OPTIMAL DETERRENCE:
AN EVALUATION OF THE LEAKS-REGULATING REGIME

Aadhithi Padmanabhan, Tina Thomas & Jacob Victor[1]

December 10, 2012

EXECUTIVE SUMMARY

Recent high-profile leaks have led to renewed calls, especially from some members of Congress, for a more rigorous leaks-prosecuting regime. In response, others, most visibly the press and certain watchdog groups, have strongly resisted the claim that a more forceful response to unauthorized disclosures benefits the American public.

This report evaluates the existing leaks-regulating regime and considers which of the current reform proposals are most likely to provide optimal deterrence. First, this report outlines the myriad and sometimes contradictory interests at stake implicated by unauthorized disclosure of classified information: protecting national security, safeguarding First Amendment rights, ensuring government accountability and transparency, promoting consistency in prosecution, and furthering efficient government functioning.

Second, this report examines why it has proven difficult for the government to successfully prosecute leaks. It identifies four leading reasons. First, it can be difficult to identify a leaker, given the vast proliferation of the classification system and the expansion of national security bureaucracy. Second, the government faces significant legal burdens at trial—prosecutors often have to rely on circumstantial evidence; in the case of intangible information disclosure, the government may also have to deal with a heightened scienter requirements. Third, a trial may attract unwanted attention to an issue the government prefers to keep secret and defendants sometimes try to capitalize on this by using "graymail" defenses. Finally, the recipients of unauthorized disclosures—usually members of the press—enjoy robust constitutional protections that can restrict evidence gathering.

Third, this report describes and evaluates several existing proposals for deterring leaks:

- legislative changes;
- an independent prosecutor;
- a more concerted effort to prosecute leaks;
- increased use of administrative sanctions; and
- creation of more robust internal whistleblower channels.

The report concludes that an approach that combines increased transparency about the government's criteria for prosecutorial priorities with a robust internal mechanism to channel productive dissent is most likely to bring the U.S. leak-regulating regime closer to optimal deterrence.

---

[1] J.D. Candidates, Yale Law School. This report was prepared in connection with *International Law and Foreign Affairs*, a course at Yale Law School, under the supervision of Professor Oona Hathaway, Gerard C. and Bernice Latrobe Smith Professor of International Law, Yale Law School, and with the assistance of Spencer Amdur, Sally Pei, Julia Brower, Carlton Forbes, Christina Koningisor, Ryan Liss, and Michael Shih.

Contents

INTRODUCTION

The leaking of classified information from within the U.S. government has come under intense political scrutiny in recent months. Many have advocated for increased measures to prevent these leaks, which can harm national security. Others caution against wholesale preventative measures, citing countervailing interests such as ensuring government accountability and safeguarding First Amendment rights. And some argue that even if the only goal is to reduce leaks, preventative measures could actually foster the very leaking behavior they are meant to prevent. At the very least, they argue that such measures do not adequately differentiate between "good leaks" and "bad leaks."

This Report evaluates the existing leaks-regulating regime and considers which of the current reform proposals are most likely to provide optimal deterrence. Part I considers some of the varied interests implicated by any regime that seeks to limit the disclosure of unauthorized information—protecting national security, ensuring government transparency accountability, safeguarding First Amendment rights, promoting consistency in prosecution, and furthering efficient government functioning. The balance of these interests cautions against structuring our legal regime to focus solely on preventing leaks. This Report is therefore informed by the notion that "optimal" rather than "maximum" deterrence should be the goal. Proposals aimed at greater deterrence are unlikely to deter *all* leakers—nor should they, given the varied interests at stake. Moreover, leaks can be mutually beneficial in the dialogue between the government and the public. Therefore, deterrence measures should take account of the various interests at play for all the actors involved.

Part II identifies the difficulties associated with investigating and prosecuting leaks of classified information given the current legislative and policy landscape. One difficulty is actually identifying the leaker, which is partly a result of the vast expansion of the classification system. Even if the leaker is identified, successfully prosecuting a case can be difficult because of the legal burdens the government bears at trial. Furthermore, defendants sometimes use "graymail" at trial to force the government to disclose even more secrets, with the goal of halting the prosecution, or severely limiting its scope. Finally, robust protections for recipients of leaked information, particularly journalists, complicate investigations and prosecutions of leaks.

Part III describes and evaluates five proposals to discourage unauthorized disclosures more effectively. It first discusses legislative changes, but concludes that the main obstacles the government faces in prosecuting leaks would not be adequately addressed by statutory fixes. It then discusses the use of an independent prosecutor, which offers the advantage of reducing any perception of political expediency in the selective prosecution of certain types of leaks and leakers. On the other hand, because an independent counsel's authority is difficult to cabin, this proposal would require the President to forfeit a certain level of influence over prosecutorial decisions. A third option is simply increasing the frequency and intensity of leaks prosecutions. However, this could chill routine and mutually beneficial interactions between government employees, the media, and the public. Some also caution that a heavy-handed approach could *increase* the frequency of unauthorized disclosures. If more vigorous leaks prosecution is pursued, it should be combined with increased transparency with regard to the criteria the government uses in choosing which leaks and leakers to investigate and sanction. Next, this Part assesses the proposal for increased use of administrative sanctions, which are much easier for the government to impose than criminal sanctions. However, the same caution about chilling beneficial interactions between the government and the public applies in this context as well.

Finally, this Part evaluates options for creating more robust whistleblower channels, using the State Department's "dissent channel" as a model. While this approach has many advantages, it may only deter certain types of leakers, and its success is contingent on a perception that dissent expressed in these channels will be taken seriously and acted upon. Nonetheless, when properly executed—and when combined with increased transparency about the government's criteria for prosecutorial priorities—such an approach could reduce leaking and open alternative avenues for productive dissent.

I. THE INTERESTS AT STAKE

Before weighing the merits of particular proposals, this Report considers five interests implicated by a leaks-regulating regime: protecting national security, safeguarding First Amendment rights, ensuring government transparency and accountability, promoting consistency in prosecution, and furthering efficient government functioning. The analysis in Part III shows that any proposed reform for the leaks-regulating regime will affect these interests. These interests are, moreover, sometimes at odds with one another. For example, proposals that would likely strengthen protections for national security might in some cases lie in tension with First Amendment rights. We therefore recommend a balanced approach, one that takes into account the effect of any proposal on all the relevant interests.[1]

A. Protecting National Security

One of the primary reasons to identify and punish leakers is that leaks can harm national security. Even those who recognize competing interests, such as ensuring government accountability, acknowledge the serious harm to national security that some leaks have caused—harm that is sometimes underestimated by non-governmental actors.[2] Moreover, keeping certain governmental activities shielded from public view can be extremely important for national security. For example, the NSA's program to intercept the communications of Al Qaeda suspects in the United States and abroad before the *New York Times* leaked that information had led to an arrest, seizure of useful property, and the exposure of a terrorist plot.[3]

Several considerations, however, complicate this picture. Attempting to identify the most damaging leaks in advance is an imperfect science. As a result, the government may misjudge the likely impact of a disclosure.[4] Levels of classification, for example, are not sure guides for judging the likely national security impact of a leak, due in part to widespread over-classification.[5] Moreover, the timing of a leak can affect its impact on national security—a leak's

[1] This report relies upon and engages with the work of several scholars. It places particular emphasis on the few who have undertaken comprehensive studies of how to deter government leakers while balancing various competing interests: Jack Goldsmith, David Pozen, and Geoffrey Stone.

[2] *See* JACK GOLDSMITH, POWER AND CONSTRAINT: THE ACCOUNTABLE PRESIDENT AFTER 9/11, at 216 (2012) ("Journalists misjudge the national security harms of publishing classified secrets not only because they lack expertise but also because they are motivated in part by fame and money."); David Pozen, The Law of Leaks: Why the Government Criminalizes, and Condones, Unauthorized Disclosures of Information 23 (Dec. 8, 2012) (unpublished manuscript).

[3] GABRIEL SCHOENFELD, NECESSARY SECRETS: NATIONAL SECURITY, THE MEDIA, AND THE RULE OF LAW 32-33 (2010).

[4] Pozen, *supra* note 2, at 74.

[5] *See infra* notes 23-26 and accompanying text.

damage to national security may be minimal or nonexistent in some cases involving time-sensitive information.[6]

B. Safeguarding First Amendment Rights

Actions taken to prevent leaks can, in some cases, lead to excessive chilling of free speech and hence improper infringement or restrictions on First Amendment rights. The current Administration has unflinchingly reaffirmed its commitment to the First Amendment when pursuing prosecutions of individual leakers.[7] Yet even when individual prosecutions do not violate the First Amendment, "[t]he interjection of the government into the very heart of the journalist-source relationship could have a serious chilling effect on journalist-source exchanges."[8] This chilling effect may make it more difficult for individuals involved to exercise their rights to free speech under the First Amendment.

Increased prosecution of non-governmental actors can lead to a chilling effect that intrudes on First Amendment guarantees—guarantees that ensure the information flow needed to support a constitutional democracy. This is reflected in the Department of Justice's internal guidelines, which make subpoenaing journalists extremely difficult[9] and emphasize First Amendment values.[10] Robust protections for nongovernmental actors make it possible for those actors to keep the executive in check through what Harvard professor and former OLC Assistant Attorney General Jack Goldsmith calls "accountability journalism."[11] Even absent prosecution, if the government is seen as tightly controlling all information that is released, the media may distance itself from the government, fearing the reputational harm that could come from being seen as a pawn of the government. This might undermine the capacity of the media to provide effective accountability.[12]

Government employees also enjoy certain First Amendment safeguards, albeit more limited than those of nongovernmental actors. These safeguards are differentiated depending on whether a government employee is punished "by the government in the latter's capacity as employer or whether she is punished by the government in the latter's sovereign capacity as prosecutor."[13] Increased use of administrative and criminal sanctions against government employees may not only infringe on government employees' First Amendment rights but may also discourage them from sharing information with the public that is important for government transparency and good governance.[14]

---

[6] Pozen, *supra* note 2, at 77.

[7] Heidi Kitrosser, *Free Speech Aboard the Leaky Ship of State: Calibrating First Amendment Protections for Leakers of Classified Information* 4 (Univ. of Minn. Law Sch. Legal Studies Research Paper Series, Research Paper No. 12-22, 2012), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2071265 ("The Obama, Bush, and Reagan Administrations all have argued that such prosecutions do not implicate the First Amendment in any way.").

[8] Geoffrey R. Stone, *Government Secrecy vs. Freedom of the Press*, 1 HARV. L. & POL'Y REV. 185, 212 (2007).

[9] Pozen, *supra* note 2, at 19-20.

[10] *See* 28 C.F.R. § 50.10 (2010) (emphasizing "freedom of the press," "the news gathering function," and "a reporter's responsibility to cover as broadly as possible controversial public issues")

[11] GOLDSMITH, *supra* note 2, at 60-61.

[12] *See* Pozen, *supra* note 2, at 37.

[13] *See* Kitrosser, *supra* note 7, at 3.

[14] *See* Pozen, *supra* note 2, at 35-39.

C. Ensuring Government Accountability and Transparency

Leakers can in some instances play an important role in government accountability and transparency. Leaks can inform the public and thus allow the public to hold the government accountable for its actions.[15] Scholars such as Jack Goldsmith have acknowledged that leaks have been fundamental in the last decade in spurring Congress, the courts, and the public to respond to abuses of executive power.[16] Government employees are specially situated to reveal abuses or mistakes to which they alone may be privy. And there is evidence that some leakers have been motivated by their desire to hold the government accountable.[17]

In response, some have argued that those who wish to hold the government accountable should proceed through formal governmental channels for whistleblowing rather than through leaking.[18] (A proposal for strengthening internal channels for whistleblowing is considered in Part III.) Whether these proposals are sufficient turns in part on whether government accountability can be ensured without leaks to the public. It also turns in part on whether transparency to the public is considered an independent value. In the handful of leak cases the government has chosen to prosecute, it has been criticized for being non-transparent even when the information revealed did not further the goal of holding the government accountable for its actions. For instance, John Kiriakou was prosecuted for exposing a CIA officer who had engaged in torture.[19] Many argued the prosecution was improper because it provided public transparency of improper government action, even though the leaked information did not lead to action against the officer.[20] Indeed, leakers have often been cast as "whistleblowers," indicating that government transparency is regarded an inherent good. For example, critics of leaks prosecutions have referred to leaker Thomas Drake as a "classic whistle-blower who tried to save taxpayers more than $1 billion."[21]

Finally, the interest in ensuring government accountability and transparency is especially salient given what many regard as a culture of "over-classification" of government documents.[22]

---

[15] Geoffrey R. Stone, *Wikileaks, the Proposed SHIELD Act, and the First Amendment*, 5 J. NAT'L SECURITY L. & POL'Y 105, 108 (2011).

[16] GOLDSMITH, *supra* note 2, at 69, 82.

[17] For example, Daniel Ellsberg believed he was likely to be incarcerated for the rest of his life for leaking the Papers, yet chose to do so anyway. *See* Heidi Kitrosser, *What If Daniel Ellsberg Hadn't Bothered?*, 45 IND. L. REV. 89, 89 (2011). And Thomas Drake found it extraordinary that telling the congressional oversight committee about financial waste, bureaucratic dysfunction, and dubious legal practices in government counterterrorism programs constituted leaking. He also was willing to lose his job for the sake of government accountability. *See* Jane Mayer, *The Secret Sharer: Is Thomas Drake an Enemy of the State?* THE NEW YORKER, May 23, 2011, http://www.newyorker.com/reporting/2011/05/23/110523fa_fact_mayer.

[18] *See, e.g.*, Valerie Caproni, *IV. Panel: The Role of Whistleblowers to Facilitate Government Accountability*, 57 AM. U. L. REV. 1243 (2008).

[19] Jesselyn Radack, *BREAKING: The Back Story to Kiriakou's Imminent Guilty Plea,* DAILY KOS (Oct. 23, 2012, 05:57 AM), http://www.dailykos.com/story/2012/10/23/1148729/-BREAKING-The-Back-Story-to-Kiriakou-s-Imminent-Guilty-Plea.

[20] *Id.*

[21] Scott Shane & Charlie Savage, *Administration Took Accidental Path to Setting Record for Leak Cases*, N.Y. TIMES, June 19, 2012, http://www.nytimes.com/2012/06/20/us/politics/accidental-path-to-record-leak-cases-under-obama.html; *see also* Mayer, *supra* note 17 (profiling Drake and providing a summary of the events leading up to his prosecution).

[22] *See, e.g.*, Kitrosser, *supra* note 7, at 16 ("J. William Leonard, the former director of the Information Security Oversight Office in the George W. Bush administration, acknowledges a problem of 'excessive classification.' Leonard says that he has 'seen information classified that [he's] also seen published in third-grade textbooks.' At a

Documents are designated as classified even when they do not necessarily require insulation from the public; as a result, information is increasingly being shielded from public view. Erwin Griswold, the former Solicitor General of the United States, argued that increased classification was being used not for the necessary protection of sensitive information, but rather to prevent "governmental embarrassment."[23] And the Moynihan Commission, set up in the 1990s to study government secrecy, observed in its 1997 report that "[t]he classification system . . . is used too often to deny the public an understanding of the policymaking process, rather than for the necessary protection of intelligence activities and other highly sensitive matters."[24] Indeed, various government actors, recognizing the value of government accountability and transparency, have advocated for less secrecy, including the President's Foreign Intelligence Advisory Board under President John F. Kennedy[25] and the Secrecy and Disclosure Subcommittee of the Senate Select Committee on Intelligence under President Jimmy Carter.[26]

D. Promoting Consistency in Prosecution

There is currently a disconnect between the government's public condemnation of leaking and its quiet toleration of most disclosures of classified information.[27] One reason leak laws are rarely enforced is precisely because many of those in government have an interest in maintaining some leakage of information to the press and the public.[28] In part as a result, only a small number of leaks are actually prosecuted. Yet the small number of prosecutions and the absence of any public criteria for prosecution have created an impression of selective prosecution. Such inconsistency may compromise public confidence in the motivations for, and hence legitimacy of, leaks prosecutions. Some may be concerned, for example, that the government targets low-level employees in leak prosecutions, rather than prosecuting high-level officials who are more likely to leak information that is not already widely known.[29] More consistent or public criteria for prosecution would thus lend greater legitimacy to the government's leak prosecutions.

2004 congressional hearing, both Leonard and Carol Haave, then the Defense Department's Undersecretary for Intelligence, estimated that 'probably about *half* of all classified information is overclassified.'"). The number of classified documents has increased exponentially since the system began in 1951. *See* Kitrosser, *supra* note 17, at 96 ("By the 1970s, millions of documents were classified yearly and estimates on the number of persons with some form of classification authority ranged from several thousand to more than one million. Today, roughly sixteen million new official secrets are created yearly, and several million persons in the United States have some form of classification authority.").

[23] Erwin N. Griswold, *Secrets Not Worth Keeping*, WASH. POST, Feb. 15, 1989, at A25.

[24] Kitrosser, *supra* note 7, at 17 (quoting S. DOC. NO. 105-2, at XXI (1997) (Comm. Rep.)). For another critique of over-classification, see GOLDSMITH, *supra* note 2, at 69-73.

[25] *See* KENNETH MICHAEL ABSHER, MICHAEL C. DESCH & ROMAN POPADIUK, PRIVILEGED AND CONFIDENTIAL: THE SECRET HISTORY OF THE PRESIDENT'S INTELLIGENCE ADVISORY BOARD 81 (2012).

[26] SUBCOMM. ON SECRECY AND DISCLOSURE, S. SELECT COMM. ON INTELLIGENCE, 95TH CONG., REP. ON NATIONAL SECURITY SECRETS AND THE ADMINISTRATION OF JUSTICE 34 (Comm. Print 1978) [hereinafter SSCI Report]. Such reforms are, of course, extremely difficult to implement. Pozen, *supra* note 2, at 53 ("Unwinding overclassification is exceedingly difficult to do, however. Years of reform efforts have barely made a dent, and it is not clear they ever will.").

[27] Pozen, *supra* note 2, at 2, 12-17 (arguing that leaks are widespread, mentioning that "[i]t is a commonplace that leaks course through the nation's capital. Classified information leaks to the media are thought to occur so regularly in Washington as to constitute 'a routine method of communication about government.'").

[28] *Id.* at 4.

[29] *Id.* at 43-44.

E. Furthering Efficient Government Functioning

Leaks may play a positive role in furthering efficient government functioning. For example, the interest in government accountability and transparency emphasizes a desire to identify and correct any governmental wrongdoing. But even if no wrongdoing is found, leaks enhance the executive's credibility and legitimacy, which may lead to an increase in popular approval of future government actions. Leaking can thus enhance long-term executive power. If members of the public believe that leaking is pervasive, they will believe that they will come to learn about any nefarious activities within the government.[30] Members of the public would then expect that the government would internalize this prospect and therefore hesitate to engage in such activities in the first place.[31] A "bloated official secrecy system," on the other hand, does not engender trust among members of the public.[32] Such a system makes it seem as if the government has something to hide. Although leaking may reduce presidential power in the short term, it "ultimately serve[s] to enhance it by sustaining the institution's credibility and legitimacy and thereby securing popular approval of further grants of discretionary authority."[33]

Leaks also facilitate information flows throughout the government.[34] Leaks have been used to attract the attention of an otherwise inaccessible President.[35] In turn, the executive has used leaks to signal policy shifts or disapproval.[36] One could argue that these flows are enhanced by the existence of anti-leak laws, even if rarely enforced. That is, such laws decrease the overall amount of leaking, enhancing the informative and signaling power of the disclosures that are made.[37]

Finally, leaks also enhance the government's relationship with certain groups, like the media. Columbia law professor and former Special Advisor to the Legal Adviser at the Department of State David Pozen argues that the laws against leaks increase the value of the information that the media actually procure: "Publicizing leaks is how they scoop their competitors."[38] By channeling leaks to favored media outlets, the executive branch can influence the subsequent coverage; this, therefore, becomes a "mutually beneficial arrangement."[39] Leaks also benefit Congress, which receives information from the media without much additional work on its part.[40]

---

[30] *Id.* at 47.
[31] *Id.*
[32] *Id.* at 48.
[33] *Id.* at 47.
[34] *Id.* at 49-51.
[35] *Id.* at 50.
[36] *Id.*
[37] *Id.*
[38] *Id.* at 52.
[39] *Id.*
[40] *Id.* at 54-55.

II. THE DIFFICULTIES OF INVESTIGATING AND PROSECUTING UNAUTHORIZED DISCLOSURES OF CLASSIFIED INFORMATION

The Obama administration has investigated and prosecuted a record number of leaks: six prosecutions, compared with three under all previous Presidents combined.[41] However, a combination of factors makes the task of investigating and prosecuting unauthorized disclosures difficult. In this section we identify four major difficulties.

A. Identifying the Leaker

As then-Attorney General John Ashcroft noted in a letter to Congress in October 2002, "identifying the individual who disclosed classified information without authority has been difficult, at best."[42] Similarly, his predecessor Janet Reno told Congress, "[T]he universe of individuals with authorized access to the disclosed information is so large as to render impracticable further efforts to identify the leaker."[43] This is due in part to growth in the national security bureaucracy. For example, a covert action, which once was an "intimate affair," today typically requires multiple layers of review and clearance by "dozens of lawyers and policymakers in the CIA, the Office of the Director of National Intelligence, the National Security Council, and the Departments of Justice, State, and Defense, before being presented to the President and his principals for a final decision and then being sent on to Congress."[44]

It is also difficult to track the source of leaks by working backwards from publication, because many recent disclosures have come "from deeply reported projects" that "tend to have diffuse sourcing, making it hard to isolate who first disclosed the essence of what later becomes an article."[45] However, the existence of an electronic trail may, in some instances, make it easier to build a "circumstantial case" today than in earlier eras.[46]

B. Legal Burden at Trial

Once the source of a classified information leak is identified, successfully prosecuting a case still presents challenges. Of the nine prosecutions the government has brought for national

---

[41] Kitrosser, *supra* note 17, at 111 ("As for the Obama Administration, observers who expected a departure from the Bush Administration's aggressive pursuit of leaks were in for a shock . . . the Obama administration has pursued more leak prosecutions than every other administration in history combined"); Charlie Savage, *Nine Leak-Related Cases,* N.Y. TIMES, June 20, 2012, http://www.nytimes.com/2012/06/20/us/nine-leak-related-cases.html (briefly describing the nine leaks prosecutions). However, many of the six prosecutions under the Obama Administration were actually initiated during the Bush Administration. Shane & Savage, *supra* note 22. Some suggest that the total count of leak prosecutions under the current and past administrations may actually be thirteen. Pozen, *supra* note 2, at 17. Whatever the actual count, there is general agreement that the number of prosecutions is miniscule.

[42] Letter from John Ashcroft, U.S. Att'y Gen., to J. Dennis Hastert, Speaker of the House of Representatives, at 4 (Oct. 15, 2002) [hereinafter Letter from John Ashcroft], *available at* http://www.justice.gov/ag/readingroom/letter_house.pdf.

[43] *Unauthorized Disclosure of Classified Information: Hearing Before the S. Select Comm. on Intelligence*, 106th Cong. 8 (2000) (statement of Janet Reno, Att'y Gen.) [hereinafter Reno Testimony].

[44] GOLDSMITH, *supra* note 2, at 72.

[45] Charlie Savage, *For U.S. Inquiries on Leaks, a Difficult Road to Prosecution,* N.Y. TIMES, June 9, 2012, http://www.nytimes.com/2012/06/10/us/for-us-inquiries-on-leaks-a-difficult-road-to-prosecution.html.

[46] *Id.*; *see also* Adam Liptak, *A High-Tech War on Leaks,* N.Y. TIMES, Feb. 11, 2012, http://www.nytimes.com/2012/02/12/sunday-review/a-high-tech-war-on-leaks.html ("Today, advances in surveillance technology allow the government to keep a perpetual eye on those with security clearances.")

security leaks, only one has resulted in a successful trial outcome. Samuel Morison, a naval intelligence analyst who gave *Jane's Defence Weekly* satellite photographs of Soviet shipbuilding in 1984, was convicted by a jury and sentenced to two years in prison.[47]

Because the government often has to rely on circumstantial evidence, "the leaker . . . cannot be identified beyond a reasonable doubt, as is required for a successful prosecution."[48] Furthermore, Attorney General Reno explained that the government declines to bring cases even once a leaker is identified because it decides that it "could not convince a jury beyond a reasonable doubt that the person had committed every element of the offense or that a jury would likely refuse to convict notwithstanding the evidence."[49]

Another difficulty presents itself when "intangible" classified information—as opposed to documentary evidence—is leaked. The case law is unsettled on the content of the government's burden when a defendant is charged, not with relaying documents, but rather with disseminating intangible information "relating to the national defense, which . . . the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation."[50] Courts are divided on the content of this "reason to believe" scienter requirement, which is distinct from, and additional to, the "willfulness" requirement[51] found in the rest of the Espionage Act. In *United States v. Rosen,* where two former lobbyists of AIPAC were indicted, a federal district court ruled that the government had to prove that the defendants had "a bad faith purpose to harm the United States or to aid a foreign government."[52] However, this October, another federal district court ruled that this same heightened scienter showing does not necessarily apply in the case of a government employee.[53] That court distinguished *Rosen,* stating, "Kiriakou was a government employee trained in the classification system who could appreciate the significance of the information he allegedly disclosed. Accordingly, there can be no question that Kiriakou was on clear notice of the illegality of his alleged communications."[54] If more district courts follow *Kiriakou*'s lead, the government's ability to successfully prosecute government employees may increase. However, because of the way in which the *Kiriakou* court distinguished *Rosen,* the impediment remains if the government wants to prosecute an individual other than the initial government source.

C. Graymail and Unwanted Publicity

In addition to the difficulties associated with proving all the elements of the offense, evidentiary hurdles also present a challenge for the government at trial. Sometimes the mere fact of the trial draws attention to an issue that the government would rather keep secret.

---

[47] United States v. Morison, 844 F.2d 1057 (4th Cir. 1984); Savage, *Nine Leak-Related Cases, supra* note 41.
[48] *Oversight of the Federal Bureau of Investigation: Hearing Before the S. Comm. on the Judiciary*, 111th Cong. 46 (2009) (written response of Robert Mueller, Dir., Fed. Bureau of Investigation) [hereinafter Mueller Response].
[49] Reno Testimony, *supra* note 43, at 10.
[50] 18 U.S.C. §793(d) (2006).
[51] *Id.* ("Whoever, lawfully having possession of, access to, control over, or being entrusted with any document . . . or information . . . willfully communicates, delivers, transmits . . . [s]hall be fined under this title or imprisoned not more than ten years, or both.").
[52] United States v. Rosen, 520 F. Supp. 2d 786, 793 (E.D. Va. 2007); *see also* United States v. Rosen, 445 F. Supp. 2d 602, 641 n.56 (E.D. Va. 2006) ("[T]he additional scienter requirement contained in the 'reason to believe' clause that applies to intangible information, is not superfluous because it relates not to the nature of the information, but to the subjective understanding of the defendant as to the possible *effect* of the disclosure.").
[53] United States v. Kiriakou, No. 1:12cr127, 2012 U.S. Dist. LEXIS 149508 (E.D. Va. Oct. 16, 2012).
[54] *Id.* at *10.

Furthermore, despite the existence of the Classified Information Procedures Act,[55] intended to allow leaks prosecutions to continue without revealing further secrets, "judges have not always agreed with the government that certain information can be withheld from a public trial."[56] Defendants also use a tactic known as "graymail defense," in which they argue that their right to a fair trial is contingent on identifying other personnel within their agency who also had access to the information they are accused of relaying.[57] When judges rule for the defense on such evidentiary issues, the government is sometimes forced to amend its charges or drop the case completely to avoid further disclosure. For instance, in 2011, the government essentially abandoned its case against NSA official Thomas Drake when the district court "issued a discovery ruling that likely would have resulted in public references at trial to certain NSA activities."[58] Indeed, a report by the Secrecy and Disclosure Subcommittee of the Senate Select Committee on Intelligence emphasized that the enforcement of anti-leak laws often required the disclosure of the very information the laws were intended to protect.[59]

D. Robust Protections for Recipients

The government has never prosecuted a journalist for publishing leaked information. Given the resulting paucity of case law on criminal sanctions for media outlets, there are many unresolved questions on how courts would react if the recipients of government leaks were prosecuted for holding or disseminating classified information. The government may benefit from the existing uncertainty, and there is the risk that litigation could create precedent that would harm the government's cause. This is especially true because there are some indicators that courts would apply robust protections for recipients in such cases if they did get litigated.

For instance, in the Pentagon Papers case, the Supreme Court refused to grant the government an injunction barring the *New York Times* from publicizing classified information, distinguishing between the methods the government could use to limit the spread of information before and after that information was disseminated outside the government.[60] Although the case involved a civil injunction, the Supreme Court's demarcation between government employees and other individuals likely carries over to the criminal context.[61]

There are likely further hurdles for the government to criminally sanction recipients and publishers of unauthorized disclosures. Geoffrey Stone, professor and former Dean at the University of Chicago Law School, argues that the implication of the reasoning in the Pentagon

---

[55] 18 U.S.C. app. 3 §§ 1-16 (2006).

[56] Savage, *supra* note 45. *But see* Pozen, supra note 2, at 31 ("If anything, the literature on [the Classified Information Procedures Act] tends to underscore how harsh it has proven for defendants, who complain they are rarely given access to the government's classified evidence or permitted to submit their own classified evidence.").

[57] Savage, *supra* note 45.

[58] David Laufman, *Prosecuting Leaks of Classified Information*, HUFFINGTON POST (June 12, 2012, 1:17 PM), http://www.huffingtonpost.com/david-laufman/prosecuting-leaks_b_1585193.html. The government dropped the felony charge; in exchange, Drake pled guilty to a minor misdemeanor. *Id.*

[59] SSCI Report, *supra* note 26, at 1.

[60] N.Y. Times Co. v. United States, 403 U.S. 713 (1971).

[61] *See* Stone, *supra* note 15, at 116 ("The standard applied in the Pentagon Papers case is *essentially* the same standard the Court would apply in a criminal prosecution of an organization or individual for publicly disseminating information about the conduct of government. The clear and present danger standard has never been limited to cases of prior restraint.").

Papers case and the balancing of interests in *Pickering*[62] is that the appropriate test for nongovernment employees would involve consideration of both "the harm caused by the speech *and* the value of the speech."[63] Functionally, this could mean that, to successfully prosecute recipients, the government would not only have to show that an individual's use of classified information would result in grave and imminent harm to national security, but also that "the publication would *not* significantly contribute to public debate."[64]

De facto shielding of journalists also occurs even when they are not the subjects of the investigation. Although DOJ's position is that there is no constitutional or common law privilege for journalists to withhold their source's identity, DOJ's own internal regulations, justified on First Amendment grounds, create special procedures to subpoena journalists, which essentially restrict the issuing of subpoenas to very rare circumstances.[65] The FBI has interpreted this same regulation as "requiring that . . . leak investigations focus on potential leakers rather than reporters."[66] Although it may not be required by either statute or the Constitution, this internal policy defines the contours of DOJ investigations and contributes to the difficulties associated with identifying leakers.

Commentators have argued that "political and legal developments of the past several years have made the executive branch increasingly willing to subpoena journalists to demand source information."[67] A 2007 study by the Reporters Committee for the Freedom of the Press found "a five-fold increase since 2001 in subpoenas seeking information on a media outlet's confidential sources."[68] An increased willingness to pursue news organizations to identify leakers may facilitate leaks investigations. But it is not immediately clear that subpoenaing journalists would yield much greater success. Not only does the media strenuously contest subpoenas, some journalists—famously including *New York Times* journalist Judith Miller—may choose jail time and contempt orders rather than comply.[69]

III. EVALUATING PROPOSED CHANGES TO LAW AND POLICY

There have been several proposals made to address the problem of government leaks. This Part outlines and evaluates five of the leading proposals that have been put forward to deter leaks. The analysis aims to assess how each proposal will affect the interests identified in Part I.

At the outset, it is important to note that the goal of these proposals cannot be to eliminate leaks altogether. An individual who is so disillusioned with the system that he or she thinks the public is best-served by revealing a vast and indiscriminate array of government secrets is

---

[62] Pickering v. Bd. of Educ. of Twp. High Sch. Dist. 205, 391 U.S. 563 (1968) ("[T]he State has interests as an employer in regulating the speech of its employees that differ significantly from those it possesses in connection with regulation of the speech of the citizenry in general.").
[63] Stone, *supra* note 15, at 117.
[64] *Id.* at 117-18.
[65] 28 C.F.R. §50.10 (2010); Pozen, *supra* note 2, at 20.
[66] Mueller Response, *supra* note 48, at 46.
[67] Kitrosser, *supra* note 7, at 26. *But see* GOLDSMITH, *supra* note 2, at 222 ("[W]hat is remarkable about the last decade is not the slight increase in attempts to use subpoenas against journalists but rather the relative sparse use of subpoenas given the number and type of leaks.").
[68] Kitrosser, *supra* note 17, at 111 (quoting Laura Rozen, *Hung Out To Dry: The National-Security Press Dug Up the Dirt, but Congress Wilted*, COLUM. JOURNALISM REV., Jan-Feb. 2009, at 34).
[69] *See* Mueller Response, supra note 48, at 46 ("There are often lengthy legal challenges to the subpoena, which on a rare occasion can entail a reporter electing to serve jail time for contempt rather than comply with the subpoena.")

unlikely to be deterred by any change in legal regime. To the extent there is a deterrence effect, it is likely to be on a subset of those who engage in leaks.

Perfect deterrence is an ephemeral goal for another reason: the vast over-classification of government documents[70] and the commonplace nature of leaking.[71] There are simply too many classified documents in too many hands to perfectly prevent leaks. As a result, any changes to law or policy must aim not for complete deterrence, but for optimal deterrence.

A. Legislative Changes

Proposed Reforms:

(1) In 2000, Congress passed a bill that provided for "comprehensive" legislation that criminalized all leaks of classified information. It made leaking classified information punishable by three years in prison for any "officer or employee of the United States" or any other person with authorized access to that information who knowingly and willfully disclosed that information.[72] President Clinton vetoed this legislation, stating that the felony provision was "overbroad" and would "create an undue chilling effect."[73]

(2) In the wake of Wikileaks' release of classified documents in 2010, the Securing Human Intelligence and Enforcing Lawful Dissemination ("SHIELD") Act was introduced.[74] Unlike the 2000 measure, the SHIELD Act was intended to fill gaps in the Espionage Act, and, specifically, to bolster 18 U.S.C. § 798, which prohibits disclosures of cryptographic and communications information.[75] The SHIELD Act proposed to "add coverage for disclosures of classified information related to human intelligence activities."[76] One of the main effects of this bill would have been to "make it a crime for any person knowingly and willfully to disseminate, in any manner prejudicial to the safety or interest of the United States, 'any classified information . . . concerning the human intelligence activities of the United States or . . . concerning the identity of a classified source or informant' working with the intelligence community of the United States."[77] The amendment's language was not limited to government employees,[78] and there is no indication that the government bringing prosecution under this

---

[70] *See supra* Section I.C.

[71] *See supra* Section I.D.

[72] *See* H.R. 4392, 106th Cong. § 304 (2000). The full text of this provision reads:

> Whoever, being an officer or employee of the United States, a former or retired officer or employee of the United States, any other person with authorized access to classified information, or any other person formerly with authorized access to classified information, knowingly and willfully discloses, or attempts to disclose, any classified information acquired as a result of such person's authorized access to classified information to a person(other than an officer or employee of the United States) who is not authorized access to such classified information, knowing that the person is not authorized access to such classified information, shall be fined under this title, imprisoned not more than 3 years, or both.

[73] President's Message on Returning Without Approval to the House of Representatives the "Intelligence Authorization Act for Fiscal Year 2001," 36 WEEKLY COMP. PRES. DOC. 2784, 2785 (Nov. 13, 2000).

[74] H.R. 6506, 111th Cong. (2010).

[75] Stone, *supra* note 15, at 105.

[76] JENNIFER K. ELSEA, CONG. RESEARCH SERV., R41404, CRIMINAL PROHIBITIONS ON THE PUBLICATION OF CLASSIFIED DEFENSE INFORMATION 28 (2012).

[77] *See* Stone, *supra* note 15, at 105 (quoting H.R. 6506, *supra* note 74).

[78] *Id.*

amended statute would have to show a defendant knew, or should have known, that disseminating information would have posed a clear harm to the United States.[79]

(3) In 2012, the Senate Intelligence Committee voted 14 to 1 to add an amendment to the 2013 Intelligence Authorization Act that, inter alia, would restrict interactions between the press and government officials and would impose sanctions such as loss of pension benefits and revocation of security clearance for certain types of leakers.[80] Unlike the previous two measures, this proposed legislation neither amends the Espionage Act nor makes all disclosures of classified information felonies.[81]

Assessment:

There is disagreement over whether the existing legislative framework for prosecuting leaks is sufficient. Attorney General Ashcroft concluded that, while there is no comprehensive statute that provides criminal penalties for leaks, the existing framework—including, but not limited to, the Espionage Act—provides a sufficient "legal basis to prosecute those who engage in unauthorized disclosures, if they can be identified."[82] Attorney General Reno's own position, while slightly more qualified, was essentially the same. She concluded that existing criminal statutes would allow the DOJ "to prosecute *almost all* leaks."[83] And she acknowledged that the Department has "never been forced to decline a prosecution solely because the criminal statutes were not broad enough."[84] In the past decade, neither administration has made such reforms a legislative priority.[85]

In contrast, some government studies on leaks have advocated more stringent laws, and offered suggestions similar to the three examples surveyed above. For example, the 1978 report by the Secrecy and Disclosure Subcommittee of the Senate Select Committee on Intelligence suggested a narrowly drawn law to punish the disclosure of the identity of American intelligence agents.[86] The committee members could not agree on any broader statutory changes,[87] even though it agreed that "no present statute can be effectively enforced against 'leaks.'"[88] A report prepared by a committee reviewing Department of Defense ("DoD") security policies and practices in 1985 stated that existing civilian criminal statutes "do not provide adequate remedies."[89] The report went on to state that the DoD had, in principle, supported proposed legislation to establish more effective criminal sanctions for leaking, but there was no agreement in the government on the content of such a proposal.[90] An interdepartmental group that produced the "Willard Report" in 1982 similarly argued that it would be helpful for Congress to pass a statute that provides for "criminal penalties for government employees who, without

[79] This situation is in some ways analogous to the discussion *supra* in Section II.B of the content of the second scienter requirement in the "reason to know" clause of 18 U.S.C. § 793(d) that *Kiriakou* and *Rosen* discuss.
[80] Intelligence Authorization Act for Fiscal Year 2013, S. 3454, 112th Cong. §§ 501, 502, 511, 512 (2012).
[81] Steven Aftergood, *Senate Intelligence Committee Adopts a Dozen Anti-Leak Measures*, SECRECY NEWS (July 26, 2012), http://www.fas.org/blog/secrecy/2012/07/ssci_leak.html.
[82] Letter from John Ashcroft, *supra* note 42, at 3.
[83] Reno Testimony, *supra* note 43, at 10 (emphasis added).
[84] *Id.*
[85] Pozen, *supra* note 2, at 34.
[86] SSCI Report, *supra* note 26, at 3.
[87] *Id.* at 22-23.
[88] *Id.* at 5.
[89] KEEPING THE NATION'S SECRETS: A REPORT TO THE SECRETARY OF DEFENSE BY THE COMMISSION TO REVIEW DOD SECURITY POLICIES AND PRACTICES, 74 (1985).
[90] *Id.*

authorization, disclose information that is properly classified pursuant to statute or Executive order."[91] It reasoned that such a law would be appropriate "in view of the substantial body of criminal statutes punishing unauthorized disclosure of other kinds of sensitive information by government employees, such as banking, agricultural, and census data. Classified national security information deserves at least the same degree of protection."[92] The Willard Report recommended that any such statute be "simple and general in order to cover all situations" and went on to provide its own suggested language.[93]

Although there is no clear answer on whether revised legislation is required, the difficulties identified in Part II support the conclusions drawn by Attorneys General Reno and Ashcroft that more legislation would not necessarily make it easier to prosecute leaks. It appears that the main obstacles the government faces in prosecuting leaks involve either constitutional or policy constraints that a statute could not adequate address. Moreover, any changes to the law, as the three examples described earlier in this section demonstrate, would raise constitutional and policy concerns of their own.

For instance, legislation that seeks to regulate interactions between the media and government employees runs the risk of being over-inclusive and hampering communications that would be mutually beneficial for the administration, the press, and the public (as discussed in Part I). Another related critique leveled against the 2013 amendment—that would also apply to "comprehensive" legislation of the variety Congress tried to pass in 2000—is that it fails to differentiate between "information that is properly classified and the vast pile of information that poses no national risk but has been deemed secret thanks only to a dysfunctional system of over-classification of government documents."[94] By reducing any individual official's use of discretion when communicating with the media, such revisions to the law could inadvertently chill the exercise of First Amendment rights.

Blanket criminalization of leaks where no attempt is made to differentiate between government employees, the press, and members of the general public may not properly call for different scienter requirements. For instance, the lack of a knowledge requirement in the SHIELD Act could render it unconstitutional when applied to non-government employees.[95] Attorney General Reno opposed the 2000 legislation in part because it might have criminalized "inadvertent disclosures."[96]

---

[91] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO/GGD-83-15, REPORT OF THE INTERDEPARTMENTAL GROUP ON UNAUTHORIZED DISCLOSURES OF CLASSIFIED INFORMATION 2 (1982) [hereinafter Willard Report], *available at* http://www.fas.org/sgp/library/willard.pdf.

[92] *Id.*

[93] *Id.* at 13-14.

[94] Editorial, *A Pernicious Drive Towards Secrecy*, N.Y. TIMES, Aug. 2, 2012, http://www.nytimes.com/2012/08/03/opinion/a-pernicious-drive-toward-secrecy.html; *see also* Editorial, *A Bill To Stop Security Leaks Puts a Plug in Democracy,* WASH. POST. (July 30, 2012), http://www.washingtonpost.com/opinions/squelching-public-interest-in-national-security/2012/07/30/gJQAF0pHLX_story.html ("Serious reform would deal not only with protecting secret information but also repair a dysfunctional system that wildly overclassifies documents which would enrich the public debate").

[95] Stone, *supra* note 15, at 105.

[96] Reno Testimony, *supra* note 43, at 12-13.

B. Independent Prosecutor

Proposed Reform:

Earlier this year, responding to leaks on cyber-attacks against Iran, drones and "kill lists," and an undercover operative who infiltrated Al Qaeda in Yemen, Senators Joseph Lieberman and John McCain called for an independent prosecutor to investigate and bring charges against government sources of leaks.[97] Instead, President Obama appointed two U.S. attorneys to lead the investigations. Attorney General Eric Holder responded to criticisms by stating, "We have people who have shown independence . . . . And the charge that I've given them is to follow the leads wherever they are."[98]

Assessment:

The old adage is that "the ship of state is the only vessel that leaks from the top."[99] The major benefit of appointing an independent prosecutor would be, as Senator Lieberman argued, the "avoid[ance] [of] any appearance of conflict of interest."[100] Given the high volume of leaks prosecutions in recent years, the Obama Administration is particularly susceptible to criticism that it unevenly targets leakers whose message it does not like, while "eagerly volunteer[ing] anonymous 'senior administration officials' for interviews when politically expedient."[101] A special prosecutor would address such criticism.

While an independent prosecutor would manage the perception that only certain types of *leaks* are prosecuted, such an appointment would also address the perception that only certain types of *leakers* are targeted. The current system "privileges White House officials over agency officials, political appointees over civil servants, senior staff over junior staff, and non-[Intelligence Community (IC)] employees over IC employees, both in terms of the type of sanctions utilized and in the amount of disclosure discretion given."[102] A special prosecutor might not do the same. Furthermore, if this prosecutor were to clamp down on leaking from senior officials at the "top of the ship," it might also reduce leaking from below to the extent that "widespread disrespect of the secrecy system at or near the top of government embolden[s] the unusual number of whistle-blowers further down."[103]

The benefit of an independent prosecutor is also its primary drawback: the President forfeits a great deal of control and influence over prosecutorial decisions. Once an independent prosecutor is created, it can be difficult to cabin its authority. Such a possibility is vividly captured in Patrick Fitzgerald's prosecution of I. Lewis Libby for obstruction of justice and perjury, after Fitzgerald was initially called upon to investigate the leak of Valerie Plame's

---

[97] *See* Pam Benson, *Republicans Demand (Again) Special Investigator To Investigate Leaks,* CNN, June 26, 2012, http://security.blogs.cnn.com/2012/06/26/republicans-demand-again-special-investigator-to-investigate-leaks/; Will Dunham et al., *Key Senator Calls for Special Counsel for Leaks Probe*, REUTERS, June 17, 2012, http://www.reuters.com/article/2012/06/17/us-usa-security-leaks-idUSBRE85G0ET20120617; Jeremy Herb, *McCain Set To Offer Resolution on Special Counsel on Leaks as Early as Tuesday*, THE HILL, June 11, 2012, http://thehill.com/blogs/defcon-hill/policy-and-strategy/232069-mccain-resolution-calling-for-special-counsel-on-leaks-could-come-tuesday.

[98] Quoted in Benson, *supra* note 97.

[99] *See* Kitrosser, *supra* note 7, at 17.

[100] Dunham et al., *supra* note 97 (quoting the Senator's statement).

[101] Uri Friedman, *Good Leak, Bad Leak: A Look at the Obama Administration's Hot-and-Cold Approach to Secrets*, FOREIGN POLICY (June 8, 2012), http://www.foreignpolicy.com/articles/2012/06/07/good_leak_bad_leak.

[102] Pozen, *supra* note 2, at 61.

[103] GOLDSMITH, *supra* note 2, at 71.

identity to the press.[104] An "independent counsel has no need to view a particular case in relation to similar cases, past or future . . . . [He or she] is cut off from the accumulated lore and wisdom of career Department of Justice officers."[105]

A special prosecutor could impede a President who wanted to exercise substantial control over balancing leak-deterrence with other policy priorities. However, the current referral process to DOJ from the various agencies could mitigate this effect to a certain extent.[106] Most leak cases are filtered out before they reach the DOJ. Moreover, most agencies tend to manage the referral process in a "relatively centralized fashion, as by routing all concerns through their general counsel's office."[107] By exercising influence at the agency level, the President could still maintain some control over which leaks end up at the prosecutor's desk. Nevertheless, the impropriety of the White House discussing particular cases with the individual agencies may be greater than if it discretely influences categories of cases at DOJ.

C. More Concerted Effort To Prosecute Leaks

Proposed Reform:

The government could address leaks by simply increasing the frequency and intensity of leaks prosecutions under the current regime. Several mechanisms are available if the government chooses to pursue this option. The government could be more aggressive in bringing prosecutions under statutes other than the Espionage Act.[108] It could cast a wider net by increasing the pressure on non-Intelligence Community agencies that handle national security information to more fully participate in the DOJ referral process.[109] More invasive techniques are also available to help the government identify (and thereby deter) leakers. In fact, a DNI Press Release from June contemplates exactly such a measure by "mandating that a question related to unauthorized disclosure of classified information be added to the counterintelligence polygraph used by all agencies that administer the examination."[110] That same press release also identifies ways to increase coordination of leaks investigations by involving the Office of the Intelligence Community Inspector General (IC-IG) to lead a task force of IC inspectors general. This alternative mechanism was proposed to "ensure that selected unauthorized disclosure cases suitable for administrative investigations are not closed prematurely."[111] There is no reason why such a parallel process could not apply to criminal investigations as well. The WMD Report (written before a DNI Inspector General was named) suggested that IC-IG-led investigations

---

[104] *See* Neil A. Lewis, *Libby Guilty of Lying in C.I.A. Leak Case,* N.Y. TIMES (Mar. 6, 2007), http://www.nytimes.com/2007/03/06/washington/06cnd-libby.html?pagewanted=all.

[105] *In re* Sealed Case, 838 F.2d 476, 510 (1988), *rev'd sub nom.* Morrison v. Olson, 487 U.S. 654 (1988).

[106] According to Pozen, the "primary mechanism for triggering legal scrutiny of a leak is a referral process." Agencies can submit crime reports of suspected leaks to the DOJ. The DOJ then decides whether to open an investigation. Pozen, *supra* note 2, at 19. For some agencies within the Intelligence Community, this reporting is mandated by executive order, requiring that violations of federal law be reported to the DOJ. *See* Reno Testimony, *supra* note 43, at 3.

[107] Pozen, *supra* note 2, at 33, 59.

[108] *Id.* at 32. Specifically, Pozen notes that 18 U.S.C. § 641, the general theft and conversion statute, does not have a comparable scienter requirement to the Espionage Act.

[109] *Id.* at 33.

[110] Press Release, Office of the Director of National Intelligence, Director Clapper Announces Steps to Deter and Detect Unauthorized Disclosures (June 25, 2012), *available at* http://www.dni.gov/index.php/newsroom/press-releases/96-press-releases-2012/586-director-clapper-announces-steps-to-deter-and-detect-unauthorized-disclosures.

[111] *Id.*

would be particularly helpful when interagency coordination was required.[112] IGs are statutorily appointed and as such should exercise a degree of independence.[113] This would address some of the concerns that led to calls for the appointment of a special prosecutor.

Assessement:

Even if successful trial outcomes remain difficult for the reasons explored in Part II, the very act of aggressively seeking criminal penalties can still have a significant deterrent effect. However, the drawback of a more vigorous leaks-monitoring regime that focuses on sanctions to deter leaks is that it would also likely have a chilling effect that would be felt across the board. There is already evidence that the increase in FBI investigations, described as "a hunt for leakers," has "cast[] a distinct chill over press coverage of national security issues as agencies decline routine interview requests and refuse to provide background briefings" to the media.[114] This decrease in the number of interviews and briefings implicates both the First Amendment interests discussed in Part I and the interest in government transparency.

It is also not clear that increased enforcement will, in fact, lead to fewer leaks. In fact, Pozen argues that "more vigorous enforcement of the laws against leaking would lead to a *greater* amount of unlawful disclosures, or at least to a greater amount of destructive disclosures."[115] He suggests this is because "[a]n escalation in enforcement risks alienating those many officials who take the informal prohibitions on leaking seriously, corroding their feeling of stewardship over the secrecy system and unraveling cultural and psychological constraints on information sharing."[116]

There is no empirical research that links prosecution with greater or fewer leaks. But the notion that employees internalize the norms, including informal prohibitions, that the executive articulates can be extended to suggest that any increased enforcement should be accompanied by more transparent criteria for the types of leaks that are most likely to be investigated and prosecuted. Given the vast number of leaks that do occur, some of which benefit both the government and public, a prosecution regime that articulates the criteria for the types of leaks it considers most harmful and most likely to result in investigation and criminal sanctions may send clearer signals to government employees about which types of disclosure it is most important for them to avoid. Such an approach tracks the WMD Report, which found that "[p]olicymakers who leak intelligence to the press . . . may do so without fully appreciating the potential harm that can result to sources and methods," and recommended a "campaign to educate individuals about their legal obligations—and possible penalties."[117] Rather than risk alienating those whose cooperation is required to safeguard the nation's secrets, a more transparent procedure that is combined with "[b]etter education and training"[118] could put government employees on better notice of the government's priorities, which they would then be more likely to internalize.

---

[112] COMM'N ON THE INTELLIGENCE CAPABILITIES OF THE U.S. REGARDING WEAPONS OF MASS DESTRUCTION, REPORT TO THE PRESIDENT OF THE UNITED STATES 382-83 (2005) [hereinafter WMD Report].
[113] *See* GOLDSMITH, *supra* note 2, at 99, 105.
[114] Scott Shane, *Inquiry into U.S. Leaks Is Casting Chill Over* Coverage, N.Y. TIMES, Aug. 1, 2012, http://www.nytimes.com/2012/08/02/us/national-security-leaks-lead-to-fbi-hunt-and-news-chill.html.
[115] Pozen, *supra* note 2, at 68.
[116] *Id.* at 69.
[117] WMD Report, *supra* note 112, at 383.
[118] *Id.*

D. Increased Use of Administrative Sanctions

Proposed Reform:

A fourth option for addressing leaks would be to increase the use of administrative sanctions. Despite the relative ease of bringing administrative sanctions against government employees who leak classified information, most agencies do not systematically use this as a tool to prevent leaks.[119] Yet, the threat of job loss and the revocation of security clearance may serve as potent deterrents, and government reports as well as scholars have recommended that this tool be used more frequently.[120]

One of the impediments to increasing the use of administrative sanctions is the lack of an effective process for investigating leaks that have no chance of eventually resulting in criminal prosecutions. Mueller notes that the FBI is not involved in pursuing administrative actions beyond sharing the results of its investigations with the referring agency,[121] and recommends that these agencies consider involving their own "internal security divisions for possible administrative action."[122] The Willard Report goes further, recommending that FBI authority "should be clarified to include investigation of unauthorized disclosures of classified information under circumstances where the likely result of a successful investigation will be imposition of administrative sanctions rather than criminal prosecution."[123] Increased cooperation on these investigations through the IC-IG's office as contemplated by the DNI would also serve this purpose.[124]

Assessment:

Since administrative sanctions are easier for the government to impose than criminal prosecution, they may serve as a more effective way of "provid[ing] a large measure of deterrence."[125] The government also does not need to convince a court before it can impose administrative sanctions. Moreover, even if the matter ends up in litigation, the executive acts with greater capacity as an employer than as a prosecutor.[126]

Even though the government may exercise greater constitutional authority to impose administrative rather than criminal sanctions on leakers, the two are not wholly dissimilar in their impact. A job or security clearance loss can be devastating, and the incentives such a possibility creates are not much different from those imposed by the possibility of criminal sanctions—

---

[119] Pozen, *supra* note 2, at 21, 35.

[120] *See, e.g.*, WMD Report, *supra* note 112, at 383 (recommending "vigorous application of DNI administrative authorities" including "fines, suspension or revocation of clearances, or even firings"); Reno Testimony, *supra* note 43, at 14 ("[I]n general, we believe that the better way to address the problem of leaks is to try to prevent them through stricter personnel security practices . . . and through administrative sanctions, such as revocations of clearances."); Letter from John Ashcroft, *supra* note 42, at 3 ("A comprehensive, coordinated, Government-wide, aggressive, properly resourced, and sustained effort to address administratively the problem of unauthorized disclosures is a necessity.").

[121] Mueller Response, *supra* note 48, at 46.

[122] *Id.* at 47.

[123] Willard Report, *supra* note 91, at 21.

[124] *See supra* Section III.C for discussion of the DNI press release from June 25, 2012.

[125] Letter from John Ashcroft, *supra* note 42, at 3.

[126] *See supra* Section I.B.

except with the caveat that the latter can be significantly more severe.[127] Therefore, the caution about chilling legitimate and beneficial dialogue between the government and public—described in Part I—is an appropriate consideration here as well.

E. Creation of More Robust Internal Whistleblower Channels

Proposed Reform:

Another possible approach would be to create more robust internal whistleblower channels patterned on the State Department dissent channel. The dissent channel provides an avenue for "responsible dissenting and alternative views on substantive foreign policy issues that cannot be communicated in a full and timely manner through regular operating channels and procedures."[128] The dissent channel is controlled by the Secretary of State's Policy Planning Staff,[129] which remains outside the formal chain of command of the State Department and is thus ideally suited to intervene based on concerns raised through the channel. Use of the dissent channel is confidential, and the State Department provides clear assurances that an employee will not be retaliated against for raising any concerns through the channel.[130] Indeed, the State Department seems to foster a culture in which use of the channel is widely encouraged.[131]

Several government agencies already maintain Inspector General (IG) offices designed to provide an ombudsman-like function in monitoring the affairs of the agency.[132] Some IG offices are also charged with providing a forum for whistleblowers to air their concerns. For example, the CIA IG is "authorized to receive and investigate complaints or information from any person concerning the existence of an activity constituting a violation of laws, rules, or regulations, or mismanagement, gross waste of funds, abuse of authority, or a substantial and specific danger to the public health and safety."[133] If such a complaint is received, the IG must usually protect the employee's anonymity,[134] and the employee must be immune from reprisals by other Agency officials.[135]

---

[127] Thomas Drake apparently "agonized over the decision" by "research[ing] the relevant legal statutes and concluded that if he spoke to a reporter about unclassified matters the only risk he ran was losing his job." Mayer, *supra* note 17. Perhaps the possibility of spending time in prison would have been stronger deterrence in his case.

[128] *Dissent Channel*, AM. FOREIGN SERV. ASS'N, http://www.afsa.org/dissent_channel.aspx (last visited Dec. 2, 2012) (quoting the Foreign Affairs Manual's Dissent-Channel-related provisions).

[129] *Id.*

[130] *Id*. For a history of the dissent channel, see Hannah Gurman, *The Other Plumbers Unit: The Dissent Channel of the U.S. State Department*, 35 DIPL. HIST. 321 (2011). Fourteen dissents were filed through the dissent channel during President Obama's first year in office. Glenn Kessler, *State Department Honors Three with 'Constructive Dissent' Awards*, WASH. POST, June 25, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/06/24/AR2010062406294.html.

[131] Kessler, *supra* note 130 (describing the use of awards to "encourage Foreign Service officers to speak out if they think U.S. policy is going in the wrong direction").

[132] For example, the CIA IG is charged with "initiat[ing] and conduct[ing] independent inspections, investigations, and audits relating to programs and operations of the Agency." 50 U.S.C. § 403q(a)(1) (2006).

[133] *Id*. at § 403q(e)(3).

[134] *Id.* at § 403q(e)(3)(A) ("[T]he Inspector General shall not disclose the identity of the employee without the consent of the employee, unless the Inspector General determines that such disclosure is unavoidable during the course of the investigation or the disclosure is made to an official of the Department of Justice responsible for determining whether a prosecution should be undertaken.")

[135] *Id.* at § 403q(e)(3)(B). This comes with the caveat that anyone who reports information "with the knowledge that it was false or with willful disregard for its truth or falsity" will receive no protection from reprisal. *Id*.

While it would seem that IGs a role similar to that of the dissent channel, it is unclear to what extent government agencies have provided mechanisms to facilitate direct contact between employees and IG offices. For example, the CIA is required by statute to provide the Inspector General's contact information on its internal website,[136] but no direct and easy-to-access avenue, like the dissent channel, seems to exist.[137] Some scholars have even claimed the CIA IG is ineffective as a place for would-be whistleblowers to turn to, reporting that leakers often prefer to take their grievances to the press rather than working through the IG.[138] Indeed, most of the office's major investigations began only after whistleblowers had already leaked information to the press.[139] While none of these problems foreclose the potential for the IG's office to provide a useful internal authority for would-be leakers to turn to, they underscore the fact that such offices will only prove successful if employees consider them effective and trustworthy.

Assessment:

The State Department's dissent channel provides a promising model for bolstering U.S. government employees' faith in internal whistleblower mechanisms. To the extent that leaks are often a result of employees who believe that they have no recourse left except to leak information to the outside world, the dissent channel model might provide a useful mechanism for channeling employee discord into internal government processes. Indeed, Pozen has argued that the dissent channel should be replicated in other Departments, claiming that it could reduce temptation for disgruntled employees to "take their grievances to the outside world."[140]

Implementing the model in other departments could help foster greater sentiment that internal whistleblower channels are safe and effective. This, in turn, might deter some leakers from going to the press.[141] The dissent channel model could be implemented to better funnel would-be leakers to preexisting Inspector General offices or used in conjunction with other impartial offices (like the Director of Policy Planning at the State Department). Either way, the model could help create easier-to-access whistleblowing avenues for employees, and help foster broader workplace cultures in which internal whistleblowing is commended and encouraged.[142]

It is important to note that greater use of the dissent channel model may not necessarily overcome government employees' inherent suspicion of internal whistleblower mechanisms.

---

[136] *Id.* at § 403q(h)(1).

[137] It is possible the CIA has already created additional mechanisms (apart from simply providing the IG's email address on its internal website) to encourage would-be whistleblowers to seek out the IG's office. If that is the case, the CIA has not made this information publicly available.

[138] Richard Moberly, *Whistleblowers and the Obama Presidency: The National Security Dilemma*, 16 EMP. RTS. & EMP. POL'Y J. 51, 124 (2012).

[139] Ryan M. Check & Afsheen John Radsan, *One Lantern in the Darkest Night: The CIA's Inspector General*, 4 J. NAT'L SECURITY L. & POL'Y 247, 287 (2010).

[140] David E. Pozen, *Deep Secrecy*, 62 STAN. L. REV. 257, 337 (2010) ("And broader use of mechanisms such as the 'Dissent Channel' can help elevate the perception of internal dissent to a kind of civic contribution, rather than a deviant practice. This inversion might ironically be good for the maintenance of secrecy, as well as for the quality of governance, because disaffected employees who lack a Dissent Channel may find it more tempting to take their grievances to the outside world."). For a general discussion of the dissent channel model, focusing especially on its potential ability to foster a better-functioning and more competent civil service, see Neal Kumar Katyal, *Internal Separation of Powers: Checking Today's Most Dangerous Branch from Within*, 115 YALE L.J. 2314, 2328-29 (2006).

[141] Pozen notes that in some of the most famous leak cases, individuals only went to the press after trying and failing to take their case directly to Congress through internal channels. Pozen, *supra* note 2, at 54 n.298.

[142] USAID recently created its own dissent channel, modeled after the State Department's version. Francisco Zamora, *Dissent: USAID's New Dissent Channel*, FOREIGN SERVICE J., Jan. 2012, at 52.

Such structures will only function as an alternative to leaking if employees feel their concerns are being taken seriously and acted upon.[143] Experts have noted that "most classified information leakers are either uninterested in availing themselves of the prescribed whistleblower channels or do not trust that they will prove safe or effective."[144]

Furthermore, many of the values described in Part I involve greater *public* scrutiny of executive decision-making. Reporting mechanisms internal to the executive branch may create some oversight, but they neither shed the same bright light on government action, nor do they contribute to the good generated from a well-informed public.

Finally, an internal reporting mechanism would likely not dissuade leakers who have a desire to inflict damage on the U.S. government. It would also not dissuade those who feel they are acting in the government's interest by leaking information they are implicitly authorized to disseminate. Therefore, while a dissent channel may provide internal avenues for some would-be leakers and may create a culture where potential whistleblowers believe their concerns will be taken seriously by their agency, such a solution will not clamp down on all leaks or leakers.

CONCLUSION

None of the proposals evaluated herein will completely deter all leakers or stop all leaks. Nor should it. This is not a result of a failing national security system, but rather a consequence of a functioning system that has to balance multiple, competing interests. Within these constraints, it appears that a targeted approach that provides clear notice to government employees as to what behavior the government considers most destructive and not to be tolerated, and that creates alternative mechanisms for internal reporting, will best serve the purpose of reducing unauthorized leaking.

[143] This concern is especially relevant if a dissent channel model used to funnel would-be leakers to IGs offices (rather than alternative oversight offices). If IGs also maintain a role in prosecuting leaks, *see supra* Section III.C, it is possible that would-be leakers would feel uncomfortable taking their concerns to IGs. The risk of IGs playing this dual role is that the dissent channel may come to be viewed as a mechanism to keep tabs on employees by the office also be charged with investigating them. To reap the rewards of a well-functioning dissent channel, as well as the perception that the government takes its employees concerns seriously, it would be important for the agencies, at a minimum, to clearly stipulate that nothing told to an IG by a would-be whistleblower can be used against that employee during a potential future prosecution.

[144] Pozen, *supra* note 2, at 11 n.52 (citing Interview with Steven Aftergood, Dir., Project on Gov't Secrecy, Federation of Am. Scientists, in Washington, D.C. (Apr. 10, 2012)).