, they could be an effective way to discipline current employees who resort to external channels rather than internal ones.

Potential reforms to the Espionage Act: Numerous proposals for reform or repeal of the Espionage Act have been made, including:

- Repeal the overbroad Espionage Act and replace it with narrower laws designed specifically to address leaking to the press and, separately, actual espionage.
- Reform the Espionage Act to require, in cases where unauthorized disclosures of information are not made to a foreign government, the prosecution to prove that the disclosure actually damaged national security.[207] However, this change may be difficult to enact, as members of Congress have expressed concerns about giving the courts, rather than the executive branch, the power to determine what may reasonably harm national security.[208]
- Replace broad, vague language in the Act. For example, the law's current reference to information "relating to the national defense" covers a vast array of information, and could be made more specific. Other vague terms like "unauthorized possession" could also be replaced with more specifically defined terms.[209]
- Incorporate additional defenses, including:
    - A public interest defense (discussed in more detail below);
    - Allowing the defendant to argue that the information in question was improperly classified;
    - As a defense or mitigating factor, attempts to use internal channels to raise concerns prior to making an external disclosure.

However, some experts expressed reservations about opening the Espionage Act to amendment and said that doing so might result in Congress replacing it with an even more severe law. Moreover, congressional staffers with whom PEN spoke did not see near-term prospects for legislative reform of the Act. As Stephen Vladeck remarked:

> What's frustrating is that people like me have been telling Congress for the better part of 45 years now,

> ever since the Pentagon Papers case, that it's long past time to reform the Espionage Act. And every five years Congress has hearings, someone introduces a bill and it goes nowhere. In 1973 two Columbia Law professors referred to this as a state of benign indeterminacy, but I'm increasingly unconvinced that it's benign…. I fear that in fact this status quo is increasingly chilling expression that we ought to protect.[210]

The public interest defense: If the Espionage Act is to remain an available means of pursuing national security leakers, Congress (and, failing it, the courts) must allow defendants to raise additional defenses at trial, including a public interest defense.

There are several countries that already have a public interest defense or elements of it in their national security information protection statutes. Denmark's Criminal Code and Canada's Security of Information Act 1985 both provide for a public interest defense.[211] At least seven countries in Europe allow as a defense or mitigating factor the previous usage of internal channels by the whistleblower prior to making an external disclosure. The European Court of Human Rights has also recognized a public interest defense.[212] Finally, the Tshwane Principles require that public employees in criminal and civil proceedings be allowed to raise the defense, "if the public interest in disclosure of the information in question outweighs the public interest in non-disclosure." The document describes standards that prosecutorial and judicial authorities could use to determine whether or not the public interest in disclosure trumps the government's interest in nondisclosure.[213]

A public interest defense to the Espionage Act could follow the model proposed by Professor Yochai Benkler. This model would permit defendants facing Espionage Act charges for the dissemination of information to defend themselves by demonstrating "(a) reasonable belief that exposure discloses a substantial violation of law or substantial systemic error, incompetence, or malfeasance, (b) mitigation to avoid causing imminent, articulable, substantial harm that outweighs the benefit of disclosure, and (c) communication to a channel likely to result in actual exposure to the public." This includes not only mainstream media, but also "an organization that has a capacity or history of managing sensitive documents responsibly." Benkler has also noted that if the Espionage Act were amended to incorporate a public interest defense, some revisions would have to be made to the Classified Information Procedures Act as well, to allow courts to accept as evidence classified documents and descriptions of documents that are already in the public domain.[214]

A staffer for the U.S. Senate Select Committee on Intelligence noted that a public interest defense would be "tricky" to pass because "there's something of an eye of the beholder in that."[215] A test for balancing the government's interest in secrecy with the public interest in disclosure was established in the Supreme Court's 1968 *Pickering v. Board of Education* judgment.[216]

The establishment of an admissible public interest defense is more likely to obtain support from the government than abolishing the Act altogether, as prosecutors would still be able to bring cases under the Espionage Act, and to argue that disclosures were not made in the public interest, or that the harm to the public outweighed the benefit of the disclosure.

Computer Fraud and Abuse Act: The Computer Fraud and Abuse Act of 1986 (CFAA) incorporates language directly from the Espionage Act. The law makes it a crime to access a computer without authorization (or by exceeding "authorized access") to obtain national defense or foreign relations information for the purposes of retaining it or communicating, delivering or transmitting it (or attempting to) to any person "not entitled to receive it."[217] Manning was found guilty of two counts of violating the Computer Fraud and Abuse Act for "exceeding authorized access" to a computer system and Drake pled guilty to the same charge.[218] Search warrants related to WikiLeaks also claim that the organization violated this Act.[219]

According to the Center for Constitutional Rights (CCR), "there is a serious risk" globally that cyber laws like the CFAA, "will displace secrecy laws as a tool to prosecute whistleblowers on the basis of their activities accessing and obtaining information."[220] As Carey Shenkman, a First Amendment and human rights attorney who represents Assange and who is currently working on a book about the Espionage Act, said, "We are seeing growing opposition to the Espionage Act... so there is a real risk that more and more freedom of expression and whistleblowing issues are going to be framed as computer crimes rather than as espionage."[221]

Conversion of government property: Several national security leakers have been charged with the federal crime of theft and conversion of public money, property or records under 18 U.S.C. § 641. In relevant part, it states: "Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract for the United States or any department of agency thereof; or [w]hoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted—[s]hall be fined under this title or imprisoned…"[222]

In short, the statute prohibits the theft of any federal government "thing of value," although that term has not been defined.[223] Specifically, it is unclear if a "thing of value" is limited to a tangible piece or property, or if it also applies to intangible property such as information.[224] The circuits are split on this issue, with the Fourth Circuit interpreting § 641 to include all government produced information, whereas the Ninth Circuit held that information that can be duplicated cannot be a "thing of value."[225] Congressional intent behind the statute is additionally unclear. Some commentators argue that there is no

evidence to support its application to intangible concepts such as information when it was initially passed in the 19th century, although others cite its broad language to indicate an intent to reach a wide array of property—anything that the government values.[226] The U.S. Attorney's Manual suggests that § 641 should not be used to prosecute information leaks as the statute is not listed in its discussion of "Key National Defense and National Security Provisions."[227] Moreover, while the manual states that § 641 prohibits theft or receipt of stolen government information, the Criminal Division writes that the statute should not be used against whistleblowers releasing information for the "primary purpose of disseminating it to the public" when it was not obtained through wiretapping, intercepting correspondence, or through criminal or civil trespass or entry.[228]

Despite the DOJ's advice, ambiguous congressional intent, and conflicting case law, several national security leakers charged under the Espionage Act have also been charged with conversion of government property under § 641. Anthony Russo, Daniel Ellsberg,[229] Samuel Morison,[230] Jeffrey Sterling,[231] Edward Snowden,[232] and Chelsea Manning were all charged with violating this statute.[233] Three of the six were ultimately found guilty; charges against two were dropped;[234] and Snowden's case is pending.

Selective enforcement of criminal laws that apply to leakers: Leaking information to the press is a pervasive practice in Washington. In a 1980s survey conducted by the Harvard Kennedy School of current and former senior government officials, 42% of respondents said they had at least once "felt it appropriate to leak information to the press."[235] In the post-9/11 landscape, Harvard Law School Professor Jack Goldsmith counted hundreds of stories reported in the press that "self-reported disclosure of classified information."[236]

Most of these leaks go unpunished. The case of John Kiriakou, a former CIA analyst and case officer, highlights the inconsistencies and hypocrisies in the administration's decisions regarding which disclosures to prosecute. In 2007, Kiriakou publicly confirmed during an *ABC News* interview that the CIA was using waterboarding as part of its interrogation practices.[237] He was subsequently investigated and charged with three counts of violating the Espionage Act, one count of violating the Intelligence Identities Protection Act and one count of making a false statement. [238] Although these charges were not based on his disclosure to *ABC News*, Kiriakou believes they were brought against him in retaliation for his public disclosure about waterboarding. The specific charges were that in 2008, Kiriakou confirmed the name of a CIA officer—which was already well known to people in the human rights community, according to the Government Accountability Project—to someone who claimed to be writing a book about the agency's rendition practices. In a separate 2008 incident, Kiriakou gave a *New York Times* journalist the business card of a CIA agent who worked for a "private government contractor known for its involvement in torture."[239] That agent had never been undercover and his contact information and affiliation with the CIA was already publicly available on the Internet.[240] Kiriakou faced up to 45 years in prison and millions of dollars in legal fees for these charges. In October 2012, he agreed to plead guilty to one charge of having violated the Intelligence Identities Protection Act by giving a CIA agent's name to a reporter, and was sentenced to 30 months in jail.[241]

The case of John Kiriakou, a former CIA analyst and case officer, highlights the inconsistencies and hypocrisies in the administration's decisions regarding which disclosures to prosecute.

After Kiriakou pled guilty, then-CIA Director David Petraeus released a statement in which he praised the conviction and noted, "There are indeed consequences for those who believe they are above the laws that protect our fellow officers and enable American intelligence agencies to operate with the requisite degree of secrecy."[242] General Petraeus would later be accused of having illegally disclosed classified information to his mistress, including code words, covert officers' names and correspondence with the president. But although Petraeus revealed significantly more information than Kiriakou and didn't claim to be acting in the public interest, he wasn't charged under the Espionage Act or Intelligence Identities Protection Act (IIPA). He pled guilty to removing and retaining classified information and was sentenced to only two years of probation and a $100,000 fine.[243] In addition, no senior government officials have been prosecuted for their role in designing and overseeing the torture program revealed by Kiriakou.

Kiriakou is only the second person to be prosecuted under the IIPA, which carries with it a sentence of up to 15 years in prison.[244] The other person, Sharon Scranage, was prosecuted in 1985 for disclosing information to a foreign agent.[245] During discovery, Kiriakou asked for how often the names of CIA officers were leaked. According to Kiriakou, "It happened so frequently that the Justice Department was unable to answer the question… they said they prosecuted me and not anyone else because of prosecutorial discretion."[246] As Radack, Kiriakou's attorney, said:

> It's the leaks that are in the public interest that are being investigated and prosecuted for espionage and it's the leaks that serve no legitimate right to know or public interest purpose that are given a pass. The government is the biggest leaker in the U.S. Those leaks that benefit the government or make them look good are met with no consequence, whereas leaks that are in the public interest are entirely the ones that have been prosecuted.[247]

Many people whom PEN spoke with echoed the refrain that the government targets leakers selectively in an overly aggressive effort to control the dissemination of information that is of significant interest or benefit to the public. They pointed out that the administration has failed to prosecute the people who leaked classified information about the killing of Osama bin Laden to the *Zero Dark Thirty* film producers or the people who have leaked classified information to journalist Bob Woodward. As Paul Rosenzweig, the editor of the book *Whistleblowers, Leaks and the Media*, said, "There are lots and lots of leaks of highly classified information by very, very senior officials as a means of justifying the president's policies and those people get off scot-free..… What I'm most struck by is if a major does it it's a crime, and if a four-star general does it, it's public relations."[248]

The Insider Threat program and other attempts to crack down on government leaks: In 2011 President Obama issued Executive Order 13,587, which created the "Insider Threat Program." The order attempts to crackdown on unauthorized leaks by creating a government-wide program for "deterring, detecting, and mitigating insider threats, including the safeguarding of classified information…"[249] The program requires federal employees to monitor their co-workers' behavior in order to ensure they are not engaging in unauthorized disclosures.[250] If they fail to report "high-risk persons or behaviors," they could potentially face criminal charges or other penalties.[251]

Although the order says that the program should not be used to prevent employees or contractors from making whistleblower disclosures, there is no enforcement mechanism for this provision.[252] Senator Charles Grassley, a strong advocate for whistleblowers, claims that the "Insider Threat Program has the potential for taking the legs out from underneath all of the whistleblower protections we have."[253] Tom Devine, legal director for GAP, said the program is, "an opportunity to institutionalize retaliatory investigations of whistleblowers."[254] Most of the advocates and whistleblowers with whom PEN talked were critical of the program. Steven Aftergood of the Federation of American Scientists said that Insider Threat "runs the risk of turning government offices into hostile workplaces where everybody feels they are constantly under surveillance."[255] Thomas Drake said the program reminded him of "East Germany and other dystopian regimes in history, especially in the 20th century."[256]

In addition to implementing Insider Threat, the government has taken steps to address previous leaks. Director of National Intelligence James Clapper requested the Inspector General for the Intelligence Community to investigate leak cases that had not been prosecuted to determine if any administrative actions should be taken.[257] According to a 2012 report by the IG, 375 investigations into leaks were underway.[258] Then, in March 2014, Clapper issued Intelligence Community Directive 119, which requires intelligence community employees to "obtain authorization for contacts with the media," including when talking about unclassified information.[259] This Directive could have a significant chilling effect.[260] It is this chilling effect, amplified by numerous Espionage Act prosecutions, that presents such a formidable problem for whistleblowers and leakers as a whole.

CONCLUSION

As his second term comes to a close, President Obama can fulfill his campaign promise of protecting whistleblowers and demonstrate his commitment to freedom of expression by implementing stronger protections against retaliation for whistleblowers and ceasing to bring Espionage Act charges against leakers. Doing so would also support the values he espoused in a 2011 speech in which he said, "we must support those basic rights to speak your mind and access information.... In the 21st Century, information is power; the truth cannot be hidden; and the legitimacy of governments will ultimately depend on active and informed citizens."[261] But if the administration continues to prosecute those who expose the truth while failing to provide them with adequate mechanisms to raise their concerns internally or to challenge retaliatory action take against them, its legitimacy—and legacy—will likely be tarnished.

RECOMMENDATIONS

This section summarizes key recommendations for reforms to the legal and procedural framework to strengthen protections for free speech, press freedom, and the free flow of information, while protecting the government's legitimate interest in discouraging unnecessary leaks of classified information that are truly damaging to national security.

Recommendations for Congress

- Establish strong, clear whistleblower protections for all intelligence community workers, including contractors. These should include judicial remedies, including an express cause of action and appropriate relief, to challenge alleged retaliation as well as penalties for retaliation against legitimate whistleblowers.

- Reform the Espionage Act to allow defendants to raise a public interest defense.

- Enact a federal shield law to protect all individuals engaged in journalism from being compelled to identify or testify against confidential sources.

Recommendations for the Executive Branch

- Establish an independent expert commission to examine the issue of intelligence community whistleblower retaliation and create a plan to strengthen and make more consistent the whistleblower protections available to all intelligence community workers.

- Limit Espionage Act prosecutions to cases in which the disclosure of the information is specifically intended to aid a foreign government or to harm the U.S. national defense.

- Strengthen the intelligence community's Inspectors General by:

    - Filling existing Inspector General vacancies;
    - Ensuring that all agencies comply with records requests from Inspectors General; and
    - Ensuring the independence of Inspectors General by placing clear limits on how they can be removed or fired.

- Implement measures to protect whistleblowers from retaliation, including:

    - Educating and training employees and contractors on the rights and remedies available to whistleblowers;
    - Creating materials that clearly and simply advise each category of potential whistleblower of the avenues available to them to raise concerns and the applicable protections;
    - Maintaining and publicly reporting data regarding the number of intelligence community whistleblower retaliation complaints received annually and how those complaints were resolved; and
    - Holding visibly accountable those responsible for retaliatory actions against whistleblowers, using all available legal remedies.

- Incentivize declassification by providing more resources and technology to assist declassification efforts.

- Strictly limit the FBI's practice of issuing national security letters to obtain journalists' call records to cases of extreme urgency that are subject to direct authorization from the Attorney General.

ACKNOWLEDGMENTS

This report was researched and co-authored by Shelley Walden, consultant and former international program officer for the Government Accountability Project. The report was edited by Katy Glenn Bass, Deputy Director of Free Expression Programs at PEN American Center. Report design was done by Suzanne Pettypiece. PEN thanks the civil society representatives, lawyers, whistleblowers and leakers, scholars, government representatives and journalists interviewed for this report. PEN extends special thanks to Professor Stephen Vladeck of American University Washington College of Law for reviewing an early draft of the report, as well as Anna Shwedel and Alex Weaver for research assistance. PEN is deeply grateful for the support of the Fritt Ord Foundation and the Sy Syms Foundation, without which this project would not have been possible.

ENDNOTES

1 ACLU v. Clapper, No. 14-42 (2d Cir. 2015); USA Freedom Act (Public Law 114-23); U.N. General Assembly, The Right to Privacy in the Digital Age, U.N. Doc A/RES/68/167 (Dec. 18, 2013).

2 Peter Finn and Sari Horwitz, *U.S. Charges Snowden with Espionage*, Wash. Post (June 21, 2013), *available at* https://www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1-11e2-a016-92547bf094cc_story.html.

3 Andrea Peterson, *Is the Obama Administration softening on Edward Snowden?*, Wash. Post (Jul. 7, 2015), *available at* https://www.washingtonpost.com/news/the-switch/wp/2015/07/07/is-the-obama-administration-softening-on-edward-snowden/. Additionally, President Obama's then-White House Press Secretary Jay Carney said that he "should be returned to the United States, where he will be accorded full due process." *Id.*

4 John Cassidy, *Hillary Clinton is Wrong about Edward Snowden*, The New Yorker (Oct. 14, 2015), *available at* http://www.newyorker.com/news/john-cassidy/hillary-clinton-is-wrong-about-edward-snowden.

5 Jonathan Topaz, *Kerry: Snowden a 'Coward…Traitor'*, POLITICO (May 28, 2014), *available at* http://www.politico.com/story/2014/05/edward-snowden-coward-john-kerry-msnbc-interview-nsa-107157.

6 Mike Lillis, *NSA Leaker Snowden Is Lying, Say Leaders of House Intelligence Committee*, The Hill (June 13, 2013), http://thehill.com/homenews/house/305409-house-intel-chiefs-snowden-lying.

7 Joe Davidson, *Obama's Misleading Comment on Whistleblower Protections*, Wash. Post (Aug. 12, 2013), https://www.washingtonpost.com/politics/federal_government/obamas-misleading-comment-on-whistleblower-protections/2013/08/12/eb567e3c-037f-11e3-9259-e2aafe5a5f84_story.html.

8 50 U.S.C. § 3234 (2012).

9 Title VII, Pub. L. No. 105-272, 105th Congress. 2nd Sess. (1998).

10 Peter Lattman, *Barack Obama Was Once a Lowly Law-Firm Associate*, The Wall Street J. L. Blog (Jan. 4, 2008), http://blogs.wsj.com/law/2008/01/04/barack-obama-was-once-a-lowly-law-firm-associate/.

11 Ethics Agenda, The Office of the President-Elect (2008), *available at* http://change.gov/agenda/ethics_agenda/.

12 Macon Phillips, *Change Has Come to WhiteHouse.Gov*, The White House (Jan. 20, 2009), https://www.whitehouse.gov/blog/2009/01/20/change-has-come-whitehousegov.

13 5 U.S.C. § 2302(a)(2)(C)(ii) (2012).

14 *Jailed for Speaking to the Press: How the Obama Admin Ruined Life of State Department Expert Stephen Kim*, Democracy Now (Feb. 18, 2015), *available at* http://www.democracynow.org/2015/2/18/jailed_for_speaking_to_the_press.

15 Leonard Downie Jr., *The Obama Administration and the Press: Leak Investigations and Surveillance in Post-9/11 America*, Committee to Protect Journalists (Oct. 10, 2013), *available at* https://cpj.org/reports/us2013-english.pdf.

16 Daniel Ellsberg, *Lying About Vietnam*, N.Y. Times (June 29, 2001), *available at* http://www.nytimes.com/2001/06/29/opinion/lying-about-vietnam.html; *The Most Dangerous Man in America: Daniel Ellsberg and the Pentagon Papers*, PBS (Oct. 5, 2010), available at http://www.pbs.org/pov/mostdangerousman/photo_gallery_background.php?photo=4#.VhClR-RNViko.

17 David E. Pozen, *The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information*, 127 Harv. L. Rev. 528-529 (2013).

18 *Id.*

19 United States District Court for the Eastern District of Virginia Case No. 1:08dm61—LMB In Re: Grand Jury Subpoena, James Risen, Declaration of Dana Priest, http://sblog.s3.amazonaws.com/wp-content/uploads/2014/03/13-1009-petition-RISEN-v-USA-PETITION-FOR-A-WRIT-OF-CERTIORARI.pdf, 274a, 275a.

20 The Fourteenth Amendment's due process clause extends constitutional protection of press freedom to actions taken by state and local governments. Near v. Minn., 283 U.S. 697, 51 S.Ct. 625 (1931).

21 International Covenant on Civil & Political Rights [hereinafter ICCPR], art. 19 (Dec. 19, 1966) [hereinafter Art. 19]; *see also* Construction and Application of ICCPR, 11 A.L.R. Fed. 2d 751 (detailing ICCPR's limited implementation in the United States).

22 Freedom of Information Act (FOIA), 5 U.S.C. § 552.

23 Office of the White House Press Secretary, Statement by the President Upon Signing S. 1160 (Jul. 4, 1966), available at http://nsarchive.gwu.edu/nsa/foia/FOIARelease66.pdf.

24 Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555 (1980).

25 *Id.* at 538.

26 Detroit Free Press v. Ashcroft, 303 F.3d 681, 683 (6th Cir. 2002) *holding*, among other things, that there is a First Amendment right of access to deportation proceedings. *But see* North Jersey Media Group, Inc. v. Ashcroft, 308 F.3d 198, 219-21 (3d Cir. 2002) (holding that there was no right of access to deportation proceedings).

27 *Id.* at art. 19; U.N. Human Rights Comm., General Comment No. 34, Article 19: Freedoms of Opinion and Expression ¶¶ 11-12, U.N. Doc. CCPR/C/GC/34 (Sept. 12, 2011) [hereinafter General Comment No. 34], http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

28 General Comment No. 34 at ¶ 11.

29 ICCPR at ¶ 18.

30 Resolution 59(1), Calling of an International Conference on Freedom of Information, (Dec. 14, 1946); UDHR, Art. 19.

31 CEDAW, The Council of Europe, the Organization of American States, the Arab Charter, the Association of Southeast Asian Nations, and the African Union have all acknowledged the right of access to information, to varying extents. In 2008, the Council of Europe acknowledged a right to access documents held by government institutions in certain select terms. Additionally, the European Convention on Human Rights allows for access to court documents through Article 40 of the convention.

32 Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Rep. of the Special Rapporteur to the General Assembly on the Protection of Sources and Whistleblowers, ¶ 26, U.N. Doc. A/70/361 (September 8, 2015), available at http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/361; *see also* Joint Declaration on Surveillance Programs and Their Impact on Freedom of Expression by the United Nations Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression and Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights (June 13, 2013) available at: http://www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1.

33 U.N. Convention Against Corruption, art. 10, 13, 33 (2005), *available at* https://www.unodc.org/documents/brussels/UN_Convention_Against_Corruption.pdf.

34 The Global Principles on National Security and the Right to Information (Tshwane Principles), 12 June 2013 published by Open Society Foundation, available at: https://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf. *See also* the work of the NGO Article 19 on this issue, including the Johannesburg Principles on National Security, Freedom of Expression and Access to Information, Article 19 (November 1996), available at: https://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf; The Public's Right to Know: Principles of Information Legislation, Article 19 (June 1999), available at: https://www.article19.org/data/files/pdfs/standards/righttoknow.pdf; The Camden Principles on Freedom of Expression and Equality, Article 19 (April 2009), available at: https://www.article19.org/data/files/pdfs/standards/the-camden-principles-on-freedom-of-expression-and-equality.pdf.

35 Lovell v. City of Griffin, 303 U.S. 444, 452 (1938).

36 U.N. Human Rights Comm., General Comment No. 34, Article 19: Freedoms of Opinion and Expression ¶ 44, U.N. Doc. CCPR/C/GC/34 (Sept. 12, 2011) [hereinafter General Comment No. 34], available at http://www2.ohchr.org/english/bodies/hrc/docs/GC34.pdf (noting, in addition, that any accreditation schemes to enable privileged access must be applied in a non-discriminatory manner, based on objective criteria, and "taking into account that journalism is a function shared by a wide range of actors."); see also Special Rapporteur on the Situation of Human Rights Defenders, Fourth Rep. on the Situation of Human Rights Defenders ¶ 122, U.N. Doc. A/HRC/19/55 (December 21, 2011), available at http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session19/A-HRC-19-55_en.pdf (stating that the "protection of journalists and media workers active on human rights issues should not be limited to those formally recognized as such, but should include other relevant actors, such as community media workers, bloggers and those monitoring demonstrations.")

37 New York Times Co. v. Sullivan (explaining that the freedom of expression upon public questions is long secured by the First Amendment), The government must prove a heavy burden when justifying a press restraint to suppress information. New York Times Co v. Us, 403 U.S. 713, 713 (1971), citing Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 70, 83 S.Ct. 631, 639, 9 L.Ed.2d 584 (1963); see also Near v. Minnesota ex rel. Olson, 283 U.S. 697, 51 S.Ct. 625, 75 L.Ed. 1357 (1931).

38 Scott Neuman, Pentagon Papers Leaker Daniel Ellsberg Praises Snowden, Manning, NPR (Aug. 3, 2013), http://www.npr.org/sections/thetwo-way/2013/08/03/208602113/pentagon-papers-leaker-daniel-ellsberg-praises-snowden-manning; Elizabeth Chuck, Pentagon Papers Whistleblower: Snowden Won't Get a Fair Trial, NBC News (May 30, 2014), http://www.nbcnews.com/feature/edward-snowden-interview/pentagon-papers-whistleblower-snowden-wont-get-fair-trial-n118561.

39 New York Times Co. v. U.S., 403 U.S. 713, 726 (1971). William E. Lee, *Deep Background: Journalists, Sources, and the Perils of Leaking*, 57 Am. U. L. Rev. 1453 (2008); Meredith Fuchs, *Judging Secrets: The Role Courts Should Play In Preventing Unnecessary Secrecy*, 58 Admin. L. Rev 131 (2015); Jon Swaine, *The Impact of the Pentagon Papers 40 Years On*, The Telegraph (June 13, 2011), http://www.telegraph.co.uk/news/worldnews/northamerica/usa/8573899/The-impact-of-The-Pentagon-Papers-40-years-on.html.

40 Branzburg v. Hayes, 408 U.S. 665 (1972), 681.

41 *Id.* at 707. The Supreme Court reaffirmed this right in Richmond Newspapers v. Virginia, 448 U.S. 555 (1980), 576-78 ("It is not crucial whether we describe this right to attend criminal trials to hear, see, and communicate observations concerning them as a 'right of access,' or a 'right to gather information,'...The explicit, guaranteed rights to speak and to publish concerning what takes place at a trial would lose much meaning if access to observe the trial could, as it was here, be foreclosed arbitrarily.").

42 ICCPR at art. 19 (3) (restrictions on freedom of expression are limited to situations which implicate the rights of others or for the protection of national security, public order, public health, or morals); General Comment No. 34 at ¶ 21.

43 General Comment No. 34 at ¶¶ 27-35.

44 Angela Canterbury, "Advocates Laud President Obama's Signing of Federal Whistleblower Reforms," Project on Government Oversight, Dec. 3, 2012, *available at* http://www.pogo.org/about/press-room/releases/2012/20121203-advocates-laud-president-whistleblower-reforms.html?referrer=https://www.google.com/.

45 John Cassidy, Hillary Clinton is Wrong about Edward Snowden, The New Yorker, (Oct. 14, 2015) available at http://www.newyorker.com/news/john-cassidy/hillary-clinton-is-wrong-about-edward-snowden.

46 Exec. Order No. 12,674, 5 C.F.R. § 2635 (1989).

47 Thomas Devine & Steven Katz, *The National Security Whistleblower's Tightrope: Legal Rights to Government Employees and Contractors*, 86, in Whistleblowers, Leaks and the Media: the First Amendment and National Security (Rosenzweig, McNulty, & Shearer eds., 2015); U.S. Merit Systems Protection Board, Blowing the Whistle 12-13 (Nov. 2011).

48 *Id.* at 90.

49 The Military Whistleblower Protection Act was passed in 1988 and revised in 2013. Under this law, military whistleblowers can have an administrative hearing before the applicable Board of Correction of Military Records. Members of the military can only make disclosures within their chain of command or to Congress or an IG office. Devine & Katz, *supra* note 47, at 93. *See also* Dan Meyer & David Berenbaum, *The WASP's Nest: Intelligence Community Whistleblowing & Source Protection*, 8 J. Nat'l Sec. L. & Pol'y, 36 (2015), *available* at http://jnslp.com/wp-content/uploads/2015/05/The-Wasp's-Nest.pdf; 2015 GAO Report, GAO, *available at* http://www.gao.gov/assets/680/670067.pdf. *See also* Nick Schwellenbach, *Pentagon Watchdogs Rarely Side with Military Whistleblowers*, POGO (Dec. 14, 2014), http://www.pogo.org/our-work/articles/2011/pentagon-watchdogs-rarely-side-with-whistleblowers-20111214.html?referrer=https://www.google.com/

50 Interview with Elizabeth Goitein, Co-Director of the Liberty & National Security Program at the Brennan Center for Justice (July 9, 2015).

51 Interview with Thomas Devine, Legal Director for the Government Accountability Project (GAP), (July 24, 2015).

52 Open Society Foundation, *supra* note 34, at 53.

53 The Office of the President-Elect, *supra* note 11.

54 Devine & Katz, *supra* note 47, at 91.

55 Interview with Jesselyn Radack, head of the Whistleblower and Source Protection Program at ExposeFacts, (July 10, 2015). It should also be noted that if national security whistleblowers were to gain access to court, the Justice Department would potentially invoke the State Secrets doctrine to move to dismiss their cases. Congress should therefore address this issue in any legislative reforms involving court access that it considers.

56 Devine & Katz, *supra* note 47, at 99.

57 S. Rep. No. 113-120, at 402 (2013-2014).

58 Katie Pavlich, *Inspectors General Testify About Lack of Transparency, Stonewalling of Internal Federal Government Investigations*, Townhall.com (Feb. 3, 2015), http://townhall.com/tipsheet/katiepavlich/2015/02/03/inspectors-general-testify-about-lack-of-transparency-stonewalling-of-internal-federal-government-investigations-n1952221.

59 Interview with Stephen Vladeck, Professor of Law at the American University Washington College of Law (July 27, 2015).

60 Alex Abdo, David Cole, George Ellard, Kenneth Wainstein, & Stephen Vladeck, *A New Paradigm of Leaking*, 8 J. Nat'l Sec. L. Pol'y 5, *available at* https://www.justsecurity.org/wp-content/uploads/2015/10/8JNatlSecLPoly5.pdf. Darren Samuelsohn, *NSA Watchdog Talks Snowden*, Politico (Feb. 25, 2014), http://www.politico.com/story/2014/02/nsa-inspector-general-edward-snowden-103949.html; Conor Friedersdorf, *A Key NSA Overseer's Alarming Dismissal of Surveillance Critics*, The Atlantic (Feb. 27, 2014), http://www.theatlantic.com/politics/archive/2014/02/a-key-nsa-overseers-alarming-dismissal-of-surveillance-critics/284090/ .

61 50 U.S.C. § 1801 (2012).

62 Charles Clark, *Senators to Obama: Fill the Inspector General Vacancies*, Gov. Exec. (June 3, 2015), http://www.govexec.com/oversight/2015/06/senators-obama-fill-inspector-general-vacancies/114412/ .

63 *Id*.

64 Marisa Taylor, *Judge Probes Destruction of Evidence in NSA Leak Prosecution*, McClatchy DC (June 2, 2015), http://www.mcclatchydc.com/2015/06/02/268564/judge-probes-destruction-of-evidence.html; Melissa Goodman, Catherine Crump, & Sara Corris, *Disavowed: The Government's Unchecked Retaliation Against National Security Whistleblowers*, Am. Civ. Liberties Union, 9 (2007), *available at* https://www.aclu.org/files/pdfs/safefree/disavowed_report.pdf.

65 Interview with Thomas Drake, (July 20, 2015).

66 Marisa Taylor, *Rejection of NSA Whistleblower Claim Draws Criticism*, McClatchy DC (Feb. 23, 2015), http://www.mcclatchydc.com/news/nation-world/national/national-security/article24780436.html.

67 *Sharp Criticism Follows Rejection of NSA Whistleblower's Retaliation Claim*, GAP (Feb. 24, 2015), http://whistleblower.org/press/sharp-criticim-follows-rejection-nsa-whistleblower%E2%80%99s-retaliation-claim.

68 Marisa Taylor, *upra* note 66.

69 *Sharp Criticism Follows Rejection of NSA Whistleblower's Retaliation Claim*, Government Accountability Project (Feb. 24, 2015), *available at* http://www.commondreams.org/newswire/2015/02/24/sharp-criticism-follows-rejection-nsa-whistleblowers-retaliation-claim.

70 Devine & Katz, *supra* note 47, at 103.

71 Scott Horton, *Traitor: Six Questions for Jesselyn Radack*, Harper's Mag. (June 1, 2012), *available at* http://harpers.org/blog/2012/06/_traitor_-six-questions-for-jesselyn-radack/.

72 Interview with Jesselyn Radack, *supra* note 55.

73 *Semiannual Report to the Congress October 1, 2014 to March 31, 2015*, Inspector General U.S. Department of Defense, 34; VI; 41, *available at* http://www.dodig.mil/pubs/sar/SAR_Mar_2015_Book.pdf.

74 Interview with Thomas Devine, *supra* note 51.

75 5 USC § 2302(b)(8) (2012).

76 Open Society Foundation, *supra* note 34, at 51

77 Kevin Casey, *Till Death Do Us Part: Prepublication Review in the Intelligence Community*, 115 Colum. L. Rev. 417, 431-432; 444 (2015), *available at* http://columbialawreview.org/till-death-do-us-part-prepublication-review-in-the-intelligence-community/.

78 Interview with Stephen Kohn, Executive Director of the National Whistleblowers Center (July 16, 2015).

79 Robert Litt, *Keynote Remarks as Prepared for Delivery: Mr. Robert S. Litt, General Counsel, ODNI*, Office of the Director of National Intelligence, Public Affairs Office 2, 8 (Mar. 18, 2014), *available at* http://www.dni.gov/index.php/newsroom/speeches-and-interviews/202-speeches-interviews-2014/1031-as-prepared-for-delivery-remarks-of-odni-general-counsel-robert-litt-at-american-university-washington-college-of-law-freedom-of-information-day-celebration?tmpl=-component&format=pdf.

80 Andrew Croner, *A Snake in the Grass?: Section 798 of the Espionage Act and Its Constitutionality as Applied to the Press*, 77 Geo. Wash. L. Rev. 791 (2012). The Congressional Commission on Protecting and Reducing Government Secrecy (Moynihan Commission), for example, examined the overclassification problem in the 1990s and made a number of recommendations for fixing the system. Among other things, the Committee found that "The classification and personnel security systems are no

longer trusted by many inside and outside the Government. It is now almost routine for American officials of unquestioned loyalty to reveal classified information as part of ongoing policy disputes--with one camp "leaking" information in support of a particular view, or to the detriment of another--or in support of settled administration policy. In the process, this degrades public service by giving a huge advantage to the least scrupulous players. The best way to ensure that secrecy is respected, and that the most important secrets remain secret, is for secrecy to be returned to its limited but necessary role." *See* Senate Document 105-2, Report of the Commission on Protecting and Reducing Government Secrecy, Summary of Findings and Recommendations, FAS 6 (1997), http://www.fas.org:8080/sgp/library/moynihan/sum.html. Similarly, the Public Interest Declassification (PID) board, an advisory committee established by Congress to promote public access to national security information, found in a 2012 report that "Present practices for classification and declassification of national security information are outmoded, unsustainable, and keep too much information from the public." Report to the President: Transforming the Security Classification System, Public Interest Declassification Board 1 (November 2012), https://www.archives.gov/declassification/pidb/recommendations/transforming-classification.pdf.

81 Many of the classified documents that Manning released outline mundane correspondence, such as a description of a wedding in Dagestan. R. Kyle Alagood, *Manning and Snowden: Wakeup Call on Overclassification*, Brennan Center for Justice (Jul. 10, 2013), *available at* https://www.brennancenter.org/analysis/manning-and-snowden-wakeup-call-overclassification. Snowden's document release presents a slightly different problem, of documents and policies that should never have been classified in the first place. Indeed, after Snowden released the documents outlining a secret NSA surveillance program, Director of National Intelligence James Clapper declassified much of the information and material related to the program. Eli Lake, *Spy Chief: We Should've Told You We Track Your Calls*, The Daily Beast (Feb. 17, 2014), http://www.thedailybeast.com/articles/2014/02/17/spy-chief-we-should-ve-told-you-we-track-your-calls.html. Even further, in February 2014, Clapper told The Daily Beast that the agency should have been more transparent about the government-sponsored surveillance program since the beginning. *Id.* As Denver Nicks wrote about Chelsea Manning's disclosures, "The question that went too often unasked in the wake of the War Logs and the leaks that followed was the one that should have troubled us most deeply: why was this information secret? Clearly there was good reason to keep secret *some* of what was included in the logs [Chelsea] Manning leaked. Publicizing the names of Afghan informants may well have put innocent lives at risk. And in the short term, of course, the army requires secrecy in its communications in order to wage war. But taken on the whole, the logs were profoundly, troublingly boring, of interest primarily to journalists and historians … Had the Pentagon revealed most of the information in the logs responsibly, it's difficult to image what 'serious damage to national security' would have resulted, as required for information to be classified at the Secret level." Denver Nicks, Private: Bradley Manning, WikiLeaks, and the Biggest Exposure of Official Secrets in American History 193; 204-205 (2012).

82 Interview with John Fitzpatrick, Director of the Information Security Oversight Office (Aug. 3, 2015)..

83 Exec. Order No. 13,526, 3 C.F.R. (2009), at 1.7 (a)(1) & (2).

84 *See* Senate Document 105-2, Report of the Commission on Protecting and Reducing Government Secrecy, Summary of Findings and Recommendations, FAS 6 (1997), http://www.fas.org:8080/sgp/library/moynihan/sum.html; Report to the President: Transforming the Security Classification System, Public Interest Declassification Board 1 (November 2012), https://www.archives.gov/declassification/pidb/recommendations/transforming-classification.pdf.

85 Interview with John Fitzpatrick, *supra* note 82.

86 *Id*.

87 Interview with Elizabeth Goitein, *supra* note 50.

88 Title VII, Pub. L. No. 105-272, 105th Congress. 2nd Sess. (1998).

89 Interview with Ben Wizner, Attorney for Edward Snowden (July 30, 2015).

90 Interview with Dan Meyer, ICW&SP Executive Director (July 21, 2015).

91 Interview with Elizabeth Goitein, *supra* note 50.

92 About the Intelligence Community Whistleblower Protection Act (ICWPA), Office of the Inspector General, U.S. Dep't of Defense, http://www.dodig.mil/programs/whistleblower/icwpa.html; Intelligence Community Whistleblower Protection Act of 1998, Pub. L. No: 105-272, Title VII (1998).

93 Interview with John Kiriakou, (Aug. 4, 2015).

94 Mike German & Jay Stanley, *Drastic Measures Required*, Am. Civ. Liberties Union 10 (2011) https://www.aclu.org/files/assets/secrecyreport_20110727.pdf.

95 Interview with Michael German, Brennan Center for Justice (July 23, 2015).

96 Letter to Steven Aftergood, Office of the Director of National Intelligence (Mar. 18, 2014), *available at* http://fas.org/irp/dni/icig/icwpa-use.pdf.

97 Siobhan Gorman, *System Error*; The Baltimore Sun, (Jan. 29, 2006), *available at* http://articles.baltimoresun.com/2006-01-29/news/0601280286_1_intelligence-experts-11-intelligence-trailblazer.

98 Jesselyn Radack & Kathleen McClellan, *The Criminalization of Whistleblowing*, 2 Labor & Employment L. Forum 60 (2011), *available at* http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1034&context=lelb.

99 Government Accountability Project, *Bio: William Binney and J. Kirk Wiebe*, 2015, *available at* http://whistleblower.org/bio-william-binney-and-j-kirk-wiebe; Yochai Benkler, *A Public Accountability Defense for National Security Leakers and Whistleblowers*, 8(2) Harv. Rev. L. & Policy, 314-15 (2014), *available at* http://dash.harvard.edu/bitstream/handle/1/12786017/Benkler.pdf?sequence=3.

100 Interview with William Binney, NSA Whistleblower (July 19, 2015).

101 *Id.*; *see also* William Binney, *United States of Secrets: William Binney*, Frontline (Dec.13, 2013), *available at* http://www.pbs.org/wgbh/pages/frontline/government-elections-politics/united-states-of-secrets/the-frontline-interview-william-binney/

102 Peter Eisler & Susan Page, *3 NSA Veterans Speak Out on Whistle-blower: We Told You So*, USA Today (June 16, 2013), *available at* http://www.usatoday.com/story/news/politics/2013/06/16/snowden-whistleblower-nsa-officials-roundtable/2428809/; Interview with Jesselyn Radack, *supra* note 55.

103 Email from William Binney (Aug. 18, 2015) (on file with PEN).

104 Daniel D'Isidoro, *Protecting Whistleblowers and Secrets in the Intelligence Community*, Harv. Nat. Security J. Online (2014), *available at* http://harvardnsj.org/2014/09/protecting-whistleblowers-and-secrets-in-the-intelligence-community/.

105 P.L.110-181, Sec. 846; 10 U.S.C. § 2409 (2012).

106 Interview with Thomas Devine, *supra* note 51; *Organizations Call on Congress to Restore Whistleblower Rights*, POGO (Oct. 20, 2014), http://www.pogo.org/about/press-room/releases/2014/49-organizations-call-on-congress-to-restore-whistleblower-rights.html.

107 P.L. 112-239, Sec. 827; 10 U.S.C. § 2409 (2012).

108 Sarah Damian, *49 Orgs Call on Congress to Restore Whistleblower Rights to Intelligence Contractors*, Government Accountability Project (Oct. 30, 2014), *available at* http://whistleblower.org/blog/121230-49-orgs-call-congress-restore-whistleblower-rights-intelligence-contractors.

109 Interview with Thomas Devine; Jamie LaPlante, Stimulus Bill Contains Whistleblower Protections for Employees of State & Local Governments and Private Employers Who Receive Stimulus Funds, Employer Law Report (Feb. 25, 2009), http://www.employerlawreport.com/2009/02/articles/traps-for-the-unwary/stimulus-bill-contains-whistleblower-protections-for-employees-of-state-local-governments-and-private-employers-who-receive-stimulus-funds/.

110 Dana Priest & William Arkin, *National Security, Inc.*, Wash. Post, *available at* http://projects.washingtonpost.com/top-secret-america/articles/national-security-inc/.

111 Interview with Mandy Smithberger & Liz Hempowicz, Project on Government Oversight (POGO) (July 8, 2015).

112 Arden Arnold, *Does New Policy Protect Intelligence Whistleblowers*, Project on Government Oversight (July 10, 2013), *available at* http://www.pogo.org/blog/2013/07/20130710-does-new-policy-protect-intelligence-whistleblowers.html.

113 Interview with Thomas Devine, *supra* note 51.

114 The order doesn't protect FBI employees or members of the Armed Forces from any form of non-security clearance related reprisal, as they have separate statutory protections under 5 U.S.C. § 2303 and 10 U.S.C. § 1034. FBI whistleblowers have equivalent rights to civil service employees, except that the DOJ Office of Attorney Management and Recruitment conducts FBI whistleblower hearings, whereas whistleblowers protected under the WPEA can have their cases reviewed by the U.S. Merit Systems Protection Board and also have recourse to jury trials in federal district court. The Military Whistleblower Protection Act was passed in 1988 and revised in 2013. Under this law, military whistleblowers can have an administrative hearing before the applicable Board of Correction of Military Records. Members of the military can only make disclosures within their chain of command or to Congress or an IG office. Devine & Katz, *supra* note 47, at 93. *See also* Dan Meyer & David Berenbaum, *The WASP's Nest: Intelligence Community Whistleblowing & Source Protection*, 8 J. Nat'l Sec. L. & Pol'y, 36 (2015), *available* at http://jnslp.com/wp-content/uploads/2015/05/The-Wasp's-Nest.pdf.

115 Joe Davidson, *Obama Issues Whistleblower Directive to Security Agencies*, Wash. Post (Oct. 11, 2012), *available at* http://www.washingtonpost.com/blogs/federal-eye/post/obama-issues-whistleblower-directive-to-security-agencies/2012/10/10/5e2cbbfe-132d-11e2-ba83-a7a396e6b2a7_blog.html.

116 Interview with Jesselyn Radack, *supra* note 55.

117 Presidential Policy Directive PPD-19, Oct. 10, 2012.

118 Interview with Thomas Devine, *supra* note 51.

119 Government Accountability Project, Take Action to Protect Whistleblowers 2015, *available at* http://whistleblower.org/takeaction.

120 Joe Davidson, *Obama's 'Misleading' Comments on Whistleblower Protections*, Wash. Post (Aug. 12, 2013), *available at* http://www.washingtonpost.com/politics/federal_government/obamas-misleading-comment-on-whistleblower-protections/2013/08/12/eb567e3c-037f-11e3-9259-e2aafe5a5f84_story.html.

121 Pieter Omtzigt, *Improving the Protection of Whistle-blowers*, Parliamentary Assembly of the Council of Europe, Doc. 13791 5 (May 19, 2015) *available at* http://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?-FileID=21651&lang=en.

122 Interview with Michael German, *supra* note 95.

123 Meyer & Berenbaum, *supra* note 114, at 28.

124 Interview with a House Permanent Select Committee on Intelligence Staff Member (requesting anonymity).

125 Interview with Dan Meyer, *supra* note 90.

126 Email from Andrea Williams, Public Affairs Officer, IC IG (Aug. 28, 2015) (on file with PEN); Meyer & Berenbaum, *supra* note 114, at 1.

127 Interview with Thomas Devine, *supra* note 51.

128 Meyer & Berenbaum, *supra* note 114, at 7.

129 *Id*. at 9.

130 Interview with Dan Meyer, *supra* note 90.

131 However, when PEN spoke with the executive director for ICW&SP, he noted that staffing may be more of a problem for the Inspector General's Offices that are earlier in the process, such as the DOD IG, than for his office.

132 Interview with Thomas Devine, *supra* note 51.

133 Rodney M. Perry, *Intelligence Whistleblower Protections: In Brief*, Congressional Research Service 7 (Oct. 23, 2014), *available at* http://www.fas.org/sgp/crs/intel/R43765.pdf.

134 P.L. 113-126 Title VI. 50 USC 3234 sec 601 (b).

135 *Id*.

136 Mary Jane Wilmoth, *Intelligence Whistleblowers Should Use 'Expanded Protections' With Caution*, The Whistleblower Blog, Kohn, Kohn & Colapinto, July 9, 2014, *available at* http://www.whistleblowersblog.com/2014/07/intelligence-whistleblowers-use-expanded-protections-caution/.

137 P.L. 113-126 Title VI. 50 USC 3234; Perry, *supra* note 133, at 7-8.

138 Perry, *supra* note 133, at 7.

139 Wilmoth, *supra* note 136.

140 Meyer & Berenbaum, *supra* note 114, at 37

141 Interview with Dan Meyer, ICW&SP Executive Director (July 21, 2015).

142 Radack & McClellan, *supra* note 98, at 76-77.

143 Interview with Stephen Vladeck, Professor of Law at the American University Washington College of Law (July 27, 2015).

144 Stephen I. Vladeck, *Prosecuting Leaks under U.S. Law*, 30, in Whistleblowers, Leaks and the Media: the First Amendment and National Security (Rosenzweig, McNulty, & Shearer eds., 2015).

145 Interview with Kathleen Clark, Professor of Law at Washington University (July 29, 2015).

146 Affidavit in Support of Application for Search Warrant in Case No. 1:10-mj-00291-AK available at http://www.nytimes.com/interactive/2013/05/25/us/politics/james-rosen-affidavit.html?_r=0.

147 Interview with Denver Nicks, Biographer of Chelsea Manning (August 19, 2015).

148 Vladeck, *supra* note 144, at 31-32; David E. Pozen, *The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information*, 127 Harv. L. Rev. 535, 554 (2013), *available at* http://cdn.harvardlawreview.org/wp-content/uploads/pdfs/vol127_pozen.pdf.

149 18 USC § 793 (d) (e); Pamela Takefman, *Curbing Overzealous Prosecution of the Espionage Act: Thomas Andrews Drake and the Case for Judicial Intervention at Sentencing*, 35 Cardozo L. Rev. 897, 902 (2013), *available at* http://www.cardozolawreview.com/content/35-2/TAKEFMAN.35.2.pdf,.

150 Jesselyn Radack, *Why Edward Snowden Wouldn't Get a Fair Trial*, Wall Street J. (Jan. 21, 2014), *available at* http://www.wsj.com/articles/SB10001424052702303595404579318884005698684.

151 Comment from Stephen Vladeck to PEN (Oct. 23, 2015).

152 Gene Policinski, *First Amendment Considerations on National Security Issues: From Zenger to Snowden*, 68, in Whistleblowers, Leaks and the Media: the First Amendment and National Security (Rosenzweig, McNulty, & Shearer eds., 2015); Jim Snyder, *The Espionage Act: A Spy-Fighting Tool is Now Aimed at U.S. Leakers*, Bloomberg Quick Take (Oct. 3, 2014), *available at http://www.bloombergview.com/quicktake/the-espionage-act;* Gregg P. Leslie & Emily Grannis, *History of Leaks in the United States from the Pentagon Papers through Wikileaks to Rosen*, 22, in Whistleblowers, Leaks and the Media: the First Amendment and National Security (Rosenzweig, McNulty, & Shearer eds., 2015).

153 Steven Aftergood, *FBI Found 14 Intel Leak Suspects in Past 5 Years*, Federation of American Scientists: Secrecy News (June 21, 2010), *available at* http://fas.org/blogs/secrecy/2010/06/intel_leak/.

154 Jesselyn Radack & Kathleen McClellan. *The Criminalization of Whistleblowing*, 2 Labor & Employment Law Forum 60 (2011), *available at* http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1034&context=lelb.

155 Jamie Tarabay, *Obama and Leakers; Who Are the Eight Charged Under the Espionage Act?*, Al Jazeera America (Dec. 5, 2013), *available at* http://america.aljazeera.com/articles/2013/12/5/obama-and-leakerswhoaretheeightchargedunderespionageact.html; Charlie Savage, *Former F.B.I Agent to Plead Guilty in Press Leak*, N.Y. Times (Sept. 23, 2013), *available at* http://www.nytimes.com/2013/09/24/us/fbi-ex-agent-pleads-guilty-in-leak-to-ap.html

156 Takefman, *supra* note 149, at 904-905 (2013), *available at* http://www.cardozolawreview.com/content/35-2/TAKEFMAN.35.2.pdf.

157 Leonard Downie Jr., *The Obama Administration and the Press: Leak Investigations and Surveillance in Post-9/11 America*, Committee to Protect Journalists (Oct. 10, 2013), available at https://cpj.org/reports/us2013-english.pdf. In a statement released by Stephen Jin-Woo Kim's lawyer, Abbe D. Lowell, Kim said he released the report in an effort to warn the American public about North Korea's nuclear threats. This was approximately three years after North Korea conducted its first nuclear test in October 2006, and on the heels of then-leader Kim Jong-il's declining health. Ann Marimow, Ex-State Department Adviser Stephen J. Kim Sentenced to 13 Months in Leak Case, Wash. Post (Apr. 2, 2014), https://www.washingtonpost.com/world/national-security/ex-state-dept-adviser-stephen-j-kim-sentenced-to-13-months-in-leak-case/2014/04/02/f877be54-b9dd-11e3-96ae-f2c36d2b1245_story.html; Choe Sang-hun, North Korea Claims to Conduct 2nd Nuclear Test, N.Y. Times (May 24, 2009), http://www.nytimes.com/2009/05/25/world/asia/25nuke.html.

158 Leonard Downie Jr., *The Obama Administration and the Press: Leak Investigations and Surveillance in Post-9/11 America*, Committee to Protect Journalists (Oct. 10, 2013), *available at* https://cpj.org/reports/us2013-english.pdf.

159 Yochai Benkler, *A Public Accountability Defense for National Security Leakers and Whistleblowers*, 8 Harv. Rev. L. & Policy 282-284 (2014), *available at* http://dash.harvard.edu/bitstream/handle/1/12786017/Benkler.pdf?sequence=3.

160 *Id*. at 284; 303.

161 Interviews with Abbe Lowell, Head of Litigation at Chadbourne and Attorney for Stephen Kim (August 25, 2015); Mike German; Mandy Smithberger & Liz Hempowicz; Stephen Vladeck; Edward MacMahon, Attorney (July 27, 2015).

162 The Associated Press, *Kerry to Snowden; 'Man Up' and Come Home*, San Jose Mercury News (May 28, 2014), *available at* http://www.mercurynews.com/politics-government/ci_25849262/kerry-tells-snowden-man-up-and-come-home.

163 Daniel Ellsberg, *Daniel Ellsberg: Snowden Would Not Get a Fair Trial—and Kerry is Wrong*, The Guardian (May 30, 2014), *available at* http://www.theguardian.com/commentisfree/2014/may/30/daniel-ellsberg-snowden-fair-trial-kerry-espionage-act.

164 Trevor Timm, *If Snowden Returned to US for Trial, All Whistleblower Evidence Would Likely Be Inadmissible*, Freedom of the Press Foundation (Dec. 23, 2013), *available at* https://freedom.press/blog/2013/12/if-snowden-returned-us-trial-all-whistleblower-evidence-would-likely-be-inadmissible; Brennan Center for Justice, *National Security Whistleblowing: A Gap in the Law*, *available at* http://www.brennancenter.org/sites/default/files/analysis/Factsheet%20-%20National%20Security%20Whistleblowing.pdf; Jesselyn Radack, *Why Edward Snowden Wouldn't Get a Fair Trial*, Wall Street J. (Jan. 21, 2014), *available at* http://www.wsj.com/articles/SB10001424052702303595404579318884005698684.

165 Vladeck, *supra* note 144, at 34-35.

166 Ellsberg, *supra* note 163.

167 Interview with Trevor Timm, Freedom of the Press Foundation (Aug. 4, 2015).

168 Interview with Mandy Smithberger & Liz Hempowicz, Project on Government Oversight (POGO) (July 8, 2015).

169 Marcy Wheeler, *Government Tries to Convict Jeffrey Sterling for Retroactively Classified Documents about Rotary Phones*, ExposeFacts (Jan. 21, 2015), https://exposefacts.org/government-tries-to-convict-jeffrey-sterling-for-retroactively-classified-documents-about-rotary-phones/; Jesselyn Radack, *The New Yorker's Damning Dissection of "Leak" Prosecution of Thomas Drake*, GAP (May 15, 2011), http://whistleblower.org/blog/120016-new-yorkers-damning-dissection-leak-prosecution-thomas-drake; Marcy Wheeler, *In Political Press, Hillary Clinton Gets Subjected to the Thomas Drake and Jeffrey Sterling Standard*, ExposeFacts (July 24, 2015), *available at* https://exposefacts.org/in-political-press-hillary-clinton-gets-subjected-to-the-thomas-drake-and-jeffrey-sterling-standard/.

170 United States v. Morison, 844 F.2d 1065, 1081-83 (4th Cir. 1988).

171 18 U.S.C. § 793 (f).

172 Timm, *supra* note 164.

173 Radack, *supra* note 150.

174 Interview with Thomas Drake, *supra* note 65.

175 Interview with Shamai Leibowitz, (Aug. 11, 2015).

176 Vladeck, *supra* note 144, at 34.

177 Gregg P. Leslie & Emily Grannis, *History of Leaks in the United States from the Pentagon Papers through Wikileaks to Rosen*, 22, in Whistleblowers, Leaks and the Media: the First Amendment and National Security (Rosenzweig, McNulty, & Shearer eds., 2015).

178 Pozen, *supra* note 148, at 535, note 117.

179 Bruce Methven, *First Amendment Standards for Subsequent Punishment of Dissemination of Confidential Government Information*, 68 Cal. L. Rev. 84 (1980), *available at* http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2299&context=californialawreview.

180 Pozen, *supra* note 148, at 516.

181 Radack & McClellan, *supra* note 154, at 68.

182 Robert Mahoney, *Greenwald Wants to Return to US, But Not Yet*, Committee to Protect Journalists (Oct. 15, 2013), *available at* https://cpj.org/blog/2013/10/greenwald-wants-to-return-to-us-but-not-yet.php.

183 Affidavit in Support of Application for Search Warrant in Case No. 1:10-mj-00291-AK available at http://www.nytimes.com/interactive/2013/05/25/us/politics/james-rosen-affidavit.html?_r=0.

184 Paul Rosenzweig, et al., *The Fundamental Tension: An Introduction*, 6, in Whistleblowers, Leaks and the Media: the First Amendment and National Security (Rosenzweig, McNulty, & Shearer eds., 2015); Leslie & Grannis, *supra* note 177.

185 Interview with Abbe Lowell, Head of Litigation at Chadbourne and Attorney for Stephen Kim (August 25, 2015). *See also Jeffrey Sterling Convicted For New York Times Leak*, Reuters (May 11, 2015), *available at* http://www.huffingtonpost.com/2015/05/11/jeffrey-sterling-convicted_n_7260836.html.

186 David Franke, *Journalists Just Agreed: 'Obama is by Far the Worst,' In this Important Area*, Western Journalism (June 5, 2015), *available at* http://www.westernjournalism.com/jailbird-journalists-gather-at-press-club/.

187 Matt Apuzzo, *Times Reporter Will Not be Called to Testify in Leak Case: Legal Fight Ends for James Risen of the New York Times*, N.Y. Times (Jan. 12, 2015), *available at* http://www.nytimes.com/2015/01/13/us/times-reporter-james-risen-will-not-be-called-to-testify-in-leak-case-lawyers-say.html?_r=0.

188 U.S. v. Sterling, 724 F.3d 482 (4th Cir. 2013).

189 Leslie & Grannis, *supra* note 177, at 24.

190 Zachary Roth, *Holder: I Won't Send Journalists to Jail for Doing Their Job*, MSNBC (Oct. 14, 2014), http://www.msnbc.com/msnbc/holder-i-wont-send-journalists-jail-doing-their-job; *Lynch: No Reporter Will Go to Jail for Doing His or Her Job*, U.S. News (Oct. 9, 2015), http://www.usnews.com/news/politics/articles/2015/10/09/lynch-no-reporter-will-go-to-jail-for-doing-his-or-her-job.

191 *Amending the Department of Justice Subpoena Guidelines*, Reporters Committee for Freedom of the Press, *available at* http://www.rcfp.org/attorney-general-guidelines; Department of Justice Policy Regarding Obtaining Information From, or Records of, Members of the News Media; and Regarding Questioning, Arresting, or Charging Members of the News Media, 28 C.F.R. § 50; 59 (Feb. 21, 2014), *available at* https://www.documentcloud.org/documents/1020977-final-rule-28-cfr-50-10-ag-order.html.

192 Solomon & Wheeler, *infra* note 195; Timm, *infra* note 197.

193 Matt Apuzzo, *Defiant on Witness Stand, Times Reporter Says Little*, N.Y. Times (Jan. 5, 2015), *available at* http://www.nytimes.com/2015/01/06/us/james-risen-in-tense-testimony-refuses-to-offer-clues-on-sources.html.

194 Kimberly Chow, *Revising the Attorney General's Guidelines*, Reporters Committee for Freedom of the Press, 2015, *available at* http://www.rcfp.org/browse-media-law-resources/news-media-law/news-media-and-law-winter-2015/revising-attorney-generals-; Apuzzo, *supra* note 187; Matt Zapotosky, *Ex-CIA Officer convicted in leak case sentenced to 3 ½ years in prison*, The Washington Post (May 11, 2015) available at https://www.washingtonpost.com/local/crime/ex-cia-officer-convicted-in-leak-case-sentenced-to-3-12-years-in-prison/2015/05/11/fc5427a6-f5a0-11e4-84a6-6d7c67c50db0_story.html.

195 Norman Solomon & Marcy Wheeler, *The Government War Against Reporter James Risen*, The Nation (Oct. 8, 2014), *available at* http://www.thenation.com/article/government-war-against-reporter-james-risen/; Charlie Savage, *U.S. Subpoenas Times Reporter Over Book on C.I.A.*, N.Y. Times (Apr. 28, 2010), *available at* http://www.nytimes.com/2010/04/29/us/29justice.html.

196 Sophia Cope, *Excessive Government Secrecy is Antithetical to a Free and Democratic Society*, 258, in Whistleblowers, Leaks and the Media: the First Amendment and National Security (Rosenzweig, McNulty, & Shearer eds., 2015).

197 Solomon & Wheeler, *supra* note 195; Trevor Timm, *We Just Sued the Justice Department Over the FBI's Secret Rules for Using National Security Letters on Journalists*, Freedom of the Press Foundation (July 30, 2015), *available at* https://freedom.press/blog/2015/07/we-just-sued-justice-department-over-fbis-secret-rules-using-national-security-letters.

198 Lindy Royce-Bartlett, *Leak Probe Has Chilled Sources, AP Exec Says*, CNN (June 19, 2013), *available at* http://www.cnn.com/2013/06/19/politics/ap-leak-probe/.

199 Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Rep. of the Special Rapporteur to the General Assembly on the Protection of Sources and Whistleblowers, ¶ 23, U.N. Doc. A/70/361 (September 8, 2015), available at http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/361.

200 Senator Charles Schumer has introduced one such proposal in the Senate, but it has not received a vote. Rem Rieder, *Rieder: Shield Law for Journalists a Gridlock Casualty*, USA Today (Sept. 22, 2014), http://www.usatoday.com/story/money/columnist/rieder/2014/09/22/federal-shield-law-for-journalists-doomed-a/16050353/.

201 PEN American Center, Committee to Protect Journalists, Freedom House, and Reporters Committee for Freedom of the Press are all examples of organizations that have called for a federal shield law. House Passes Historic Federal Shield Law: Bill Protects Public's Right to Know, PEN (Oct. 17, 2007), http://www.pen.org/press-release/2007/10/17/house-passes-historic-federal-shield-law-bill-protects-publics-right-know; Sandy Rowe, *CPJ Report Reflects Seriousness of U.S. Press Freedom Gaps*, Committee to Protect Journalists (Oct. 11, 2013), https://cpj.org/blog/2013/10/cpj-report-reflects-seriousness-of-us-press-freedo.php; Karin Deutsch Karlekar, *Set Global Example: Pass US Journalism Shield Law*, Freedom House (Sept 15, 2005), https://freedomhouse.org/article/set-global-example-pass-us-journalism-shield-law. For members of the press who have also supported a shield law, *see* Shield Law 101:Frequently Asked Questions, Soc. Prof. Journalists (accessed Nov. 5, 2015), http://www.spj.org/shieldlaw-faq.asp; Cora Currier, *Pressure, Potential for a Fedeal Shield Law*, Colum. Journalism Rev. (June 13, 2014), http://www.cjr.org/behind_the_news/shield_law_risen_etc.php.

202 Interview with Jesselyn Radack, *supra* note 55.

203 Pozen, *supra* note 148, at 524.

204 *Id*. at 539.

205 *Id.* at 540.

206 Department of Justice Office of Information and Privacy, Letter to Steven Aftergood 14 (Mar. 8, 2007), http://www.fas.org/sgp/othergov/renoleaks.pdf.

207 Center for Constitutional Rights, Call for Submissions on the Protection of Sources and Whistleblowers by the United Nations Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, Written Submission of the Center for Constitutional Rights 10 (June 22, 2015), *available at* https://ccrjustice.org/sites/default/files/attach/2015/06/CCR%20Whistleblower%20Submission%20Final%20(2).pdf.

208 Hearing on the Espionage Statutes: A Look Back and a Look Forward, Statement of Senator Kyl, 111th Congress (2010), *available at* http://fas.org/irp/congress/2010_hr/espionage.html.

209 18 USC § 793 (e).

210 Interview with Stephen Vladeck, *supra* note 59.

211 Center for Constitutional Rights, *supra* note 207.

212 Benjamin Buckland & Aidan Wills, *Blowing in the Wind? Whistleblowing in the Security Sector*, Right2Info 95 (2012), *available at* http://www.right2info.org/resources/publications/pretoria-finalization-meeting-april-2013-documents/whistleblowing-and-security-sector-buckland-and-wills.

213 Open Society Foundation, *supra* note 34, at 55-56.

214 Benkler, *supra* note 159, at 285-6; 306; 310.

215 Interview with U.S. Senate Select Committee on Intelligence Staff Member (requesting anonymity).

216 Vladeck, *supra* note 144, at 38.

217 18 U.S.C. § 1030.

218 U.S. v. Thomas A. Drake (Plea Agreement), U.S. Department of Justice Criminal Division (June 9, 2011), *available at* https://www.fas.org/sgp/jud/drake/plea.pdf.

219 Center for Constitutional Rights, *supra* note 207, at 24.

220 *Id*. at 3, 24-26.

221 Interview with First Amendment and human rights attorney Carey Shenkman, August 14, 2015.

222 18 U.S.C.A. § 641 (2012) (the value of the property determines whether a defendant would be charged with a felony or misdemeanor).

223 Jessica Lutkenhaus, *Prosecuting Leakers the Easy Way: 18 U.S.C. § 641*, 114 Colum. L. Rev. 1167 (2014), http://columbialawreview.org/wp-content/uploads/2014/06/Lutkenhaus-J..pdf.

224 *Id.*

225 *See* U.S. v. Morison, 844 F.2d 1057 (4th Cir. 1988), *but see* U.S. v. Fowler, 932 F.2d 306 (4th Cir. 1991). The Second and Sixth Circuits have declared prosecutions for information under 641 permissible in some circumstances. U.S. v. Jeter, 775 F.2d 670, 680-82 (6th Cir. 1985); U.S. v. Girard, 601 F.2d 69, 70-71 (2d Cir. 1979).

226 Lutkenhaus, *supra* note 223.

227 2057. Synopses of Key National Defense and Security Provisions, Office of the U.S. Attorneys (accessed Nov. 5, 2015), http://www.justice.gov/usam/criminal-resource-manual-2057-synopses-key-national-defense-and-national-security-provisions.

228 1664. Protection of Government Property—Theft of Government Information, Office of the U.S. Attorneys (accessed Nov. 5, 2015), http://www.justice.gov/usam/criminal-resource-manual-1664-protection-government-property-theft-government-information.

229 Douglas Linder, *The Trial of Daniel Ellsberg and Anthony Russo: The Indictment*, Famous Trials (accessed Nov. 5, 2015), http://law2.umkc.edu/faculty/projects/ftrials/ellsberg/indictment.html.

230 Josh Meyer, *How to Avoid Legal Trouble over Sources and Secrets*, Nat'l Sec. Zone (2014), https://assets.documentcloud.org/documents/1238167/meyer-primer-sources-secrets.pdf.

231 U.S. v. Jeffrey Sterling, Indictment in Case No. 1:10CR485 (E.D. Va., 2010), *available at* https://www.fas.org/sgp/jud/sterling/indict.pdf.

232 Jennifer Elsea, *Criminal Prohibitions on the Publication of Classified Defense Information*, Cong. Research Service (Sept. 9, 2013), https://www.fas.org/sgp/crs/secrecy/R41404.pdf.

233 Lawrence Franklin, Shamai Leibowitz, John Kiriakou, James Hitselberger, Donald Sachtleben, Thomas Drake, and Stephen Jin-Woo Kim were all charged with Espionage Act violations, but not with § 641. *See* United States v. Drake, Indictment in Case No. 10-cr-00181-RDB, 2010 WL 1513342, *available at* http://www.justice.gov/opa/pr/former-cia-officer-john-kiriakou-indicted-allegedly-disclosing-classified-information; U.S. v. Hitselberger, Indictment in Case No. 1:12-cr-00231-RC, *available at* http://www.fas.org/sgp/jud/hitsel/indict.pdf; U.S. v. Kim, Indictment in Case No. 1:10-cr-00225-CKK, *available at* https://www.fas.org/sgp/jud/kim/indict.pdf; U.S. v. Sachtleben, Statement of Offense (S.D. Ind.), *available at* http://www.justice.gov/iso/opa/resources/7642013923154527618802.pdf; U.S. v. Leibowitz, Statement of Charges (D. Mar.), *available at* http://fas.org/irp/news/2009/12/skleibowitz-charge.pdf; U.S. v. Franklin, Superseding Indictment (E.D. Va.), *available at* httlap://fas.org/irp/ops/ci/franklin0805.pdf.

234 The Pentagon Papers case against Russo and Ellsberg was dropped due to government misconduct. Martin Arnold, *Pentagon Papers Charges Are Dismissed; Judge Byrne Frees Ellsberg and Russo, Assails 'Improper Government Conduct*, N.Y. Times (May 11, 1973), *available at* http://www.nytimes.com/learning/general/onthisday/big/0511.html.

235 Pozen, *supra* note 148, at 528.

236 *Id.* at 529.

237 Government Accountability Project, *Bio: John Kiriakou*. 2015, available at http://whistleblower.org/bio-john-kiriakou.

238 Id.

239 Id.

240 Id.

241 Id.

242 David H. Petraeus, *Message from the Director: Former Officer Convicted in Leak Case*, Central Intelligence Agency (Oct. 23, 2012), *available at* https://www.cia.gov/news-information/press-releases-statements/2012-press-releasese-statements/statement--former-officer-convicted.html.

243 Evan Perez, *Gen. Petraeus Pleads Guilty to Federal Charge*, CNN Politics (March 3, 2015), *available at* http://www.cnn.com/2015/03/03/politics/general-david-petraeus-guilty-charges/.

244 Government Accountability Project, *Bio: John Kiriakou*.

245 Edward McNicholas, *U.S. Efforts to Change Leak Laws*, 53, in Whistleblowers, Leaks and the Media: the First Amendment and National Security (Rosenzweig, McNulty, & Shearer eds., 2015).

246 Interview with John Kiriakou, *supra* note 93.

247 Interview with Jesselyn Radack, *supra* note 55.

248 Interview with Paul Rosenzweig, Co-Editor of *Whistleblowers, Leaks and the Media* (July 29, 2015).

249 Exec. Order No. 13,587 (2011).

250 Downie, *supra* note 157.

251 Marisa Taylor & Jonathan Landay, *Obama's Crackdown Views Leaks as Aiding Enemies of U.S.*, McClatchy DC (June 20, 2013), *available at* http://www.mcclatchydc.com/news/special-reports/insider-threats/article24750244.html.

252 Exec. Order No. 13,587, § 7(e).

253 Scott Hingham, *Intelligence Security Initiatives Have Chilling Effect on Federal Whistleblowers, Critics Say*, Wash. Post (July 23, 2014), *available at* http://www.washingtonpost.com/world/national-security/intelligence-security-initiatives-have-chilling-effect-on-federal-whistleblowers-critics-say/2014/07/23/c9dfd794-0ea0-11e4-8341-b8072b1e7348_story.html.

254 Interview with Thomas Devine, *supra* note 51.

255 Interview with Steven Aftergood, Federation of American Scientists (July 9, 2015).

256 Interview with Thomas Drake, *supra* note 65.

257 Downie, *supra* note 157.

258 Steven Aftergood, *Hundreds of Classified Leaks Under Review by IC Inspector General*, Federation of American Scientists (June 17, 2013), *available at* https://fas.org/blogs/secrecy/2013/06/icig-leaks/.

259 Intelligence Community Directive 119 (Mar. 20, 2014), *available at* http://www.dni.gov/files/documents/ICD/ICD 119.pdf.

260 Cope, *supra* note 196 at 253.

261 President Barack Obama, *Obama Middle East Speech in Full With Analysis*, BBC (May 19, 2011), *available at* http://www.bbc.com/news/world-us-canada-13461682.

PEN AMERICA free expression. literature.