CAN TECHNOLOGY PREVENT LEAKS?

Nathan Alexander Sales*

The past decade has witnessed an unprecedented explosion in leak prosecutions. Since 2005, the government has charged leakers with violating the Espionage Act of 1917—which makes it a crime for government employees to reveal national defense information to persons not entitled to receive it[1]—ten times, including no fewer than nine prosecutions since President Obama took office in 2009. This prosecutorial surge stands in sharp contrast to the two Espionage Act cases brought in three quarters of a century after Congress enacted that World War I-era statute. Yet this dramatic jump in prosecutions does not appear to have corresponded with a comparably dramatic decline in the number of leaks that have occurred or in their severity. Government officials at all levels continue to reveal highly classified information routinely, from the senior administration officials who disclosed President Obama's personal role in selecting targets for drone strikes to low-level employees like Bradley (now Chelsea) Manning and Edward Snowden who exfiltrated huge troves of diplomatic, military, and intelligence documents. "[L]eaking classified information occurs so regularly in Washington" that it has become "a routine method of communication about government."[2]

Why? Part of the answer, I think, is that criminal prohibitions on leaking are fairly modest deterrents, especially for ideologically motivated leakers who seek to disclose large tranches of classified documents. The law attempts to deter undesirable conduct through commands backed by threats of punishment; the greater the magnitude of the sanctions, and the greater the probability those sanctions will be imposed, the less likely it is that people will commit the proscribed offense. But that familiar framework has its limits when it comes to leaks. The penalties for government employees who reveal classified information to outsiders are relatively modest, and the fraction of leaks that have resulted in legal liability over the years is so slight that the threat of punishment is hardly credible. In economic terms, the expected penalty for leaking is vanishingly small—too small, in many instances, to deter.

This essay, which is based on remarks presented at a symposium hosted by the Georgetown Center on National Security and the Law on February 25, 2014, seeks to stimulate thought about alternative, non-legal ways of preventing leaks. Its claim is that, in addition to the

---

* Associate Professor of Law, Syracuse University College of Law. Special thanks for helpful comments from Derek Bambauer, Laura Donohue, Mary-Rose Papandrea, David Pozen, Peter Shane, Peter Swire, and Steve Vladeck.

[1] 18 U.S.C. § 793(d) (2012).

[2] William E. Lee, *Deep Background: Journalists, Sources, and the Perils of Leaking*, 57 AM. U. L. REV. 1453, 1467 (2008); *see also* David Pozen, *The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information*, 127 HARV. L. REV. 512, 528–30 (2013) (describing prevalence of leaks).

threat of legal liability, authorities should make greater use of technological measures that block leaks from happening. The intelligence community is, of course, already using technology to protect classified information, but additional safeguards and more elaborate versions of existing ones might bear fruit. For instance, computer systems should be built with more stringent access controls that limit which employees may access what information for which purposes (including biometric identity verification), audit logs that create permanent records of users' system activity, and automated processes that monitor for suspicious patterns of behavior that might indicate an attempt to exfiltrate protected data. At the same time, these systems should preserve analysts' ability to share information with one another and policymakers' ability to promote democratic deliberation by revealing otherwise protected information to the public. And because technology is capable of preventing disclosures that on balance are worthwhile—that is, leaks whose promotion of privacy, accountability, and rule-of-law values outweighs any national security harms—these controls should be paired with reforms that address the persistent problem of over-classification, more meaningful whistleblower protections for military and intelligence officials, and other mechanisms that can achieve some of the same benefits of leaks.

A few initial observations will set the stage for the analysis that follows. Technology is simply a way of operationalizing normative judgments. This essay is largely descriptive, but it rests on a prior normative assumption—that the government *should* try to prevent certain catastrophic leaks of classified information that will result in grave national security harms without producing net social benefits. Examples could include revealing troop locations, thereby compromising their operations or enabling enemy forces to attack them; publicizing the identities of covert assets, thereby exposing them to capture and perhaps death; or disclosing the technical details of sensitive weapons systems, thereby enabling adversaries to develop countermeasures or to reverse engineer them for their own use. Reasonable minds can disagree on where to draw the line that separates the harmful leaks from the beneficial ones, but this essay takes no position on where that boundary lies, and the reader need not either. It is enough to agree that there is *some* category of classified information whose compromise the government has a legitimate interest in preventing. Moreover, the need to block some leaks does not imply the propriety of blocking them all. The goal should be optimal protection for classified information, not maximum protection (where optimality is a function of a given disclosure's national security harm, the public's interest in the information, and other factors whose balancing is beyond the scope of this essay).

To be precise, my claim is that technology should supplement rather than replace more traditional legal controls. Laws against leaking plainly have some deterrent effect; it's safe to assume that the Espionage Act has dissuaded an unknown but not negligible number of intelligence officials from revealing classified information to journalists.[3] Still, it seems unlikely that the law will be decisive in the cases where the stakes are the highest—where resourceful and motivated leakers seek, because of ideological concerns or for other principled reasons, to reveal classified information of the utmost sensitivity. Manning and Snowden were not cowed by the threat of jail time, even amid the widely publicized and highly salient Obama-era surge in leak

[3] *See, e.g.*, Mary-Rose Papandrea, *Leaker Traitor Whistleblower Spy: National Security Leaks and the First Amendment*, 94 B.U. L. REV. 449, 462–63 (2014) (describing chilling effect of recent Espionage Act prosecutions on willingness of some government officials to "discuss sensitive topics" with reporters).

prosecutions.[4] If nothing else, criminal prohibitions are valuable to the extent they reinforce the cultural norms against leaking among military and intelligence professionals. Even if criminal sanctions are an imperfect way of regulating leaks, there are still good reasons to keep them on the books.

Finally, technology seems better suited to the problem of low-level documentary leaks than high-level oral ones. Access controls, audit trails, and similar measures may keep intelligence analysts from downloading classified documents onto thumb drives and turning them over to reporters. But they would leave essentially unregulated the oral disclosures that senior officials routinely use to inform the public, send a signal to a foreign adversary, and so on. These disclosures are an important mechanism for informing the public, but we should not discount the grave national security harms that can result when senior officials leak to appear "in the know," to embarrass bureaucratic rivals, to boast about successful operations, or for other discreditable reasons—think of the senior State Department official who compromised the identity of CIA operative Valerie Plame after her husband criticized the run-up to the Iraq War, and the unnamed officials who confirmed that the United States was behind the Flame and Stuxnet viruses that disabled Iran's uranium enrichment facilities (thereby perhaps legitimizing other nations' use of destructive malware). Technology cannot easily solve this "Plame and Flame" problem.

Part I of this essay describes the legal instruments the government uses to regulate leaks, as well as the constitutional principles that constrain their application. In Part II, I argue that laws against leaking are modest deterrents because the expected penalty for disclosing classified information normally will be quite small. Part III discusses the use of technology to prevent leaks.

I. The Legal Framework

There are two broad categories of possible responses to leaks. First, on the supply side, the government might restrict officials from revealing secrets with which they have been entrusted. For instance, it might prosecute employees who leak classified information or enter contractual arrangements that bind employees to secrecy. Second, on the demand side, the government might restrict leak recipients from distributing the classified information they have received. It might file criminal charges against the press, either on the theory that the journalist conspired with the leaker to unlawfully reveal protected information[5] or that publishing the data

[4] The Obama administration's robust enforcement of the Espionage Act probably has increased the expected sanction for leaking, but perhaps not enough to make much difference. Given the many thousands of leaks that have gone unpunished over the years, the chances that a particular disclosure will be prosecuted will remain quite small—12 divided by, say, 100,000 is a larger fraction than 3/100,000, but not by much.

[5] *See*, *e.g.*, Ann E. Marimow, *A Rare Peek into a Justice Department Leak Probe*, WASH. POST, May 19, 2013 (recounting the Justice Department's claim, in a search warrant application, that a journalist who reported classified information about North Korea's nuclear weapons program was "an aider, abettor and/or co-conspirator" of the leaker).

is an independent crime.[6] Alternatively, the government might ask a court to issue an injunction that bars the media from publishing the material—i.e., a prior restraint.[7] The demand-side approach, of course, is fraught with both constitutional and statutory difficulties,[8] and this essay focuses largely on the supply-side constraints, legal and otherwise.

A. Criminal Law

Unlike the United Kingdom, this country has no Official Secrets Act—a comprehensive charter that authorizes a range of criminal sanctions for government employees, journalists, and citizens who leak, publish, or possess classified information.[9] Yet we have a junior varsity version in the Espionage Act of 1917.[10] Section 793(d) of that statute makes it a crime for a government official to "willfully communicate[], deliver[], [or] transmit[]" any "information relating to the national defense" to "any person not entitled to receive it," if the official "has reason to believe" that the information "could be used to the injury of the United States or to the advantage of any foreign nation."[11] Violations are punishable by jail terms of up to ten years.[12] The Espionage Act plainly applies to spies who share secrets with hostile foreign governments. Courts have held that it also applies to employees who leak secrets to the press.

The leading case is *United States v. Morison*.[13] Samuel Loring Morison was a U.S. Navy intelligence officer who provided *Jane's Defence Weekly*, a British magazine, with classified satellite imagery of a new Soviet aircraft carrier in 1984.[14] Morison later claimed that he leaked the photographs to alert the public to alarming Soviet military capabilities and prod Congress to increase the Navy's budget, but it's more likely he was angling for a full-time job at *Jane's*.[15] Charged with violating section 793(d) along with several other laws, Morison's primary defense was that the Espionage Act "was intended to punish only 'espionage' in the classic sense of divulging information to agents of a hostile foreign government and not to punish the 'leaking' of classified information to the press."[16] The district court rejected Morison's argument, he was

---

[6] *See, e.g.*, GABRIEL SCHOENFELD, NECESSARY SECRETS: NATIONAL SECURITY, THE MEDIA, AND THE RULE OF LAW 249–54 (2010) (arguing that journalists could be prosecuted for publishing leaked information).

[7] *See, e.g.*, N.Y. Times Co. v. United States, 403 U.S. 713 (1971); United States v. The Progressive, 486 F. Supp. 5 (W.D. Wisc. 1979).

[8] *See, e.g.*, *N.Y. Times*, 403 U.S. at 715–17 (Black, J., concurring); Harold Edgar & Benno C. Schmidt, Jr., *The Espionage Statutes and Publication of Defense Information*, 73 COLUM. L. REV. 929 (1973).

[9] Official Secrets Act, 1989, c.6 (U.K.).

[10] 18 U.S.C. §§ 792–99 (2012).

[11] *Id*. § 793(d).

[12] *Id*. § 793.

[13] 604 F. Supp. 655 (D. Md. 1985), *aff'd*, 844 F.2d 1057 (4th Cir. 1988).

[14] *Morison*, 844 F.2d at 1061.

[15] *Id*. at 1062.

[16] *Morison*, 604 F. Supp. at 657.

found guilty, and the Fourth Circuit affirmed his conviction. (Years later Morison would receive a presidential pardon.[17])

According to the appellate court, the notion that the Espionage Act applies to leakers follows from the plain language of the statute. "[T]he statutes themselves, in their literal phrasing, . . . plainly apply" to leaks. The statutory language "includes no limitation to spies or to an agent of a foreign government," and it "declare[s] no exemption in favor of one who leaks to the press. It covers 'anyone.'"[18] The Fourth Circuit also emphasized the act's structure. Unlike section 794—a related provision that specifically prohibits disclosures "to any foreign government"[19]—section 793(d) more broadly prohibits revealing national-defense information "to *any person* not entitled to receive it."[20] The implication is that Congress meant for these provisions to cover two "separate and distinct" crimes. "[S]ection 793(d) was not intended to apply narrowly to 'spying' but was intended to apply to disclosure of the secret defense material to *anyone* 'not entitled to receive' it, whereas section 794 was to apply narrowly to classic spying."[21] Finally, leakers can be held liable under the Espionage Act because of Congress's purpose in enacting the statute. According to the district court, Congress's goal was to prevent the nation's most sensitive secrets from falling into the hands of hostile foreign powers.[22] And that harm materializes whether a foreign power learns of a secret directly from a spy or indirectly by reading about it in the newspaper. "[T]he danger to the United States is just as great when this information is released to the press as when it is released to an agent of a foreign government."[23]

What about the Constitution? The Fourth Circuit rejected Morison's claim that the First Amendment bars the government from applying the Espionage Act to leakers. Two of the panel members believed that the case raised significant constitutional issues, not so much because of a leaker's interest in speaking but the public's corresponding interest in hearing.[24] According to Judge Wilkinson, "[c]riminal restraints on the disclosure of information threaten the ability of the press to scrutinize and report on government activity," and public debate "is diminished without access to unfiltered facts."[25] Judge Phillips went even further, arguing that the First Amendment requires the government to show that the leaked information was both classified and "*in fact* 'potentially damaging . . . or useful'" to an adversary, a question on which "the fact of classification is merely probative, not conclusive."[26] Nevertheless, the court squarely (albeit in a

---

[17] Vernon Loeb, *Clinton Ignored CIA in Pardoning Intelligence Analyst*, WASH. POST, Feb. 17, 2001.

[18] *Morison*, 844 F.2d at 1063 (some internal quotation marks omitted).

[19] 18 U.S.C. § 794(a) (2012).

[20] *Id*. § 793(d) (emphasis added).

[21] *Morison*, 844 F.2d at 1065.

[22] *Morison*, 604 F. Supp. at 660.

[23] *Id.* at 660.

[24] *Morison*, 844 F.2d at 1081, 1083 (Wilkinson, J., concurring); *id*. at 1085 (Phillips, J., concurring).

[25] *Id*. at 1081 (Wilkinson, J., concurring).

[26] *Id*. at 1086 (Phillips, J., concurring).

conclusory way) held that a government employee who reveals protected information "is not entitled to invoke the First Amendment as a shield to immunize his act of thievery." To hold otherwise "would be to prostitute the salutary purposes of the First Amendment."[27]

B. Contract Law

The Espionage Act may be the best-known legal constraint on leaks, but the government also uses contract law to prevent disclosures of classified information. Intelligence and military officials whose jobs require access to classified information typically sign secrecy agreements when they are hired. The modern version, known as SF-312,[28] contains a straightforward nondisclosure requirement: "I will never divulge classified information to anyone" unless authorized to do so. A separate agreement (SF-4414)[29] signed by those with access to highly classified "Sensitive Compartmented Information," or SCI, additionally requires prepublication review. Employees must allow their agencies to inspect any writings before they appear in print to see if they contain protected information, and they may not publish unless they receive written authorization. Prepublication review normally takes 30 days. If an employee is dissatisfied with the results, he may pursue various administrative appeals,[30] then seek (limited) judicial review.[31] Both contracts "assign to the United States Government" all proceeds resulting from any unauthorized disclosures, and both specify that their requirements apply for the period of employment "and at all times thereafter."

The Supreme Court in *Snepp v. United States*[32] and the Fourth Circuit in *United States v. Marchetti*[33] both held that these sorts of secrecy agreements are enforceable. *Marchetti* involved a CIA employee who, when he joined the agency in 1955, signed a contract promising not to "divulge, publish, or reveal . . . any classified information" unless authorized to do so.[34] Despite this pledge, after his 1969 resignation, Marchetti published a novel and several magazine articles that were alleged to contain classified information.[35] The government filed suit, alleging breach of contract. The district court held that Marchetti had violated his contractual duties and ordered him to submit his writings to the CIA for prepublication review; the Fourth Circuit affirmed.[36]

---

[27] *Id.* at 1069–70.

[28] GOV'T SERV. ADMIN., SF-312 NONDISCLOSURE AGREEMENT (2013), *available at* http://www.gsa.gov/portal/getFormFormatPortalData.action?mediaId=65765.

[29] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, NAT'L COUNTERINTELLIGENCE AND SEC. CTR., SF-4414 NONDISCLOSURE AGREEMENT (2013), *available at* http://www.ncix.gov/SEA/docs/FORM_4414_Rev_12_2013.pdf.

[30] CENT. INTELLIGENCE AGENCY, DOCID 1512158, AGENCY PREPUBLICATION REVIEW OF CERTAIN MATERIAL PREPARED FOR PUBLIC DISSEMINATION (May 30, 2007), *available at* https://www.fas.org/irp/cia/prb2007.pdf.

[31] *See infra* notes 39–40 and accompanying text.

[32] 444 U.S. 507 (1980).

[33] 466 F.2d 1309 (4th Cir. 1972).

[34] *Id*. at 1312 n.1.

[35] *Id*. at 1313.

[36] *Id*. at 1311.

The appellate court emphasized that Marchetti acquired the information he now sought to reveal—namely, "secret information touching upon the national defense and the conduct of foreign affairs"—"while in a position of trust and confidence," and that he was "contractually bound to respect it."[37] Nor did the First Amendment excuse Marchetti's conduct. Even though the secrecy agreement operated as a prior restraint on speech, and therefore bore a heavy presumption of invalidity, it was ultimately consistent with the First Amendment. The court surveyed various precedents on the need for secrecy in national security and foreign affairs, concluding that the nondisclosure requirement was "a [r]easonable [m]eans" of protecting these secrets.[38] It emphasized that, "since First Amendment rights are involved," employees are entitled to judicial review of an agency's decision to disapprove publication.[39] Yet that review is quite "limited": courts may not assess whether classification was proper, but are confined to the questions "whether or not the information was classified and, if so, whether or not, by prior disclosure, it had come into the public domain."[40]

Snepp arose out of similar facts. When Frank W. Snepp III took a job at the CIA in 1968, he signed a secrecy agreement with a pair of complementary promises: he would neither reveal classified information nor publish any writings without first obtaining the CIA's permission. "Thus, Snepp had pledged not to divulge *classified* information and not to publish *any* information without prepublication clearance."[41] After leaving the CIA in 1976, Snepp wrote a book about the CIA's involvement in the Vietnam War without allowing agency officials to review the manuscript. The government conceded that Snepp's book contained no classified information,[42] but it nevertheless filed suit to enforce Snepp's separate contractual obligation to submit his writings for prepublication review.

In a per curiam opinion, the Supreme Court upheld the prepublication review requirement. "Whether Snepp violated his trust does not depend upon whether his book actually contained classified information."[43] Instead, quite apart from its need to prevent leaks, the government has a legitimate interest in screening unpublished manuscripts for classified information. The Court suggested that the absence of prepublication review would make it harder to work with covert assets and foreign intelligence officials, both of whom understandably would worry about the United States's ability to keep their confidences.[44] The Court went on to address Snepp's primary claim—"that his agreement is unenforceable as a prior restraint on protected speech"—in an oblique and cursory way, holding that the nondisclosure and

[37] *Id*. at 1313.

[38] *Id*. at 1315–17.

[39] *Id*. at 1316.

[40] *Id*. at 1318.

[41] 444 U.S. at 508.

[42] *Id*. at 510.

[43] *Id*. at 511.

[44] *Id*. at 511–13.

prepublication review requirements are "entirely appropriate" means of protecting intelligence sources and methods.[45] (The majority's First Amendment analysis was not especially rigorous, but it did not provoke much objection from the three dissenters.[46])

Turning to the question of remedy, the Court approved a constructive trust on Snepp's earnings from the book. Snepp's publisher had already paid him a $60,000 advance—the equivalent of about $170,000 in 2015 dollars—and he stood to receive various other royalties as well.[47] At the time, the applicable secrecy agreement contained no mechanism for the government to recoup profits from faithless employees.[48] The Court nevertheless approved a constructive trust on the theory that it would serve the interests of both parties. From the government's standpoint, a trust would achieve deterrence. "Since the remedy is swift and sure, it is tailored to deter those who would place sensitive information at risk."[49] And, unlike the alternative of a tort lawsuit seeking compensatory and punitive damages, a trust wouldn't require the government to introduce evidence of the national security harms resulting from a leak, thereby potentially compromising the very secrets it sought to protect.[50] As for Snepp, a constructive trust would cap his damages at his profits from the book, thereby insulating him from potentially ruinous liability.[51] (The majority's improvised remedy was the principal concern of the dissent, which argued that the trust "is not supported by statute, by the contract, or by the common law."[52])

II. The Law's Effectiveness

Gary Becker's familiar economic account of the criminal law proposes that the law's ability to deter undesirable conduct is a function of, among other variables, the conduct's expected sanction—i.e., the severity of the applicable penalties discounted by the probability that they will be imposed.[53] To strengthen a given law's deterrent effect, policymakers may either increase the sanctions for violating it or increase the likelihood that violators will be caught and punished (although more recent scholarship has suggested that criminals may be more sensitive to heightened chances of enforcement than to more severe sanctions).[54] Similar economic

---

[45] *Id*. at 509 n.3.

[46] *See id*. at 526 n.17 (Stevens, J., dissenting) ("In view of the national interest in maintaining an effective intelligence service, I am not prepared to say that [prepublication review] is necessarily intolerable in this context.").

[47] *Id*. at 508 n.2.

[48] Both modern agreements "assign to the United States Government" any gains from unauthorized disclosures, effectively codifying *Snepp*. *See* SF-312, *supra* note 28; SF-4414, *supra* note 29.

[49] *Snepp*, 444 U.S. at 515.

[50] *Id*. at 514.

[51] *Id*. at 516.

[52] *Id*. at 517 (Stevens, J., dissenting).

[53] Gary A. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169, 176–79 (1969).

[54] *See*, *e.g.*, Dan M. Kahan, *Social Influence, Social Meaning, and Deterrence*, 83 VA. L. REV. 349, 379–80 (1997).

accounts exist for torts[55] and breaches of contracts.[56] Yet this theory of deterrence has its limits when it comes to leaks. The criminal and civil penalties for leaking classified information are relatively modest, especially when compared to the harms that can result from truly catastrophic disclosures, and the likelihood that a given leaker will be sanctioned is vanishingly small.

A. Criminal Law

Consider first the ability of the Espionage Act and similar criminal statutes to deter leaks. Statistically speaking, it is highly unlikely that the government will investigate or prosecute a given disclosure at all, let alone obtain a conviction, and the low probability of punishment substantially weakens the law's deterrent effect. Scholars have estimated that the indictment rate for leakers is "below 0.3%" and "probably far closer to zero."[57] (Part of the reason this fraction is so small is that the denominator includes a large number of minor leaks that cause such negligible harm that the government deems them unworthy of prosecution. But, as discussed below, even grave breaches often escape prosecution.[58]) Indeed, depending on how you count,[59] the government has charged leakers just twelve times over the century-long lifespan of the Espionage Act, with ten of those prosecutions coming since 2005 and nine since President Obama took office in 2009.[60]

If the leaks that are investigated and charged represent only a small fraction of all disclosures, the percentage of leaks that result in criminal liability is smaller still. Six of the twelve cases resulted in prison terms (usually through plea agreements rather than trials), four did not, and two are still pending as of this writing. The cases and their dispositions are as follows:

- Daniel Ellsberg, 1971. Defense Department analyst charged with leaking the Pentagon Papers to the *New York Times* and other publications. The presiding judge declared a mistrial and all charges were dropped.[61]

---

[55] *See*, *e.g.*, A. Mitchell Polinsky & Steven Shavell, *Punitive Damages: An Economic Analysis*, 111 HARV. L. REV. 870 (1998).

[56] *See, e.g.*, RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 118–30 (7th ed. 2007); Oren Bar-Gill & Omri Ben-Shahar, *An Information Theory of Willful Breach*, 107 MICH. L. REV. 1479 (2009).

[57] Pozen, *supra* note 2, at 536 (citing GARY ROSS, WHO WATCHES THE WATCHMEN? THE CONFLICT BETWEEN NATIONAL SECURITY AND FREEDOM OF THE PRESS (2011)).

[58] *See infra* notes 73–80 and accompanying text.

[59] *See* Pozen, *supra* note 2, at 534–35 (describing other leak cases normally excluded from the canonical list).

[60] In mid-2012, the numbers stood at nine, seven, and six. *See* Scott Shane & Charlie Savage, *Administration Took Accidental Path to Setting Record for Leak Cases*, N.Y. TIMES, June 19, 2012; Charlie Savage, *Nine Leak-Related Cases*, N.Y. TIMES, June 20, 2012. Authorities have since pursued three more cases. *See* Peter Finn & Sari Horwitz, *U.S. Charges Snowden with Espionage*, WASH. POST, June 21, 2013; Charlie Savage, *Former F.B.I. Agent to Plead Guilty in Press Leak*, N.Y. TIMES, Sept. 23, 2013; Michael S. Schmidt & Matt Apuzzo, *David Petraeus Is Sentenced to Probation in Leak Investigation*, N.Y TIMES, Apr. 23, 2015.

[61] *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#gallery-top.

- Samuel Morison, 1985. Navy intelligence analyst charged with leaking satellite images to *Jane's Defence Weekly*. Convicted and sentenced to two years in prison; pardoned in 2001.[62]
- Lawrence Franklin, 2005. Defense Department analyst charged with leaking information about Iran to lobbyists. Pleaded guilty and sentenced to 12.5 years in prison; sentence later reduced to 10 months of house arrest.[63]
- Shamai Leibowitz, 2009. FBI contractor charged with leaking documents about communications intelligence activities to a blogger. Pleaded guilty and sentenced to 20 months in prison.[64]
- Thomas Drake, 2010. NSA official charged with retaining national defense information after leaking documents about agency mismanagement to a *Baltimore Sun* reporter. Pleaded guilty to a misdemeanor charge of unauthorized use of a computer, and sentenced to one year of probation and community service.[65]
- Stephen Kim, 2010. State Department contractor charged with leaking information about North Korea's nuclear weapons program to *Fox News*. Pleaded guilty and sentenced to 13 months in prison.[66]
- Bradley Manning, 2010. Army intelligence analyst charged with leaking a large trove of military and diplomatic documents to WikiLeaks, an anti-secrecy organization. Convicted in a court-martial and sentenced to 35 years in prison. Eligible for parole after seven years.[67]
- Jeffrey Sterling, 2010. CIA officer charged with leaking information about efforts to thwart Iran's nuclear weapons program to a *New York Times* reporter. Convicted and scheduled to be sentenced on May 11, 2015.[68]
- John Kiriakou, 2012. CIA officer charged with leaking information about an operative involved in interrogating suspected terrorists to a *New York Times* reporter. Pleaded guilty and sentenced to 2.5 years in prison.[69]

---

[62] Michael Wright & Caroline Rand Herron, *Two Years for Morison*, N.Y. TIMES, Dec. 8, 1985; *see also supra* notes 13–17 and accompanying text.

[63] Jerry Markon, *Defense Analyst Guilty in Israeli Espionage Case*, WASH. POST, Oct. 6, 2005; Jerry Markon, *Nation Digest: Sentence Reduced in Pentagon-AIPAC Case*, WASH. POST, June 12, 2009. In addition to the leaker, the government also filed charges against the lobbyists who received the information, Steven Rosen and Keith Weissman. *See* United States v. Rosen, 447 F. Supp. 2d 538 (E.D. Va. 2006). These charges ultimately were dismissed. Neil A. Lewis & David Johnston, *U.S. to Drop Spy Case Against Pro-Israel Lobbyists*, N.Y. TIMES, May 1, 2009.

[64] Maria Glod, *Former FBI Employee Sentenced for Leaking Classified Papers*, WASH. POST, May 25, 2010.

[65] Ellen Nakashima, *Ex-NSA Official Thomas Drake to Plead Guilty to Misdemeanor*, WASH. POST, June 9, 2011; Scott Shane, *No Jail Time in Trial Over N.S.A. Leak*, N.Y. TIMES, July 15, 2011.

[66] Ann E. Marimow, *Ex-State Department Adviser Stephen J. Kim Sentenced in Leak Case*, WASH. POST, Apr. 2, 2014.

[67] Julie Tate, *Bradley Manning Sentenced to 35 Years in WikiLeaks Case*, WASH. POST, Aug. 21, 2013.

[68] Matt Zapotosky, *Federal Prosecutors Urge "Severe" Sentence for Ex-CIA Officer in Leak Case*, WASH. POST, Apr. 21, 2015.

[69] Justin Jouvenal, *Former CIA Officer John Kiriakou Is Sentenced to 30 Months in Prison for Leaks*, WASH. POST, Jan. 25, 2013; Greg Miller, *Former CIA Officer Charged in Leaks Case*, WASH. POST, Jan. 23, 2012.

- Donald Sachtleben, 2013. FBI agent charged with leaking information about a foiled plot by Yemeni terrorists to bomb commercial airliners to the *Associated Press*. Pleaded guilty and sentenced to 3.5 years in prison.[70]
- Edward Snowden, 2013. NSA contractor charged with leaking a large trove of documents about surveillance programs to a number of reporters. Case is currently pending in the Eastern District of Virginia.[71]
- David Petraeus, 2015. Retired general and former CIA director accused of sharing notebooks containing classified information with his biographer/mistress. Pleaded guilty to a misdemeanor charge of mishandling classified materials, sentenced to two years of probation and a $100,000 fine.[72]

Of the countless leaks since the Espionage Act went into effect, only six have resulted in jail time.

Just as important are the disclosures that did not result in prosecutions. Even notorious leaks are unlikely to see criminal charges. Here are just a few recent examples of well-known leaks whose authors have escaped liability:

- The identity of a Pakistani doctor who helped the CIA track down Osama bin Laden in Abbottabad, Pakistan.[73]
- The government's procedures for selecting targets for drone strikes, including President Obama's personal participation in the decisions,[74] as well as the content of a Justice Department memo concluding that the government lawfully may target certain American citizens.[75]
- The role of the United States and Israel in developing two pieces of malware, Stuxnet and Flame, that were designed to disable Iran's nuclear weapons program.[76]
- The identity of Valerie Plame, a CIA employee, during the run-up to the 2003 Iraq War.[77]

---

[70] Savage, *Former F.B.I. Agent*, *supra* note 60.

[71] Finn & Horwitz, *supra* note 60.

[72] Schmidt & Apuzzo, *supra* note 60.

[73] Mark Mazzetti, *Vaccination Ruse Used in Pursuit of Bin Laden*, N.Y. TIMES, July 11, 2011; *see also* Richard Leiby & Peter Finn, *Pakistani Doctor Who Helped CIA Hunt for bin Laden Sentenced to Prison for Treason*, WASH. POST, May 23, 2012.

[74] Jo Becker & Scott Shane, *Secret "Kill List" Proves a Test of Obama's Principles and Will*, N.Y. TIMES, May 29, 2012.

[75] Charlie Savage, *Secret U.S. Memo Made Legal Case to Kill a Citizen*, N.Y. TIMES, Oct. 8, 2011.

[76] Ellen Nakashima et al., *U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say*, WASH. POST, June 19, 2012; David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012.

[77] Robert D. Novak, *Mission to Niger*, WASH. POST, July 14, 2003. To be sure, vice-presidential aide Scooter Libby was convicted of perjury, making false statements, and obstruction of justice in the investigation. *See* Carol D. Leonnig & Amy Goldstein, *Libby Found Guilty in CIA Leak Case*, WASH. POST, Mar. 7, 2007. But the official who

- The CIA's network of secret prisons for detaining and interrogating senior al Qaeda figures, such as 9/11 mastermind Khalid Sheikh Mohammed.[78]
- The NSA's warrantless Terrorist Surveillance Program, which intercepted certain communications between al Qaeda suspects abroad and their contacts in the United States.[79]
- The Treasury Department's efforts to track al Qaeda's finances by collecting and analyzing data about international money transfers.[80]

None of these revelations resulted in charges and some did not even result in criminal investigations—whether because the leaker's identity was unknown, or due to uncertainty that prosecutors could establish guilt beyond a reasonable doubt, or because the disclosure was authorized by senior officials. Again, the likelihood that a given leak will be sanctioned is quite modest—and, therefore, so will be the deterrent effect of the laws against compromising classified information.

Beyond the statistical probabilities, leakers might escape punishment through a strategy that might be called *contrapuntal deterrence*: attempting to deter the government from enforcing laws whose purpose is to deter criminality. Leakers can take a number of steps to increase the government's expected costs of prosecuting them, thereby significantly reducing a leaker's expected sanction, perhaps even to zero.

One way to drive up the government's prosecution costs is to flee beyond the reach of American law. This might be accomplished by relocating to a country that lacks an extradition treaty with the United States—a class that includes such global and regional powers as China, Dubai, Indonesia, Qatar, Russia, Saudi Arabia, the United Arab Emirates, and others[81]—or to a country that is otherwise unlikely, for any number of reasons, to return the leaker to face charges at home. A leaker might, in other words, take a page from the Edward Snowden playbook, which involves fleeing initially to communist China,[82] then seeking refuge in or transit through such civil libertarian worthies as Cuba and Venezuela,[83] before finally settling on Vladimir Putin's revanchist Russia.[84]

---

was actually responsible for revealing Valerie Plame's identity—Deputy Secretary of State Richard Armitage—was never charged. *See* R. Jeffrey Smith, *Armitage Says He Was Source of CIA Leak*, WASH. POST, Sept. 8, 2006.

[78] Dana Priest, *CIA Holds Terror Suspects in Secret Prisons*, WASH. POST, Nov. 2, 2005.

[79] James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005.

[80] Eric Lichtblau & James Risen, *Bank Data Is Sifted by U.S. in Secret to Block Terror*, N.Y. TIMES, June 23, 2006.

[81] 18 U.S.C. § 3181 (2012).

[82] Jia Lynn Yang, *Edward Snowden Faces Strong Extradition Treaty if He Remains in Hong Kong*, WASH. POST, June 10, 2013.

[83] Max Fisher, *Why Cuba Might not be Safe for Snowden*, WASH. POST, June 25, 2013; Juan Forero & Will Englund, *With Snowden Offer, Venezuela's Maduro Is on World Stage*, WASH. POST, July 9, 2013.

[84] Michael J. de la Merced, *Russia Plans to Extend Snowden Asylum, Lawmaker Says*, N.Y. TIMES, Jan. 24, 2014.

The challenge of prosecuting suspects who have fled abroad is not unique to leaks. But the problem seems especially acute in this context. Extradition treaties ordinarily require dual criminality—the conduct must be an offense and subject to similar penalties under the laws of both states—and foreign countries may not have comparable prohibitions on leaking classified information. Or foreign countries might consider such disclosures to be "political" crimes that normally are not eligible for extradition under the treaties. The saga of WikiLeaks founder Julian Assange illustrates both barriers. The U.S. extradition treaty with Sweden, where Assange is wanted for questioning in a rape investigation, contains a dual criminality requirement.[85] It also provides that "[e]xtradition shall not be granted . . . [i]f the offense is regarded by the requested State as a political offense."[86] A member of Sweden's Supreme Court has publicly speculated that these restrictions may bar Assange's extradition to the United States.[87]

Another way to amplify the government's prosecution costs is to put further classified information at risk of compromise. The leaker might commission a third party to hold a tranche of sensitive documents in reserve, with instructions that they be released if the government initiates criminal proceedings or otherwise takes action against him. That is, he might threaten to use something like *Dr. Strangelove*'s Doomsday Machine. Some of the players in the Edward Snowden affair may be pursuing a strategy along these lines. Glenn Greenwald, who has publicized the Snowden disclosures, has warned that "[t]he U.S. government should be on its knees every day begging that nothing happen to Snowden, because if something does happen to him, all the information will be revealed and it could be its worst nightmare."[88]

There's also the problem of "graymail." A defendant who has been charged with leaking might, during pretrial proceedings, seek discovery of classified information, or at trial he might attempt to introduce classified materials already in his possession. These maneuvers can be bona fide, as the defendant may well have a legitimate interest in obtaining or using exculpatory evidence, but they can also be made in bad faith. Regardless of motivation, the effect is to force the government into a Hobson's choice—it "can withdraw all or part of its case to protect its information, or proceed and surrender its sensitive intelligence and possibly its source."[89] The Classified Information Procedures Act can help mitigate these problems, but perhaps not enough to alter the government's cost-benefit calculations. CIPA allows courts to take various steps to protect sensitive information at trial—e.g., an *in camera* hearing to determine whether the documents the defendant seeks to introduce are relevant and admissible, allowing the government to admit the facts to which the documents relate or prepare an unclassified summary in lieu of introducing the documents themselves, and so on.[90] But in return, the statute

[85] Convention on Extradition, U.S.–Swed., art. III, Oct. 24, 1961, 14 U.S.T. 1845.

[86] *Id.* art. V.

[87] Stefan Lindskog, *Julian Assange: Swedish Justice*, FINANCIAL REV. (Austl.), Mar. 30, 2013.

[88] *Quoted in* Mitra Taj, *Snowden Documents Could Be "Worst Nightmare" for U.S.: Journalist*, REUTERS, July 13, 2013.

[89] Al-Marri v. Pucciarelli, 534 F.3d 213, 307–08 (4th Cir. 2008) (en banc) (Wilkinson, J., concurring in part and dissenting in part), *vacated sub nom.* Al-Marri v. Spagone, 555 U.S. 1220 (2009).

[90] 18 U.S.C. app. 3 § 6(a), (c)(1) (2012).

authorizes a variety of sanctions on the government, ranging from dismissing the indictment in its entirety to dismissing individual counts to "finding against the United States on any issue as to which the excluded classified information relates."[91] Even when CIPA shields sensitive information, it still imposes real costs that can deter authorities from pursuing criminal sanctions.

Not only is it exceedingly unlikely that the government will prosecute a given disclosure, the sanctions for leaking are relatively modest. The maximum sentence for violating section 793(d) of the Espionage Act, the statute most commonly deployed against leakers, is ten years of incarceration.[92] That sounds like a significant term but it is far less than the penalties for many other federal crimes, including offenses of similar or even lesser social harm. For instance, a first-time offender convicted of trafficking 500 grams of cocaine, 100 grams of heroin, a single gram of LSD, or comparably modest amounts of other narcotics faces a mandatory minimum of five years and a maximum penalty of 40 years.[93] Bank fraud is punishable by up to 30 years,[94] mail and wire fraud up to 20,[95] and bribery up to 15.[96] An intelligence official who pays hush money to a colleague to cover up the fact that he has given classified documents to a reporter has more to fear from the bribery than from the leak. This is not a statutory scheme that emphasizes leak prevention.[97]

Of course, leakers' sentences can be much longer if, like Manning, they are convicted of multiple counts of compromising classified information. But that risk seems more theoretical than real, as the sanctions actually imposed in leak cases are typically quite low. In the ten completed Espionage Act cases discussed above, the median sentence is between 1.1 and 1.7 years of incarceration and the mean is about 4.6 years. If we exclude the four defendants who

---

[91] *Id.* § 6(e)(2).

[92] 18 U.S.C. § 793(d) (2012). The Sentencing Guidelines range for the base offense—87–108 months, *see* U.S. SENTENCING GUIDELINES MANUAL § 2M3.3(a) & sentencing table (2014)—approaches the statutory maximum, though in practice most convicted leakers receive considerably lighter sentences. *See supra* notes 61–71 and accompanying text.

[93] 21 U.S.C. § 841(b)(1)(B) (2012). The Sentencing Guidelines base offense range is 51–63 months. U.S. SENTENCING GUIDELINES MANUAL § 2D1.1(c)(8) & sentencing table.

[94] 18 U.S.C. § 1344 (2012).

[95] *Id.* §§ 1341, 1343.

[96] *Id.* § 201(b)(1)–(2). Fraud and bribery carry relatively modest Sentencing Guidelines base-offense ranges of 0–6 months and 15–21 months, respectively. U.S. SENTENCING GUIDELINES MANUAL §§ 2B1.1(a)(1); 2C1.1(a)(1). However, these numbers can jump dramatically if the offenses involve more than minimal sums of money, *see id.* § 2B1.1(b)(1)(G) (twelve-level increase for fraud involving more than $200,000, for an adjusted range of 30–37 months), or senior officials, *see id*. § 2C1.1(b)(3) (four-level increase for bribery involving elected or high-level officials, for an adjusted range of 27–33 months).

[97] These other statutes' penalties may well be harsher than necessary to achieve deterrence, and their severity may well discourage "socially desirable activities at the borderline of criminal activity." Richard A. Posner, *An Economic Theory of the Criminal Law*, 85 COLUM. L. REV. 1193, 1206 (1985). *But see* Dru Stevenson, *Toward a New Theory of Notice and Deterrence*, 26 CARDOZO L. REV. 1535, 1574 n.179 (2005) (arguing that "overdeterrence or a 'chilling effect' is less of a concern with crimes than torts"). But the concern here is a comparative one. Congress reveals its priorities in what conduct it chooses to punish and how severely, and it evidently regards small-scale narcotics trafficking as a more serious problem than leaking highly classified documents.

were either exonerated or avoided jail time—Ellsberg, Franklin, Drake, and Petraeus—the numbers jump a bit to between 2 and 2.5 years (median) and about 7.6 years (mean). (In both scenarios the mean is skewed upward by Manning's outlier 35 year sentence, though parole is possible after seven years.) A year and a half isn't nothing, but neither is it the sort of draconian sanction that is calculated to strike fear into the hearts of would-be leakers.

Why not charge leakers more aggressively in an effort to obtain harsher sentences?[98] For one thing, there are statutory constraints. Consider Manning, who was charged not only with violating section 793 but also with the capital crime of aiding the enemy under article 104 of the Uniform Code of Military Justice.[99] The government's theory was that Manning had aided hostile foreign powers "through indirect means" because he must have known that they would inevitably see the materials he was sharing with WikiLeaks.[100] (Manning was charged under military law, but the same claim could be made in civilian court. Section 794 of the Espionage Act makes it a crime, punishable by life imprisonment or death, to reveal protected information "to a[] foreign government,"[101] and authorities just as easily could argue that a leak accomplishes this "though indirect means.") The judge at Manning's court-martial acquitted him of aiding the enemy—properly, in my view—because the government's novel theory effectively would have made all leaking akin to treason. Virtually every document leaked to the press will find its way into enemy hands, so leaking would almost always violate article 104 in addition to section 793, collapsing the distinction between the two different crimes. And because section 794 is uncomfortably similar to article 104, the effects of such a sweeping interpretation likely would be felt in civilian courts as well. As it is, if the Manning case is any guide, section 793's ten-year maximum seems to be the upper limit.

It's always possible that Congress could enact new legislation with stronger penalties for leaking, but that seems exceedingly unlikely. Congress's last attempt to expand the Espionage Act did not end well. In 2000, the House and Senate approved a sweeping bill that would have made it a crime, punishable by up to three years in prison, for government employees to disclose "any classified information . . . to a person . . . who is not authorized access to such classified information."[102] Unlike section 793, there was no need to show that the leak "could be used to the injury of the United States or to the advantage of any foreign nation;"[103] the mere fact that the information was classified was enough to trigger liability. President Clinton vetoed the legislation on the ground that it was "overbroad" and could "unnecessarily chill legitimate activities that are at the heart of a democracy,"[104] and Congress has shown little appetite for revisiting the issue since. Tellingly, even in its most ambitious effort in decades to rewrite the

---

[98] *Cf.* Pozen, *supra* note 2, at 594 ("Given the benefits of leakiness and the high costs of enforcement, rare imposition of stiff penalties may be an efficient approach." (citing Becker, *supra* note 53, at 183–84)).

[99] 10 U.S.C. § 904 (2012).

[100] Charlie Savage, *Soldier Faces 22 New WikiLeaks Charges*, N.Y. TIMES, Mar. 2, 2011.

[101] 18 U.S.C. § 794(a) (2012).

[102] Intelligence Authorization Act for Fiscal Year 2001, H.R. 4392, 106th Cong. § 303(a)(2) (2000).

[103] 18 U.S.C. § 793(d) (2012).

[104] *Quoted in* David G. Savage, *Clinton Vetoes Bill on Leaking of U.S. Secrets*, L.A. TIMES, Nov. 5, 2000.

law of leaks, Congress refrained from increasing the penalties for existing leak-related offenses, and it authorized even more modest penalties for the new crime it proposed to create.

In addition, practical considerations will often constrain the government from pursuing more severe sanctions against leakers. The conventional approach in leak cases is for the parties to enter a plea agreement that includes a fairly modest penalty in lieu of testing the government's case in a trial. This resolution, seen in seven of the ten completed leak cases, is often advantageous both for the defendant (who receives a lighter sentence) and for the government (which obtains a certain conviction and avoids the risk of compromising additional sensitive information at trial). The more aggressive alternative would be for the government to eschew pleas in an effort to obtain convictions and harsher penalties at trial, in effect pursuing a holdout strategy. Authorities may well be reluctant to do so, as this might produce an unacceptable risk of graymail—not to mention the risk of acquittal by a jury that sees the defendant as an admirable whistleblower.

B. Contract Law

Contract law may be even less suited for deterring leaks than criminal law. The government rarely seeks to enforce employees' nondisclosure agreements, for a fairly straightforward reason: the conduct that constitutes a breach normally constitutes a violation of the Espionage Act as well, and a prevailing contract claim would add little to a successful criminal prosecution. Indeed, the normal sanction for private parties who breach their contractual duties—money damages—may well be unavailable in leak cases. In *Snepp*, the Supreme Court observed that the government's actual damages from a breach "generally are unquantifiable" and that nominal damages "are a hollow alternative,"[105] and it warned against "saddl[ing] the former agent with exemplary damages out of all proportion to his gain."[106] (*Snepp* dealt with prepublication review, but similar concerns would arise in nondisclosure cases.) And even if the law did permit money damages, many military and intelligence officials are judgment-proof; the government might obtain a favorable ruling against a faithless employee only to find itself unable to collect.

The government's own conduct suggests that it does not regard civil liability to be a meaningful deterrent. *Marchetti* appears to be the only case in which the government pursued civil remedies against a leaker in lieu of prosecuting him. (Why? Authorities may have believed that a breach-of-contract suit was less risky. At the time, 1972, the *Morison* case had not yet established that the Espionage Act applies to leakers as well as spies. Plus the government's only prior attempt to prosecute a leaker under the statute, Daniel Ellsberg in 1971, was unraveling and would soon end in disaster.) Whatever the reason, subsequent leak cases have been entirely criminal affairs. Authorities conceivably could have sued Manning, Snowden, and others for breach of contract, either in addition to or as an alternative to criminal charges, but instead they opted to pursue each leaker solely under the Espionage Act. The government apparently considered the deterrent effect of civil liability to be negligible.

[105] Snepp v. United States, 444 U.S. 507, 514 (1980).

[106] *Id.* at 514, 516.

More frequently, the government will seek to enforce employees' separate agreement to submit their writings to prepublication review, probably because there is less overlap here with the Espionage Act. Yet the sanction for breaching this obligation—the constructive trust—is less likely to achieve deterrence than is commonly supposed. The *Snepp* Court was persuaded that this "swift and sure" remedy is "tailored to deter those who would place sensitive information at risk,"[107] but that will only be true for a subset of all leakers, and probably a small subset. The Court had in mind a particular sort of official with a particular sort of motivation—one who reveals classified information because he expects to gain financially. That person may well reconsider his plan to write a tell-all when he realizes that his royalty checks will be endorsed over to the government. But many other leakers—perhaps most—leak for very different reasons. They might reveal classified information to blow the whistle on practices they regard as unlawful or abusive, to alert the public to policies or practices they see as misguided, to assign blame to their bureaucratic rivals, to take credit for successful operations, to manipulate public opinion, and to accomplish countless other objectives. Those who leak for ideological or other non-pecuniary reasons aren't likely to be deterred by the prospect of lost profits, because they aren't doing it for money in the first place. The sanction they face is effectively zero.

The recent *Ishmael Jones* case illustrates these difficulties. Jones (a pseudonym) was a longtime CIA operative who in 2008 published a sharply critical book about his former employer entitled *The Human Factor: Inside the CIA's Dysfunctional Intelligence Culture*. The author, who saw himself as a whistleblower, submitted his manuscript to prepublication review but published it anyway when consent was refused; indeed, he seemingly boasted about defying "the CIA's censors," claiming that it was his "duty" to publish without authorization.[108] He also established something like a preemptive constructive trust, donating his profits to the children of American soldiers killed in action.[109] The government's case against Jones was a slam dunk, so much so that the judge found the author liable on the government's motion for summary judgment[110] before eventually imposing a constructive trust on his earnings from the book.[111] Yet not even the near certain prospect of legal liability was enough to achieve deterrence. Jones wasn't motivated by money, but by a desire to shed light on what he regarded as a dysfunctional intelligence bureaucracy and to contribute to the public debate on reforming the CIA. And he was especially unlikely to be cowed by the threat of lost profits since he'd already donated them to charity.

In addition to the criminal and civil penalties recounted above, government officials who leak classified information might face a variety of formal and informal administrative

---

[107] *Id.* at 515.

[108] ISHMAEL JONES, THE HUMAN FACTOR: INSIDE THE CIA'S DYSFUNCTIONAL INTELLIGENCE CULTURE viii (2008).

[109] *Id.* at xii.

[110] *See* Transcript of Motions Hearing at 18-21, United States v. Jones, Civil Action No. 10-765 (E.D. Va. June 15, 2011), *available at* http://www.fas.org/sgp/jud/jones/061511-hearing.pdf.

[111] *See* United States v. Jones, Civil Action No. 10-765 (E.D. Va. Apr. 18, 2012) (order imposing constructive trust), *available at* http://www.fas.org/sgp/jud/jones/041812-order.pdf.

sanctions.[112] Military and intelligence agencies have powerful cultural norms against leaking, and employees who breach these norms might be shunned by their colleagues, develop bad professional reputations, be excluded from key decisions, and so on.[113] More formally, they might be demoted or exiled to less desirable jobs or even have their security clearances revoked, which as a practical matter usually means the end of their careers. Like the technological controls that are the subject of this essay, these administrative penalties can substitute for more traditional legal penalties. It may be significant that a substantial number of leak cases have involved former government employees who were no longer subject to administrative discipline (such as Jones, Marchetti, and Snepp)[114] or outside contractors for whom administrative sanctions are presumably less fearsome (such as Kim, Leibowitz, and Snowden).[115] This implies that the threat of administrative discipline may have some real bite, perhaps even more than the threat of legal liability. Still, as David Pozen has argued, the possibility of informal punishment carries much more weight with senior officials than with low-level ones—a junior analyst can't be excluded from an inner circle he was never part of—and while formal administrative discipline may be more common than criminal prosecution it is "still statistically remote."[116]

III. A Technology-Based Alternative

If criminal and contract law are imperfect deterrents, what can the government do to protect against leaks? The short answer is to supplement current efforts to *deter* leaks with more robust efforts to *block* them. Intelligence systems already rely on technology to protect classified information, and they should include additional technological features that can more effectively prevent employees from accessing and exfiltrating protected data. There's no need to deter conduct that technology makes it impossible to commit.

There are at least two literatures with important insights on how to handle leaks given the difficulty of deterring them. The first is Neal Katyal's work on "cost deterrence." Katyal argues that it is possible to "constrain crime by making it more expensive"; "if crime is expensive to commit . . . individuals will be more likely to refrain from it."[117] This can be done by taking steps to increase the perpetration costs—equipment, labor, and so on—that would-be criminals

[112] Pozen, *supra* note 2, at 586–90, 592.

[113] In the same way, cultural norms among journalists can powerfully influence which leaks are published, as many reporters understand themselves to have a professional obligation to balance the public's right to know against the government's national security interests. *See, e.g.*, Patricia L. Bellia, *WikiLeaks and the Institutional Framework for National Security Disclosures*, 121 YALE L.J. 1448, 1452–53 (2012). This is why many journalists historically have been reluctant to identify covert assets by name—an aversion that is not always shared by nontraditional media, such as WikiLeaks, which has published unredacted documents that identified Afghans who worked with the U.S. military. Jeanne Whalen, *Rights Groups Join Criticism of WikiLeaks*, WALL ST. J., Aug. 9, 2010.

[114] *See supra* notes 32–52, 108–111, and accompanying text.

[115] *See supra* notes 64, 66, 71, and accompanying text.

[116] Pozen, *supra* note 2, at 592–93; *see also id*. at 595 ("Leakers operate with a high degree of impunity from criminal, civil, and administrative discipline.").

[117] Neal Kumar Katyal, *Architecture as Crime Control*, 111 YALE L.J. 1039, 1071, 1089 (2002); *see also* Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1006 (2001).

must bear to carry out their contemplated offenses. In other words, authorities should focus on the inputs of crime in addition to the outputs of completed crimes. "Unlike the speculative cost of prosecution, which criminals may wrongly discount due to poor judgment about risk, criminals are certain to incur these up-front monetary costs."[118] Real-space examples of cost deterrence include hardening potential targets, as with locks and alarms (thereby increasing criminals' labor costs), as well as designing open spaces that allow citizens to engage in "natural surveillance" (thereby requiring criminals to hire lookouts).[119] In cyberspace, Katyal proposes requiring potential targets of intrusions to implement various defenses that can prevent hackers from compromising their systems,[120] or "taxing dangerous software [or] charging small admissions fees to enter sensitive web sites."[121]

The second key insight is Larry Lessig's observation that "code is law."[122] Lessig argues that code—"the instructions imbedded in the software and hardware that make cyberspace work"[123]—can influence users' behavior in much the same way that legal commands do. In cyberspace, "regulation often comes through code. Important rules are imposed, not so much through social sanctions, and not by the state, but by the very architecture of the particular space. A rule is defined, not through a statute, but through the code that governs the space."[124] Code and law can be rough substitutes. The law constrains undesirable conduct by issuing commands backed by the threat of punishment, but the same conduct can be constrained by designing systems in ways that make the conduct impossible to commit. As an example, Lessig compares the regulation of overflights in real space (where an aircraft will not be held to interfere with the property below if it flies at a sufficiently high altitude) and in the online game space of Second Life (where it is not possible to fly lower than 15 meters above the underlying property). Both forms of regulation constrain overflights, Lessig explains:

> But notice the important difference. In real space, the law means you can be penalized for violating the "high/low" rule. In Second Life, you simply can't violate the 15-meter rule. The rule is part of the code. The code controls how you are in Second Life. There isn't a choice about obeying the rule or not, any more than there's a choice about obeying gravity.[125]

Many of the code-based regulations Lessig describes are features of the digital world, but they also exist in real space. Consider speed limiters. Some automobile manufacturers use

---

[118] Katyal, *Cyberspace*, *supra* note 117, at 1040.

[119] Katyal, *Architecture*, *supra* note 117, at 1089–90. Of course, such measures may not reduce the overall incidence of crime but rather displace crimes onto other victims, a form of negative externality.

[120] Katyal, *Cyberspace*, *supra* note 117, at 1011–12.

[121] *Id.* at 1041.

[122] LAWRENCE LESSIG, CODE VERSION 2.0 at 1 (2006).

[123] *Id.* at 72.

[124] *Id.* at 24.

[125] *Id* at 110.

limiters to restrict their vehicles' top speeds to, say, 155 miles per hour. It is not the threat of punishment that keeps the owner of a BMW M3 from reaching 160; it is the fact that his car makes it impossible to do so.[126] (Several German companies, including BMW and Mercedes, agreed to install speed limiters in the 1970s in a successful bid to dissuade the Bundestag from adopting a legal speed limit for the Autobahn. So limiters are a very literal example of technological controls on undesired conduct substituting for legal controls.) Ignition interlocks are another example of realspace regulation by code. These devices require drivers to blow into breathalyzers before their vehicles' engines can be switched on; if the blood alcohol level exceeds a specified limit, the ignition is disabled. Ignition interlocks prevent the crime of drunk driving not by threatening to punish it but by making it impossible to commit—at least for certain drivers in certain automobiles. (Ignition interlocks are normally installed when courts require their use by persons who have been convicted of alcohol-related offenses; the devices thus usefully illustrate how law and technology might collaborate to prevent socially harmful conduct.)

Taken together, cost deterrence and regulation by code counsel a different approach to preventing leaks: in addition to deterring leaks through legal commands backed by threats of punishment, authorities should increasingly rely on technological measures that make it excessively costly to exfiltrate protected data and disclose it to outsiders. Commentators have been calling for these sorts of tools for years as a way of promoting privacy and other constitutional values, and the same measures can also help prevent leaks.[127] In cost-deterrence terms, technological controls increase the costs that government employees must incur to leak classified information, perhaps raising perpetration costs to a level that dissuades them from doing so at all. In code-regulation terms, technological controls can be an effective substitute for the threat of legal sanctions. The more difficult it is to leak information, the less need there is for more traditional—and not always effective—forms of legal deterrence.

Of course military and intelligence officials already use technology to protect classified information—for example, usernames and passwords, air gapped networks, and so on. The details of what additional safeguards should be adopted is an engineering question on which I am very far from being an expert, but a few general possibilities come to mind. First, something as basic as hardware and workspace configuration can make it more difficult to compromise protected data. Officials could remove or disable USB ports, CD-ROM drives, and other removable media on computers that are connected to classified networks. Some military and intelligence agencies have been doing this for years to reduce their exposure to malware that propagates via thumb drives,[128] and a post-Manning executive order directed the intelligence

[126] To be precise, limiters do not prevent drivers from committing the crime of speeding as such but rather make it impossible for them to engage in grossly excessive speeding.

[127] *See, e.g.*, MARKLE FOUND., CREATING A TRUSTED NETWORK FOR HOMELAND SECURITY 15–16 (2003); THE PRESIDENT'S REVIEW GRP. ON INTELLIGENCE AND COMMC'NS TECHS., LIBERTY AND SEC. IN A CHANGING WORLD 248–49 (2013).

[128] JOEL BRENNER, AMERICA THE VULNERABLE 84–88 (2011); RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR 171–74 (2010).

community as a whole to implement similar restrictions[129] (though the President's Review Group reports that "implementation of that directive has been at best uneven and far too slow").[130] The same measures could also protect against exfiltration: inability to copy huge troves of electronic files would dramatically increase the cost of carrying out large-scale documentary leaks of the Manning and Snowden variety. In addition, workspaces for intelligence analysts could feature open-concept designs like "mission control" layouts or communal desks rather than individual cubicles. Some interagency intelligence fusion centers have been designed this way to facilitate information sharing and coordination. Creating spaces with open sightlines would have another advantage: enabling analysts to observe any suspicious system activity and thereby discouraging misconduct. In other words, workspaces could be designed to facilitate natural surveillance.[131]

Second, there are access and permission controls, which can "assur[e] that only people in authorized 'roles' can do particular activities in a computer system."[132] Basic identity assurance mechanisms are already in widespread use and more elaborate variants might be developed as well. Perhaps the most fundamental of all is the security clearance, issued after a lengthy background investigation, without which an employee may not access classified information at all. Existing technological controls include usernames and passwords, a ubiquitous technique for restricting access to authorized users and verifying that users are in fact who they purport to be. Authorities could supplement these measures with biometric identity verification, such as fingerprint or retina scanners. Biometrics would help prevent unauthorized personnel from using phishing, keystroke loggers, or other techniques to gain access to sensitive systems through others' accounts. (Snowden reportedly obtained some of the NSA documents he leaked by persuading agency colleagues to give him their login credentials and passwords.[133]) Customs officials recently made a similar transition to biometric identity verification at border checkpoints. The US-VISIT program collects fingerprints and facial photographs from aliens arriving at air and sea ports of entry, and there is no reason to think that military and intelligence agencies cannot widely deploy the same techniques.

Access and permission controls can also help ensure that the information users seek is related to their official duties. Systems could use Information Rights Management (IRM) to grant or deny access not just on the basis of users' *roles* (such as the fact that a user is an analyst with a certain set of security clearances, for instance, or a supervisor) but the *purposes* for which

---

[129] Press Release, The White House Office of the Press Secretary, Fact Sheet: Safeguarding the U.S. Government's Classified Information and Networks (Oct. 7, 2011), *available at* http://www.whitehouse.gov/the-press-office/2011/10/07/fact-sheet-safeguarding-us-governments-classified-information-and-networ.

[130] PRESIDENT'S REVIEW GRP., *supra* note 127, at 250.

[131] Katyal, *Architecture*, *supra* note 117 at 1089–90.

[132] Peter Swire, *Peeping*, 24 BERKELEY TECH. L.J. 1167, 1180 (2009); *see also* Seth F. Kreimer, *Watching the Watchers: Surveillance, Transparency, and Political Freedom in the War on Terror*, 7 U. PA. J. CONST. L. 133, 172–76 (2004); Ira S. Rubinstein et al., *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 267–68 (2008); K. A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 2, 75–76 (2003).

[133] Mark Hosenball & Warren Strobel, *Exclusive: Snowden Persuaded Other NSA Workers to Give up Passwords—Sources*, REUTERS, Nov. 7, 2013.

they seek the documents. As Peter Swire argues, managing access on the basis of user purpose "may be more granular" and therefore reduces the risk of "a highly privileged role getting access to too many records."[134] IRM would ensure that there is a match between the functions performed by the user requesting the information and the purposes for which that data may be useful; ideally this would be an automated process.[135] Imagine, for example, an intelligence report from a foreign liaison service that describes a new al Qaeda technique for concealing explosives. The document could be given a metadata tag that indicates its general subject matter, and the system could then grant access to analysts who are able to demonstrate (such as with digital credentials in their user profiles) that they are working, say, the terrorist threat to civil aviation and insurgent use of IEDs in war zones, while denying access to analysts whose profiles reveal their responsibilities to lie in entirely unrelated fields or to system administrators. (In fairness, the President's Review Group has expressed concern that the IRM products available today are "perhaps insufficiently robust" to support such a system, in which case policymakers should encourage further technological development.[136])

Immutable audit trails—a digital equivalent of surveillance cameras—are a third extant technique whose use might be expanded. Keystroke loggers and other mechanisms can record employees' activities on protected systems—for example, "queries made by users, the information accessed, information flows between systems, and date-and-time markers for those activities."[137] The recorded data can then be stored in ways that cannot subsequently be altered, defeating any efforts to evade detection and preserving a permanent record of system activity.[138] If classified information is disclosed, security officials would be able to examine the logs to see which users accessed the compromised documents, and would-be leakers' knowledge that they are very likely to be caught will have a powerful deterrent effect.[139] These sorts of measures have already shown some promise in policing unauthorized access to protected information. Access logs enabled State Department officials to quickly identify and discipline the outside contractors who improperly accessed Hillary Clinton, John McCain, and Barack Obama's private passport files during the 2008 presidential campaign.[140]

---

[134] Swire, *supra* note 132, at 1181 n.89 (citing Naikuo Yang et al., *A Purpose-Based Access Control Model*, 1 J. INFO. ASSURANCE & SEC. 51 (2008)); *see also* MARKLE FOUND., *supra* note 127, at 15; PRESIDENT'S REVIEW GRP., *supra* note 127, at 234.

[135] PRESIDENT'S REVIEW GRP., *supra* note 127, at 254-56.

[136] *Id.* at 255.

[137] MARKLE FOUND., IMPLEMENTING A TRUSTED INFORMATION SHARING ENVIRONMENT: USING IMMUTABLE AUDIT LOGS TO INCREASE SECURITY, TRUST, AND ACCOUNTABILITY 1 (2006); *see also* STEWART BAKER, SKATING ON STILTS: WHY WE AREN'T STOPPING TOMORROW'S TERRORISM TODAY 336–38 (2010); Kreimer, *supra* note 132, at 176–78.

[138] Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441, 1471–73 (2011).

[139] Swire, *supra* note 132, at 1186–87.

[140] Glenn Kessler, *Rice Apologizes for Breach of Passport Data*, WASH. POST, Mar. 22, 2008; *see also* BAKER, *supra* note 137, at 334–35.

Fourth, and more ambitiously, officials might use pattern analysis to protect against insider threats.[141] Intelligence officials have long sought to develop systems that are capable of processing huge troves of financial, communications, travel, and other information to identify patterns of behavior that may indicate a terrorist plot or other national security threat is underway.[142] These sorts of tools might be turned inward as well. Automated processes could monitor activity on intelligence systems in search of suspicious patterns that might suggest a user is attempting to exfiltrate protected information.[143] These processes could alert security officials, ideally in real time, when questionable behavior is detected, such as employees who open documents that concern subjects outside their normal areas of responsibility or expertise; employees who retrieve unusually large numbers of documents; employees who access protected information on computer terminals located where they cannot be observed by other users; employees who are opening sensitive documents at unusual times of day; employees who have inserted thumb drives or other removable media into their workstations; and so on. Once alerted, security officials could observe the user's system activity and intervene as appropriate. Private companies have brought to market and continue to develop a variety of software products along these lines,[144] though again the President's Review Group has expressed some doubt about the current versions' effectiveness.[145]

Not only can these sorts of technological controls be more effective than law, they can also be more nuanced. The Espionage Act is a blunt instrument that uses a uniform standard to regulate a wide and diverse range of behaviors that involve misuse of classified information—classic espionage on behalf of a foreign government, publishing secrets for monetary gain, informing the public about the government's activities, blowing the whistle on illegal conduct, massive undifferentiated data dumps, and so on. Yet these different types of disclosures are not equally harmful—spying is worse than profiteering, which in turn is worse than whistleblowing—and a legal prohibition that is appropriate for one kind of breach may be inappropriate for others. Technology can permit more precise distinctions about which misuses of classified information are especially damaging and therefore worthy of prevention. A system of technological controls could be designed to place special emphasis on, for instance, blocking large-scale data dumps while leaving policymakers' signaling leaks regulated less stringently or not at all. To be sure, the criminal law can make similarly fine-grained distinctions in the form of prosecutorial discretion, charging decisions, sentencing upon conviction, and so on. But these mechanisms seem inferior in at least one important way. Unlike ex ante technological controls (or cultural norms in the intelligence community), criminal law mechanisms generally operate ex post and thus offer less clarity and predictability on what types of breaches are regulated and how.

---

[141] *See, e.g.*, Christian Davenport, *Federal Agencies Embrace New Technology and Strategies to Find the Enemy Within*, WASH. POST, Mar. 7, 2014.

[142] *See, e.g.,* SHANE HARRIS, THE WATCHERS 144–54 (2011).

[143] PRESIDENT'S REVIEW GRP., *supra* note 127, at 247–48, 253.

[144] *See*, *e.g.*, *Insider Threats*, LANCOPE, *available at* http://www.lancope.com/solutions/security-threats/insider-threats/; *Insider Threat*, PALANTIR, *available at* https://www.palantir.com/solutions/insider-threat/; *Detecting and Preventing Insider Threats*, SPECTORSOFT, *available at* http://www.spectorsoft.com/solutions/insider-threats.html.

[145] PRESIDENT'S REVIEW GRP., *supra* note 127, at 255.

This is not to suggest that a uniform set of technological measures should be adopted by all elements of the intelligence community. A robust suite of constraints may be appropriate for agencies that generate or maintain especially sensitive national security data or that have proven to be favorite targets for leakers, whereas modest controls may suffice for more peripheral players. In the same way, technological controls need not—and, practically speaking, probably cannot—be implemented across the entire intelligence community at the same time. They could instead be deployed incrementally. One plausible scenario is to launch pilot programs at relatively small elements (such as the Department of Homeland Security's Office of Intelligence and Analysis or the State Department's Bureau of Intelligence and Research), followed by a phased rollout to larger components like the various divisions of the NSA and CIA. This would allow officials to work out the inevitable kinks in a controlled, bounded environment before attempting to scale up the systems for larger enterprises.

Candidly, these mechanisms will not be infallible; there is no technological silver bullet that can prevent all undesirable leaks at all times. But, from a normative standpoint, there shouldn't be. Technological controls should not be so severe as to block all internal or external flows of protected information. The goal is not the maximum technologically achievable level of protection but rather an efficient level of protection (where efficiency is a function of the harm caused by a given disclosure, the public's interest in the information, and other normative considerations on which this article is agnostic). Moreover, from a deterrence standpoint, even beatable countermeasures can be valuable. Sophisticated and determined users might find ways to defeat access controls, audit logs, pattern analysis, and other countermeasures, but doing so will take time and effort—and that is the very point of cost deterrence. Even imperfect technological controls will increase the labor costs of leaking, thereby discouraging at least some would-be leakers.

Which brings us to an important problem. Efforts to regulate behavior through cost deterrence and code can be problematic in "dual use" scenarios—that is, where the inputs of crime whose prices authorities seek to manipulate are useful not just to criminals but also to those who use them for entirely benign purposes.[146] Taking steps to increase the prices of computers and internet access in a bid to reduce cybercrime, as Katyal proposes,[147] would not just affect hackers but countless ordinary users who go online to check the news, share photos with friends, or for other innocuous activities. In the same way, a strategy of cost deterrence and regulation by code can restrict entirely beneficial flows of information—both internally within the government and externally between the government and the public. It is therefore essential to ensure that technological controls on leaks have workarounds that permit these activities to continue relatively unimpeded.

For instance, code-based constraints might interfere with intelligence analysts' legitimate need to exchange information with one another. Information sharing is one of the rare post-9/11 initiatives that commands virtually unanimous support. Among other advantages, pooling data

[146] Katyal, *Cyberspace*, *supra* note 117, at 1006–07.

[147] *Id.* at 1011–12, 1041.

can help analysts perceive the entire intelligence mosaic, where previously they only saw individual tiles; it can allow intelligence agencies to specialize in collecting different kinds of information, thereby promoting efficiency gains; and it can foster a system of competitive analysis that exposes policymakers to diverse perspectives and helps counter groupthink tendencies.[148] The purpose-based access controls mentioned above might preserve sharing while preventing leaks. Fine-grained access determinations that match a user's purpose to the information's content could help block leaks without reviving the pathologies of "need to know" that dominated before 9/11.

It's also important to maintain the ability of senior policymakers, like cabinet secretaries and White House aides, to reveal otherwise protected information to the public through journalists. Officially approved leaks are a valuable mechanism for informing citizens about classified national security activities, which among other benefits can build public trust and enhance the legitimacy of those programs.[149] (They also have some drawbacks, such as the risk that officials will selectively leak to manipulate public opinion, but it seems unlikely that supplementing a regime that regulates leaks through law with a technology-based alternative will make those dangers systematically more severe.) To the extent these sorts of disclosures are oral, they are unlikely to be affected by technological controls on accessing and copying protected documents. And to the extent they involve providing or describing written documents to journalists, the disclosures might be preserved by building the system with something like an off switch. If an official wants to reveal a given document, the system could be configured to allow it after the official demonstrates the requisite approvals. Presumably this would involve obtaining sign-off from higher-ups in the executive branch, which in turn would promote centralized control of disclosure decisions. (That has both upsides and downsides. Centralized control would help prevent rogue operators from compromising sensitive data unilaterally, but it would also keep dissenters from leaking to expose wrongdoing or to counter a problematic official narrative—which makes it all the more important to strengthen the alternative information channels discussed below.)

A related drawback is the potential of code-based regulation to block the subset of documentary leaks by junior employees that on balance are valuable—that is, those whose national security harms are outweighed by various benefits, such as promoting informed democratic deliberation, drawing the public's attention to unlawful or abusive practices, enabling voters to hold policymakers accountable, and so on.[150] Because increasing use of technological controls may reduce the number of valuable leaks that occur, alternative information channels should be established to achieve some of the same benefits.

---

[148] Nathan Alexander Sales, *Mending Walls: Information Sharing After the USA PATRIOT Act*, 88 TEX. L. REV. 1795, 1799–1803 (2010).

[149] Pozen, *supra* note 2, at 559–61.

[150] Indeed, technological controls could curtail low-level whistleblowing dramatically. Journalists may be willing to credit an oral description of classified documents from a senior figure like an Assistant Attorney General, especially if that official is a repeat player known to the journalistic community. But an unknown Justice Department line attorney will need to establish credibility, and that task is much more difficult if he cannot point to documents substantiating his claims.

For instance, many scholars have urged lawmakers to address the persistent problem of over-classification.[151] Classifying less information in the first place may reduce the number of circumstances in which employees conclude that leaking is necessary. One way to do this would be to trim the number of officials who are authorized to classify information; in 2010, nearly 2,400 people had "original classification" authority and several million more could classify "derivative" information.[152] Other commentators have proposed an interagency review mechanism to more carefully scrutinize controversial classification decisions. This could be accomplished by expanding the mission of the Interagency Security Classification Appeals Panel, which currently is responsible for reviewing declassification requests from members of the public that were denied by the originating agency,[153] or perhaps the Public Interest Declassification Board, whose responsibilities include advising senior officials on the declassification and release of key national security documents.[154] Another reform would be to make the processes for declassifying information more robust. This could include accelerating the timetable for automatic declassification (which is currently set at ten or 25 years, depending on the information's sensitivity)[155] or providing more detailed standards and procedures to govern discretionary declassification.[156] Relatedly, courts could more vigorously scrutinize the government's efforts to invoke national security exemptions in FOIA cases, giving greater weight to the public's countervailing interest in gaining access to the information.[157] Technology might play a role here, too. Email threads and other materials sometimes remain classified by default even after the sensitive information that initially justified their classification has been removed. Automated systems could search for and flag these sorts of documents, enabling intelligence officials to declassify them.

There is also an extensive literature urging Congress to grant more meaningful whistleblower protections to military and intelligence officials who observe practices they believe to be unlawful or abusive.[158] For instance, employees could be authorized to report a wider range of legal violations—not just, as is currently the case under the Intelligence Community Whistleblower Protection Act of 1998, matters of "urgent concern," which are

---

[151] *See*, *e.g.*, Heidi Kitrosser, *Classified Information Leaks and Free Speech*, 2008 U. ILL. L. REV. 881, 888–96.

[152] Heidi Kitrosser, *Free Speech Aboard the Leaky Ship of State*, 6 J. NAT'L SEC. L. & POL'Y 409, 426–27 (2013).

[153] Steven Aftergood, *An Inquiry into the Dynamics of Government Secrecy*, 48 HARV. C.R.–C.L. L. REV. 511, 525–28 (2013).

[154] 50 U.S.C. § 3161 (2012).

[155] Exec. Order No. 13526 § 1.5(b), 75 Fed. Reg. 707 (Dec. 29, 2009). *See* Laura K. Donohue, *Terrorist Speech and the Future of Free Expression*, 27 CARDOZO L. REV. 233, 298–99 (2005).

[156] Pozen, *supra* note 2, at 566 n.273.

[157] Mary-Rose Papandrea, *Balancing and the Unauthorized Disclosure of National Security Information*, 97 IOWA L. REV. BULL. 94, 97–98 (2012).

[158] *See, e.g.*, Bellia, *supra* note 113, at 1524–26; Mary-Rose Papandrea, *Lapdogs, Watchdogs, and Scapegoats: The Press and National Security Information*, 83 IND. L. J. 233, 245–48 (2008); Stephen I. Vladeck, *The Espionage Act and National Security Whistleblowing After* Garcetti, 57 AM. U. L. REV. 1531, 1542–46 (2008).

defined narrowly to include "serious or flagrant" legal violations[159]—and agencies could be expressly barred "from retaliating against a whistleblower by revoking his security clearance."[160] Finally, government officials might make an even bolder move to deemphasize traditional, secretive forms of intelligence gathering and analysis altogether, making more extensive use of open-source materials instead. Some scholars have argued that during the Cold War, outsiders using publicly available data did a better job diagnosing the Soviet Union's weakness and predicting its eventual collapse than government analysts relying on classified information.[161] The advantages of open-source intelligence may hold true in other settings as well. In any event, this is not the place to iron out the precise details of a reformed secrecy regime. The important point for our purposes is that, whatever the merits of these proposals when considered on a blank slate, they will become even more important in a technology-based system that can restrict valuable information flows.

Conclusion

The past decade has been an extraordinary period in the history of the government's efforts to regulate leaks by law. After lying virtually neglected for a century, the Espionage Act has been called into frequent service as authorities' most visible instrument for constraining unauthorized disclosures of classified information. The numbers are dramatic: ten prosecutions since 2005, including nine on President Obama's watch. But in many ways those figures are a sign of the system's failure, not its success. The government has had to rely on ex post solutions like criminal prosecutions to deter leaks because it has failed ex ante to block those leaks from occurring in the first place. And the law is not always up to the challenge. Even in an era of unprecedentedly aggressive enforcement, the expected penalty for employees who reveal classified information often may be too modest to achieve deterrence; the sanctions for leaking are relatively low, and the probability a leaker will be punished is slight.

This essay seeks to begin a conversation about how to prevent leaks by sketching the outlines of an alternative approach, one that emphasizes technological measures capable of blocking employee attempts to compromise protected information. The building blocks for such a technology-based regime are already in place—access controls, audit logs, pattern analysis techniques, and so on—and they need only to be refined and deployed more widely. And the time is right for reform. If the spectacular breaches accomplished by Edward Snowden and Bradley Manning don't motivate the government to rethink its approach to securing its most sensitive secrets, it's hard to imagine what could.

---

[159] 50 U.S.C. § 3517(d)(5)(G)(i) (2012).

[160] Papandrea, *Lapdogs*, *supra* note 158, at 248.

[161] *See, e.g.*, Richard Gil Powers, *Introduction* to DANIEL PATRICK MOYNIHAN, SECRECY: THE AMERICAN EXPERIENCE 4-9 (1998).