THE WASP'S NEST: INTELLIGENCE COMMUNITY WHISTLEBLOWING & SOURCE PROTECTION

Dan Meyer*
David Berenbaum**

> *"Resolved, That it is the duty of all persons in the service of the United States, as well as all other the inhabitants thereof, to give the earliest information to Congress or other proper authority of any misconduct, frauds or misdemeanors committed by any officers or persons in the service of these states, which may come to their knowledge."* [1]

On July 30, 1778, the Continental Congress enacted the first American whistleblowing legislation to respond to prisoner abuse allegations against the United States Navy. This enactment from the hearth of a new commonwealth began a legislative tradition of transparency and candor that endured, in fits and starts, to the post-Watergate era and has informed the current American governing elite's political consciousness. Two hundred and thirty-five years later, Inspector General Irvin Charles McCullough III created the Intelligence Community Whistleblowing & Source Protection (ICW&SP) directorate—an office dedicated specifically to Intelligence Community (IC or Intelligence Community) whistleblowing.[2] But the origin

---

* Executive Director of Intelligence Community Whistleblowing & Source Protection (ED–ICW&SP), Office of the Inspector General of the Intelligence Community, Office of the U.S. Director of National Intelligence; Professor of Law (Adj.), National Intelligence University (NIU). J.D. Indiana University School of Law—Bloomington 1995; B.A. Cornell University 1987 (Government & Naval Science). This article is outreach of the Intelligence Community whistleblowing program.

** Consultant, Deloitte, Washington D.C. Metro Area. J.D. The George Washington University Law School 2010; B.A. (Political Science), Duke University 2006. The authors thank the Honorable Irvin Charles McCullough III and Ms. Jeanette J. McMillian, Counsel to the Inspector General, for their thoughtful coaching and contributions. This writing is dedicated to Cornell University's Professor Isaac Kramnick on the occasion of his retirement from coaching three generations of scholars on "inside baseball." The views presented in this article are those of the authors alone, and are not to be attributed to either the inspector general of the Intelligence Community or the United States Director of National Intelligence.

[1] JOURNAL OF THE CONTINENTAL CONGRESS VOL. 11 732 (1778).

[2] ICW&SP operations are divided into three categories: (1) disclosures & appeals (including *de novo* investigations); (2) outreach to promote whistleblowing; and (3) training to increase awareness of and responsiveness to allegations of reprisal against whistleblowers. ICW&SP went "operational" on September 15, 2013. ICW&SP's plan of operations is based on previous work in this area by the U.S.

of each act differed. The 2013 initiative was from the Executive branch—not the United States Congress.

The "wasp" in this article's title refers to the acronym for the Intelligence Community's new whistleblowing program: the Intelligence Community Whistleblowing & Source Protection directorate. The Executive branch regulatory actions creating ICW&SP occurred as the United States Supreme Court was declining to hear *United States v. Sterling*[3] while simultaneously granting a writ of certiorari in *Robert J. MacLean v. Dep't of Homeland Security*.[4] The choice to hear one case over another could be for reasons completely unrelated to the arc of change impacting whistleblowing law since the early 1990s. Or the Supreme Court decision could be quite deliberate. In passing on the *Sterling* issue in *Risen v. United States*, the Court delayed resolution of First Amendment ambiguities remaining at the close of the Watergate era's "open government" movement.[5] For Intelligence Community whistleblowing, the *Risen* issue was not the reporter's proposed First Amendment testimonial privilege, but rather the prospect this privilege would enable a source to claim a public interest in making an unauthorized disclosure.

By choosing to hear *MacLean* and deciding whether regulations prohibiting unauthorized disclosure of classified information outweigh a federal *external* whistleblower protection law, the Court is perhaps reinforcing the principle that the media has no greater First Amendment rights than ordinary citizens. This would follow the trend of emphasizing *internal* over the *external* disclosures so prevalent in the 1970s and early 1980s. And a decision against *MacLean* will further tip American whistleblowing toward internal agency disclosures and the concordant reliance on Congressional oversight.[6] One such program recently established

---

Department of Defense Inspector General (DoDIG), and the inspectors general of the National Security Agency and the Defense Intelligence Agency between 2004 and 2010.

[3] 724 F.3d 482 (4th Cir. 2013), *cert. denied,* 82 U.S.L.W. 3530 (U.S. June 2, 2014) (No. 13-1009).

[4] 714 F.3d 1301 (Fed. Cir. 2013), *cert. granted* 82 U.S.L.W. 3470 (U.S. May 19, 2014) (No. 13-894).

[5] 82 U.S.L.W. 3530 (U.S. June 2, 2014) (No. 13-1009).

[6] Such a decision will not alter the fundamental distance between Beltway professionals of those supporting an Executive branch–centered Federal government (basically, the American Tories) and those supporting a legislature-centered government (similarly, the American Whigs). *See* Peter M. Shane, *Chevron Deference, The Rule of Law, and Presidential Influence in the Administrative State*, 83 FORDHAM L. REV. 679, 691–693 (2014). In a small subset of whistleblower cases,

to promote internal disclosures is ICW&SP's Intelligence Community whistleblowing program.

Issues advanced in *Sterling*, *Risen*, and *MacLean* mark a division in modern whistleblower law. These cases delineate an intellectual distance[7] between opposing camps in the debate over how and when information can flow to the People sovereign under the American constitutional order. Lawful whistleblowers and unlawful leakers alike must navigate this distance as they decide how to pass information. This article analyzes the national security policy challenge in protecting Intelligence Community whistleblowers while simultaneously maintaining fidelity to the opacity required to execute the Federal intelligence and counterintelligence mission. It is the need for secrecy that creates the intellectual distance between the sovereign's need for information regarding the performance of the Federal intelligence and counterintelligence mission and the ability to conduct that mission. To borrow from the medieval principles discussed later, the Intelligence Community is, accordingly, one large juridical marchland.

To analyze the national security policy challenge in protecting Intelligence Community whistleblowers while simultaneously maintaining fidelity to the Federal intelligence and counterintelligence mission, we will first review ICW&SP's concept of operations, in Section I. We then present in Section II an analytic lens—in the form of a paladin theory of Federal decision making—which aids in understanding why the Legislative and Executive branches chose a presidential policy directive in 2012 as the vehicle of reform in creating a system of Intelligence Community

---

this distinction is paramount in that it triggers constitutional separation of powers concerns. These are also the cases that garner public attention disproportionate to their numbers. N.B. As this article was being edited for press, the Court found for Mr. MacLean, employing a technical distinction between a 'law' and a 'rule or regulation.' This, of course, is precisely what the Court would do under a paladin theory of Federal decision making, drawing distinction between the work of the sovereign-in-legislature and others operating under the sovereign's delegated authority. *See* Dep't Homeland Sec. v. MacLean, No. 13-894, slip op. at 7-11 (U.S. Jan. 21, 2015).

[7] As with the use of the word "hearth" in the opening paragraph of this law review article, the use of the term "distance" in this law review article is very specific. The authors of this law review article use these spatial terms to note the relationship of an issue to the juridical principles of *jurisdictio* and *gubernaculum*. A "hearth" is the center of lawful authority—a sovereign or its representative. The run of that sovereign's writ is *gubernaculum*, after the distance of which, the sovereign cannot exercise its authority. A claim of authority is *jurisdictio*. When *jurisdictio* exceeds *gubernaculum*, a sovereign faces a *march*. To order a march with law, the sovereign elevates a *paladin* within a *palatine*.

whistleblowing. Section III then explores the context in which this Federal decision making occurred. In Sections IV and V, we apply the paladin theory of Federal decision making to the creation of an Intelligence Community whistleblowing program. Through all these sections, one theme is paramount: the limits of decision making are transcendent. As decision makers face limits imposed by the conditions that frame a given problem, they will treat different issues the same through time, based on the utility available in executing the decision. Where the sovereign has limited executive utility, a paladin[8] is elevated to resolve the problem.

This area's academic literature does not fall neatly into a box entitled "Intelligence Community whistleblowing." Advocates for various interests view the issues from different locales. The Intelligence Community employee's act of passing information—lawfully or unlawfully—cuts across several disciplinary areas (constitutional law, criminal law, employment law, administrative law, etc.), making comparison difficult. The bulk of the writing focuses on First Amendment law. For example, Amitai Etzioni writes on the balancing of national security policy and freedom of the press, applying a communitarian model to protect the public's right to know and the press's right to publish.[9] Etzioni advocates using the press to move beyond Congressional disclosure, taking wrongdoing directly to the People as sovereign through the free press.[10] Current law governing the Intelligence Community does not permit such leaking. They maintain a republican, rather than popular, sovereignty approach, in which the People are only sovereign *in Congress*. This raises the perhaps uncomfortable realization that a disclosure of wrongdoing could advance up through the Executive branch and even through the halls of Congress, and not lead to a correction of the problem. Whistleblowing is obligatory for Executive branch employees; acting on whistleblowing is not.

---

[8] The Middle French word *paladin* names the one turned to for a solution to a problem, derived from the "Italian *paladino*, from Old French *palatin*, from the Medieval Latin *palatinus*, courtier, from the Late Latin word for imperial official." *See Paladin Definition*, MERRIAM-WEBSTER DICTIONARY, http://www.merriam-webster.com/dictionary/paladin. *See also* BLACK'S LAW DICTIONARY 423 (4th ed. 1951) (defining "County Palatine").

[9] Amitai Etzioni, *A Liberal Communitarian Approach to Security Limitations on the Freedom of the Press*, 22 WM. & MARY BILL RTS. J. 1141 (2014) [hereinafter Etzioni]. *See also* Yochai Benkler, *National Security Whistleblower Protection in an Indefinite State of Emergency*, 8 HARV. L. & POL'Y REV. 345 (2014).

[10] *See* Etzioni, *supra* note 9, at 1179–1180.

Similarly, Mary-Rose Papandrea's *Leaker Traitor Whistleblower Spy: National Security Leaks and the First Amendment*[11] also approaches Intelligence Community whistleblowing from a First Amendment perspective. She wants the First Amendment to support a distinction between leakers in the public interest and employees engaging in espionage. Such a reading of the law would require a substantial widening of *Pickering v. Board of Education*[12] and its progeny, including *Garcetti v. Ceballos*.[13] It is the intellectual distance between the Papandrea and Vladeck theses presented in Papandrea's article that the Intelligence Community whistleblowing program bridges. The *Garcetti* distinction between whistleblowers as "citizens" or "employees" is in many ways predicated on the growth and maturation of internal whistleblowing programs in providing a safe-haven for employees required to blow the whistle.[14]

Like *Pickering* and *Garcetti, Risen* and *MacLean* are not only cases presented to the United States Supreme Court for resolution; they are also public indicators, or tracers, delineating an area of Federal decision making in which the sovereign exerts limited utility. In a constitutional order placing sovereignty in a People represented in Congress, any Federal mission requiring secrecy will underscore the limited executive utility of transparent and candid processes. In these situations, delegation becomes a means of overcoming limited utility. ICW&SP's mission, delegated from the President to the United States Director of National Intelligence (ODNI or Director) and from him to the Intelligence Community Inspector General, is to support the Intelligence Community Inspector General Forum[15] with programs that promote whistleblowing as an internal function. The goal, in part, is to protect the employees, contractors, and other sources contributing

---

[11] Mary-Rose Papandrea, *Leaker Traitor Whistleblower Spy: National Security Leaks and the First Amendment*, 94 B.U. L. REV. 449 (2014) [hereinafter Papandrea].

[12] 391 U.S. 563 (1968).

[13] 547 U.S. 410 (2006).

[14] *Compare* Papandrea, *supra* note 11, at 526–527, *with* Stephen I. Vladeck, *The Espionage Act and National Security Whistleblowing After Garcetti*, 57 AM. U. L. REV. 1531, 1535 (2008) [hereinafter Vladeck]. The ICPWA in particular provides a safe haven for whistleblowers whose disclosures straddle the orderly conduct of Legislative and Executive branch relations. *See generally* Richard Moberly, *Whistleblowers and the Obama Presidency: The National Security Dilemma*, 16 EMP. RTS. & EMP. POL'Y J. 51 (2012).

[15] The IC IG Forum is a mechanism for (1) informing Forum members of common-interest work, (2) sharing information, (3) circulating best practices, and (4) assisting with access to employees, employees of contract personnel, records, audits, reviews, documents, recommendations, or other materials that may involve or be of assistance to more than one of the member IGs. *See* 50 U.S.C. § 3033(h)(2).

to IG investigations, audits, evaluations and reviews of fraud, waste, and abuse. ICW&SP's creation was the next step in building out the Intelligence Community whistleblowing program President Obama created on October 10, 2012 with the signing of Presidential Policy Directive No. 19 (PPD-19), *Protecting Whistleblowers with Access to Classified Information*.

As ICW&SP organized, the ODNI also issued Intelligence Community Directive 120, *Intelligence Community Whistleblower Protection* (ICD 120). This directive implemented PPD-19 and reiterated Executive Order 12674's tenet: *whistleblowing is not merely a discretionary option; it is not a "nice to have."* Indeed, the ODNI has emphasized that "[p]ersonnel serving in the IC have a *responsibility* to report such violations through Protected Disclosures."[16]

Signed on March 20, 2014, ICD 120 was a response to President Obama's whistleblowing initiatives during the second half of his first term in office. PPD-19's build-out as an IC-wide concern was a deliberate action, discussed and assessed by the Intelligence Community Inspector General and members of the senior leadership in the Office of the Director of National Intelligence, led by the fourth Director of National Intelligence, James R. Clapper. The President signed the policy directive midpassage between two of the most hotly debated information releases during the Southwest Asian wars: those enabled by WikiLeaks on February 18, 2010 and those published by the *Guardian* on June 5, 2013. In this environment, the Intelligence Community returned to deconflicting the difficult and twined national security priorities of fostering *lawful* whistleblowing and protecting sources, while simultaneously executing the United States' intelligence and counter-intelligence missions.

I. ICW&SP'S CONCEPT OF OPERATIONS

[16] OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, INTELLIGENCE COMMUNITY DIRECTIVE 120, INTELLIGENCE COMMUNITY WHISTLEBLOWER PROTECTION, ¶ D.1.b (March 20, 2014), *available at* http://fas.org/irp/dni/icd/icd-120.pdf [hereinafter ICD 120]. As we have noted, intelligence community whistleblowing is not an especially robust journal-writing beat. There is a need for greater writing in this area. *See generally* Moberly, *supra* note 14; Michael P. Scharf & Colin T. McLaughlin, *On Terrorism and Whistleblowing*, 38 CASE W. RES. J. INT'L L. 567 (2007); Mika C. Morse, *Honor or Betrayal? The Ethics of Government Lawyer-Whistleblowers*, 23 GEO. J. LEGAL ETHICS 421 (2010). National security whistleblowing is covered in more depth, somewhat. *See, e.g.*, Papandrea, *supra* note 11; David E. Pozen, *The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information*, 127 HARV. L. REV. 512 (2013).

In its first full year of operation (FY 2014), ICW&SP executed twenty-eight outreach events, conducted seventeen training sessions, processed three reports of urgent concern to Congress, assisted with five Title 50 reports of wrongdoing, docketed four requests for PPD-19 review, and referred four reprisal complaints to local inspectors general. This activity was conducted prior to the rollout of community-wide training on the Intelligence Community whistleblowing program—training that will begin the culture change necessary to make the accepted mission of whistleblowing into a mission that is integrated into doctrine. As doctrine matures and is disseminated, the level of Intelligence Community whistleblowing should accordingly rise.

Since *Risen* and *MacLean* are public indicators—or tracers showing us an area of Federal decision making where the sovereign exerts limited popular utility for the needs of secrecy—the standard treatises articulating the normative consensus on the scope of national security law also reveal that whistleblowing is an area of indecision within the Intelligence Community. Consider, for example, one casebook defining the bounds of this area of law: *National Security Law* by Professor Stephen Dycus et alia.[17] Part IX of this treatise is where one would expect to find a substantive discussion of Intelligence Community whistleblowing. Chapter forty-two*, Restraining Unauthorized Disclosures on National Security Information*, would perhaps, under an intellectual rubric in which the Federal mission of whistleblowing was not only accepted but promoted, be followed by a chapter forty-three entitled *Promoting Lawful Disclosures through the Intelligence Community Whistleblowing Program*. Instead, this treatise, which provides a normative standard within the field of national security law, has a chapter forty-three entitled *Restraints on Publication of National Security Information*.[18] By encouraging awareness, ICW&SP should hopefully mitigate this lack of information and encourage Intelligence Community whistleblowing in the process.

Whistleblower—or source—protection[19] in the IC is not the same as protection of an employee's civil liberties or First Amendment rights to

---

[17] STEPHEN DYCUS, ARTHUR L. BERNEY, WILLIAM C. BANKS & PETER RAVEN-HANSEN, NATIONAL SECURITY LAW (5th ed. 2011).
[18] *Id*. at 1229–79.
[19] First Amendment protections, while valued, are distinct from whistleblower protections. Even when disclosures are lawfully made by non-IC employees via the media, the theory is that the media is merely a conduit to some entity which may correct the wrongdoing, like Congress. When you remove the media as a recipient of the disclosure, as the President has done via PPD-19, the resulting system is

speech and assembly. Whistleblowing is the lawful communication of wrongdoing to one who can correct the wrongdoing. Such whistleblowing has been required of all Executive branch employees—including those within what would become the statutorily-defined Intelligence Community—since 1989. Wrongdoing, in turn, does not include analytical or policy disputes. There can be a tendency for an unstudied confusion of the two differing traditions, one rooted in civil liberties and the other in internal management controls and, in extreme cases, Congressional oversight.

IC whistleblower protection mostly seeks to protect sources reporting the internal corruption that all Federal employees have been required to report under Executive Order 12674.[20] Much of this reporting involves simple Executive branch management issues such as time and attendance abuse, gross waste, mismanagement, and workplace violence. The disclosures that receive the most attention, however, are usually those that trigger constitutional concerns under the separation of powers doctrine, including the constitutional sub-doctrine of executive privilege. It is when the whistleblower provides the information Congress needs in order to perform the legislature's role in representing "the sovereign" that tension is usually most evident.[21] At the core of the IC whistleblowing process is the sovereign's "need to know" as that need is satisfied through the normal working relations between the Legislative and Executive branches.[22] As such, this national secu-

---

wholly internal. *See* EXEC. OFFICE OF THE PRESIDENT, PRESIDENTIAL POLICY DIRECTIVE/PPD-19, PROTECTING WHISTLEBLOWERS WITH ACCESS TO CLASSIFIED INFORMATION (Oct. 10, 2012), *available at* http://www.whitehouse.gov/sites/default/files/image/ppd-19.pdf [hereinafter PPD-19]. It is a system of protecting sources essential to maintaining internal controls within the Executive branch.

[20] Exec. Order No. 12,674, 54 Fed. Reg. 15,159 (April 12, 1989), pt. I, §101(k), *amended by* Exec. Order No. 12,731, 55 Fed. Reg. 42,547 (Oct. 17, 1990) [hereinafter Exec. Order No. 12,674].

[21] The more routine disclosures of everyday workplace wrongdoing may not raise general tension because they are largely not visible outside the agency. Inspectors general, for instance, do not automatically release their reports regarding senior officials and flag officers due to Freedom of Information and Privacy Act concerns. *See* 5 U.S.C. § 552(b)(7).

[22] There are three other areas of law that overlap with the whistleblower protection. First, if a whistleblower seeks information to prove that he or she has suffered retaliation, Executive branch officials may deny the request under an application of the Privacy Act and/or Freedom of Information Act. Over-application of these statutes can have the perverse effect of denying the public examples of their government officials *acting appropriately to protect* whistleblowers and *disciplining* management officials for engaging in reprisals after a whistleblowing incident. Second, the laws and regulations governing the detection and assessment of Insider Threats hold the potential to trigger unauthorized disclosure investigations. Third, given the cen-

rity priority can very quickly draw an employee out of the close, safe confines of their cubicle and into a nasty fight at very high levels.

The failure to adequately provide for the accepted Federal mission of whistleblowing in the normative language of national security law and policy, for instance, reinforces the confusion regarding whistleblowing within the Intelligence Community in a manner similar to the confusion generated by the national and Beltway media's use of the word "whistleblower." The lack of attention to semantic uses, demonstrated by the failure to distinguish and discriminate between, say, "leaking" and whistleblowing, has led IC employees to think whistleblower protection either protects or fails to protect those reprised against after a "politicization" of the intelligence and counterintelligence mission. "Politicization" lies within the realm of analytic and policy disputes between Executive branch employees. Analytic and policy disputes in and of themselves cannot generate protected communications, that is, disclosures. "Wrongdoing," as in a violation of law, rule, or regulation, generates protected communications.[23]

The promotion of whistleblowing *as an accepted Federal mission* engaging all supervisors, managers, and employees enables the Federal bureaucracy to curtail domestic, internal corruption. Understanding this statement is not easy for the national security professionals who came of age

---

trality of agency law departments to the legal sufficiency review of whistleblower reprisal findings, the decentralized nature of Federal attorney professional responsibility can lead to an imbalance in the relations between client and attorney as whistleblower investigations unfold. For an assertion of sovereignty in the "need to know" debate, see Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 701, 112 Stat. 2396, 2413 (1998) (finding that "Congress, as a co-equal branch of Government, is empowered by the Constitution to serve as a check on the Executive branch; in that capacity, it has a 'need to know' of allegations of wrongdoing within the executive branch, including allegations of wrongdoing in the Intelligence Community.").

[23] *Compare* Margo Schlanger, *Intelligence Legalism and the National Security Agency's Civil Liberties Gap*, 6 HARV. NAT. SEC. J. 112 (2015) (advocating policy options which limit the exercise of actions permissible at law in order to mitigate privacy and civil liberties risks and costs); Richard Morgan, *Latif v. Obama: The Epistemology of Intelligence Information and Legal Evidence*, 22 S. CAL. INTERDISC. L.J. 303 (2013) (presenting the general concern with politicization of intelligence information), *and* Robert Bejesky, *The SSCI Investigation of the Iraq War: Part I Politicization of Intelligence*, 40 S.U. L. REV. 243 (2012) (same)) (two articles presenting the general concern with politicization of intelligence information) *with* Major William E. Brown, *Whistleblower Protection for Military Members*, DA PAM 27-50-427 ARMY LAW. 58 (2008) (presenting the general outline of a protected communication as relating to "wrongdoing").

being taught that *all* Intelligence Community whistleblowing was unlawful. By signing PDD-19, President Obama reaffirmed the federal whistleblowing mission first established by President George H.W. Bush on April 12, 1989.[24] The corruption to be reported is the very corruption that can undo the excellent work of our Armed Services and Intelligence Community assets safeguarding the Republic against foreign enemies abroad.[25] The threat is 360 degrees, created by all enemies foreign and domestic.[26] An IC employee or contractor may make a lawful disclosure through a variety of venues. IG hotlines or personal meetings with IG officials afford the whistleblower statutory protection from reprisal after making such disclosures pursuant to the Inspector General Act of 1978 and the National Security Act of 1948, as amended, and the Intelligence Community Whistleblower Protection Act of 1998, as amended.[27] Similarly, other compliance offices have the authority and/or responsibility to receive specialized disclosures, like violations of equal employment laws or civil liberties and privacy laws.[28]

II. A PALADIN THEORY OF FEDERAL DECISION MAKING

The concept of operations detailed above is best understood through a particular leadership and management lens. Since 1991, whistleblowing has been an Executive branch mission required by the Executive Office of the President through Executive Order 12674. While the legislative mandates of Congress are central to American governance, even without specific Congressional requirements, Executive branch employees are required to report corruption through actions under the President's constitutional au-

---

[24] Exec. Order No. 12,674, *supra* note 20, at pt. I, §101(k) ("Employees *shall* disclose waste, fraud, abuse, and corruption to appropriate authorities.") (emphasis added).

[25] In doing this, it is important to understand whether the word "whistleblower" is being used in the vernacular or legal sense. For the purposes of conducting investigations, "whistleblower" is a legal term of art. It relates to *lawful* disclosures as well as a specific process for bringing certain classified and unclassified matters to the attention of those who may correct the wrongdoing. "Whistleblowing" does not include policy disputes over programs or activities. In contrast, *unlawful* communications are not "whistleblowing," they are "leaks" in the vernacular and may subject the leaker to criminal prosecutions, civil penalties, and administrative disciplinary actions.

[26] The Honorable James R. Clapper, Director of National Intelligence, Remarks at the AFCEA/INSA National Security and Intelligence Summit (Sept. 18, 2014).

[27] *See* 5 U.S.C. App. 3 §§ 7(c), 8H (2012); 50 U. S. C. §§ 3033(g)(3)(B), 3033(k)(5)(A), 3517(d)(5)(A), 3517(e)(3)(B) (2012).

[28] For example, the ODNI's Civil Liberties and Privacy Office (CLPO) has the responsibility to investigate privacy and civil liberties complaints within ODNI as well as to refer complaints relating to other IC elements to their IGs.

thority. Once a Federal employee reports corruption, however, the nature of protection attached to whistleblowing varies greatly across the Executive branch. Both Congress and the President have provided for protection piecemeal, reacting to events in fits and starts. It is the status of the employee that determines the scope of protection, not the act of reporting corruption itself. The legislative landscape protecting whistleblowers is not a homogenous plain; it is a varied glacial landscape replete with cirques, cols, horns, tarns, and hanging valleys.

This law review article sketches the unique circumstances framing the reporting of corruption within the Intelligence Community. The authors come to the topic with extensive experience and a unique perspective. They are both adherents to a paladin theory of American governance: the understanding that even as a society progresses, fundamental and immutable limitations on human decision making determine core aspects of governing systems. The ambit of what we *may* govern may exceed discrete institutions' capacity to make and execute the decisions *necessary* to govern,[29] leaving specific relationships transcendent, constant in time—relationships which form a distinct decision-making game space. Federal decision making generally evinces such broad concepts—*gubernaculum* and *jurisdictio*—which shape an information game space rooted in historical practices.[30] *Gubernac-*

---

[29] A nation-state's juridical center is its legal "hearth"; an area (physical or intellectual) furthest from the hearth and least-ordered from the center would be the "march." Professor Stephen I. Vladeck has written a thoughtful piece on the challenges of ordering Intelligence Community whistleblowing from the hearth. *See* Vladeck, *supra* note 14. But some cases straddle both hearth and march. *See* Jane Mayer, *The Secret Sharer: Is Thomas Drake an Enemy of the State?*, THE NEW YORKER, May 23, 2011 (discussing both hearth-directed Article III judicial filings as well as an administrative, inspector general–led investigation in what this article would label "march decision making").

[30] *See* Alfredo Gallego Anabitarte, *Administracion y Jueces: Guberativo y Contensciso*, *in* FESTSCHRIFT FÜR KARL LOEWENSTEIN: AUS ANLASS SEINES ACHTZIGSTEN GEBURTSTAGES 1–49 (Henry Steele Commager ed., 1971) (describing Professor McIlwain's 1949 articulation of Henri de Bracton's distinction between the two medieval concepts); CHARLES HOWARD MCILWAIN, CONSTITUTIONALISM, ANCIENT AND MODERN (rev. ed. 1947) [hereinafter MCILWAIN]. *See also* Jesselyn Radack, *A Legal Defense of Russell Tice, the Whistleblower Who Revealed the President's Authorization of NSA's Warrantless Domestic Wiretapping*, FINDLAW.COM (Jan. 27, 2006), http://writ.news.findlaw.com/commentary/20060127_radack.html; Dan Meyer & Everett Volk, *"W" for War and Wedge? Environmental Enforcement and the Sacrifice of American Security—National and Environmental—to Complete the Emergence of a New "Beltway" Governing Elite*, 25 W. NEW ENG. L. REV. 41, 71. (2003) [hereinafter Meyer &Volk]. The 9/11 attacks provided a decision moment regarding the end of what had been a very indecisive

ulum is the reach of the executive's authority, what we lawyers used to call the run of the King's Writ. *Jurisdictio* is the reach of the sovereign or polity's law, regardless of whether the king's rider can execute the writ. Where the law exists and the King's Writ cannot ride, the Queen or King establishes a *paladin* to either execute the law or make it *de novo*. In the Middle Ages, this could be a geographical construct, such as a "march" or "pale," or a political reality, as in the creation of a palatine or regulus to accommodate a powerful interest. Effectively, when the Queen or King cannot order society, she or he attempts to create and then leash a surrogate.[31]

Historical metaphors create intellectual marshes. But the use of history as metaphor saturates the tradition of constitutional government, which is driven by a skeptical and "not unrelievedly dark view of human nature and by the unfashionable idea that history contains lessons for statesmen."[32]

---

decade in the crafting of the American national security narrative, 1991 to 2001. "Environmental security" had been the narrative on the rise. It was soon eclipsed following the attack. *See generally* RITA FLOYD, SECURITY AND THE ENVIRONMENT: SECURITISATION THEORY AND U.S. ENVIRONMENTAL SECURITY POLICY 134, 140–45 (2010).

[31] Hearth-to-march decisions are not confined to national security law. "Change" drives reform in any area of law, sometimes moving decision making from a forum of lower discretion to one of higher discretion―from law to regulation to fiat―essentially from hearth to march. Sports law is one such area marked by recent change. The change was the increasing commoditization of athletes. *See generally*, Virginia A. Fitt, *The NCAA's Lost Cause and the Legal Ease of Redefining Amateurism*, 59 DUKE L.J. 555, 573 (2009) (citing Deborah E. Klein & William Buckley Briggs, *Proposition 48 and the Business of Intercollegiate Athletics: Potential Antitrust Ramifications Under the Sherman Act*, 67 DENV. U. L. REV. 301 (1990)).

[32] Rolf H. Weber & Shawn Gunnarson, *A Constitutional Solution for Internet Governance*, 14 COLUM. SCI. & TECH. L. REV. 1, 52 n.264 (2013)(citing THUCYDIDES, THE LANDMARK THUCYDIDES bk. 1, 16 (Robert B. Strassler ed. & Richard Crawley trans., 1996); LIVY, THE HISTORY OF ROME 3-4 (Valerie M. Warrior ed., 2006)); Lord Bolingbroke, *Letters on the Study and Use of History, in* HISTORICAL WRITINGS 61-62 (Isaac Kramnick ed., 1972); and Thomas Jefferson, Letter to John Norvell (June 14, 1807), *reprinted in* JEFFERSON: WRITINGS 1176 (Merill D. Peterson ed., 1984)). With this string of citations above, Weber and Gunnarson present a cautionary flag regarding the use of history in contemporary decision making. But in history, one can find the distance between hearth and march reflected not only in physical distance translated into the law but also in political distance translated into philosophy. During England's Augustan age, Lord Bolingbroke's 'Country party' was contrasted with the Westminster-center hearth and its 'Court party'. American Whigs and Tories need not find their roots in 'country' and 'court' to be influenced by similar human relationships transcendent through time. *See generally* ISAAC KRAMNICK, REPUBLICANISM AND BOURGEOIS RADICALISM: POLITICAL IDEOLOGY IN LATE EIGHTEENTH-CENTURY ENGLAND AND AMERICA (1990); ISAAC

And when you recognize that medieval jurisprudence was, in part, an attempt to address the differing status of decision makers, there are constants that inform even Federal constitutional decision making in the twenty-first century. The prudent Federal actor understanding his or her environment through game theory can use concepts such as *gubernaculum* and *jurisdictio* to understand the choices presented by a particular instrument of authority, such as Executive Order 12674.[33] In the American system, the People are sovereign (*gubernaculum*, read: Queen or King) and that sovereignty vests in Congress assembled. The President executes the will of the sovereign (*jurisdictio*), as it is articulated in law passed by the Congress, which oversights the Executive branch to ensure that the will of the sovereign is executed.[34] Within the ambit of the law, the President may—at her or his discre-

---

KRAMNICK, BOLINGBROKE AND HIS CIRCLE: THE POLITICS OF NOSTALGIA IN THE AGE OF WALPOLE (1992); Perez Zagorin, *The Court and the Country: A Note on Political Terminology in the Earlier Seventeenth Century*, 77 ENG. HIST. REV. 306 *(*April 1962). In Bolingbroke's paradigm, the impulse to delegate or to assume delegation may not be a matter of decision making utility, but rather of avoiding authority itself. *See also* JAMES C. SCOTT, THE ART OF NOT BEING GOVERNED: AN ANARCHIST HISTORY OF UPLAND SOUTHEAST ASIA (2010). *Compare* GRAHAM ROBB, THE DISCOVERY OF FRANCE: A HISTORICAL GEOGRAPHY (2008) (noting the fractious nature of alleged "French" society prior to the 20th century).

[33] By understanding both the scope and strength of *gubernaculum* and *jurisdictio*, the prudent Federal whistleblower works through the resulting statues, enabled by directives implemented via instructions and policies, to overcome the "strategy of conflict" created by whistleblowing. For the application of game theory to the mutual, anticipatory engagement between supervisors, managers and employees in this environment, see THOMAS SCHELLING, THE STRATEGY OF CONFLICT (1960). In understanding each other's options under the rules regulating Intelligence Community whistleblowing, supervisors, managers, and employees can anticipate the effect of their actions and proceed accordingly, allowing the underlying mission of the Federal office to continue while the disclosure moves forward.

[34] One constitutional touchstone requires listening to a speaker's use of the word "sovereign": is the institution to which the speaker is attributing sovereignty *truly* sovereign under American law? *Compare* Mike Allen, *Bush's Choices Defy Talk of Conciliation; Cabinet Is Diverse but Not Politically*, WASH. POST, Jan. 1, 2001 ("'[T]he country deserves governance and if you don't assert the sovereignty and legitimacy of your administration from the outset, you undermine your ability to achieve your goals later.'") *with Hearing to Consider the Nominations of: Gen. Paul J. Selva, USAF, for Reappointment to the Grade of General and to be Commander, U.S. Transportation Command; and VADM Michael S. Rogers, USN, to be Admiral and Director, National Security Agency/Chief, Central Security Services/Commander, U.S. Cyber Command Before the S. Comm. on Armed Serv.*, 113th Cong. 13 (2014) (statement of Vice Admiral Michael S. Rogers, United States Navy) ("Sir, I believe that one of my challenges as the director, if confirmed, is how do we engage the American people, and by extension, their representatives,

tion—issue executive orders or presidential policy directives to arrange the affairs of the Executive branch.

Principles of jurisprudence are transcendent. They exist *in* time for the decision maker with the facts in hand, but they are *through* time in that the challenges, for which the principles are developed, that decision makers face can be remarkably similar. The juridical principles of *jurisdictio* and *gubernaculum* used to order a medieval *physical* space can be likewise used to order a post-modern *intellectual* space showing the same aspects of, say, a medieval march. The salient characteristics of the medieval marches abolished by the statute 27 Hen. VIII. c. 26 lay in the fact that they were boundaries and limits between adjacent sovereigns.[35] In these spaces, a sovereign may have *de jure* power to run his or her writ, but not *de facto* power to do the same. The mismatch between *de jure* potential and *de facto* reality creates a game space unique to the march, a set of conditions that must be addressed on their own terms.[36]

---

in a dialogue in which they have a level of comfort as to what we are doing and why. It is no insignificant challenge for those of us with an intelligence background, to be honest."). Admiral Rogers' statement at his NSA director confirmation hearing reflects a quintessentially American, people-centric model of sovereignty vested in the Congress, as representative of the people, whereas the former statement is a very European, individual-centric model of sovereignty vested in a person, such as a president or monarch.

[35] *Compare* BLACK'S LAW DICTIONARY 1119 (4th ed. 1951) (defining "Marches"), *with id.* (defining "Marchers").

[36] The authors borrow the term "game space" from the technology field to delineate the mission of Federal decision making from the environment in which those decisions are made. *See generally* ERNEST ADAMS & JORIS DORMANS, GAME MECHANICS: ADVANCED GAME DESIGN 230–31 (2012). The four-variable paladin model for Federal decision making owes inspiration, in part, to Professor Idleman's seminal piece, Scott C. Idleman, *A Prudential Theory of Judicial Candor*, 73 TEX. L. REV. 1307, 1396–97 (1995). In it, Professor Idleman cites two Federal decision makers on the importance of narrative formation and conceptualization to profession definition. *See id*; Richard A. Posner, *The Decline of Law as an Autonomous Discipline: 1962–1987*, 100 HARV. L. REV. 761, 766–67 (1987) (arguing that a decline in political consensus, the prevalence of disciplines that are "complementary" to law, and a "collapse" in lawyers' faith in their ability to solve major problems in the legal system have led to a decline in "faith in law's autonomy as a discipline"). *See also* Andrew C. Barrett, *Deregulating the Second Republic*, 47 FED. COMM. L.J. 165, 170 n.19 (1994) (noting with some concern that "[a]s the legal academy no longer promotes a common, unified professional language, less intellectual comity may exist between future lawyers") [hereinafter Barrett]; Richard A. Posner, *The Material Basis of Jurisprudence*, 69 IND. L.J. 1, 26–30 (1993) (conceptualizing and charting the transformation of law and the legal profession by reference to cartel theory and the history of medieval craft guilds). The Intelligence

The same principles of jurisprudence inform *intellectual* spaces, in which a sovereign may have *de jure* power to run their collective writ, but not *de facto* power to do the same. The American people are sovereign and represented in Congress. But the same sovereign's need for secrecy in order to execute the Federal intelligence and counterintelligence missions makes the *de jure* power to receive information regarding government operations problematic. *De facto* exercise of this power is limited, hence the metaphorical echo of a medieval march. Within this American constitutional game space, four juxtaposed variables generally affect the application of *gubernaculum* and *jurisdictio* to Intelligence Community whistleblowing: on the one side, opacity and prudence, on the other transparency and candor.

Federal decision makers in the Intelligence Community apply these four characteristics of decision making, whether explicitly or implicitly, every day. These characteristics are also the values that frame the game space of Federal whistleblowing across the board, including outside the Intelligence Community.[37] When IC supervisors, managers, and employees find, for operational reasons, that prudence and opacity are essential for success, you are in an area of decision making marked by high discretion and great secrecy. In the other direction, the need for transparency and candor is often indicative of areas of decision making marked by a need for many actors to have access to high levels of information.[38] The free market

---

Community has its own narrative forms, which are central to the professional definition of itself. One challenge in building out an Intelligence Community whistleblowing program is to deconflict the IC's internal security and counterintelligence culture with a coequal narrative that now requires the protection of lawful whistleblowers. *See generally* Koen Vermier & Dániel Margócsy, *States of secrecy: an introduction*, 45 BRIT. J. HIST. & SCI. 153, 159 n.38 (2012) (citing Michael Aaron Dennis, *Secrecy and science revisited: from politics to historical practice and back*, *in* SECRECY AND KNOWLEDGE PRODUCTION (Judith Reppy ed., 1999)). The impact of institutional ignorance is studied through "Agnotology." *See* AGNOTOLOGY: THE MAKING AND UNMAKING OF IGNORANCE (Robert Proctor & Londa Schiebinger eds., 2008).

[37] *See generally* LOUIS FISHER, CONG. RESEARCH SERV., RL33215, NATIONAL SECURITY WHISTLEBLOWERS (2005), *available at* http://www.fas.org/sgp/crs/natsec/RL33215.pdf.

[38] Perhaps counterintuitively, the Cold War law–defined narrative articulating American national security gave *greater* discretion to the President in order to *limit the unpredictability* imparted by Congressional decision-making. Normally, one would associate greater discretion with higher levels of unpredictability. For a description of the narrative process, see Aziz Rana, *Who Decides on Security?*, 44 CONN. L. REV. 1417, 1487 (2012) (citing DAVID CAMPBELL, WRITING SECURITY:

is one such forum. For the IC, matters relating to external credibility with oversight authorities would fall into this category. Law, American and/or international, is required as a substructure to the game spaces created by the interaction of value characteristics, such as opacity, prudence, transparency, and candor. And it is through the law—statutory or case—that the four values are applied. Both the game spaces of the free market and intelligence collecting and analysis, as extremes, are marked by paladin decision making, in which *gubernaculum* is weak and yet *jurisdictio* remains. Both have marches that lie beyond the exercise of the law. Away from these extremes, a hearty mix of all four characteristics marks the more grounded areas of decision making.[39] Think real property law, tax law, insurance law, or the Uniform Commercial Code as such a juridical hearth.[40] There may also be

---

UNITED STATES FOREIGN POLICY AND THE POLITICS OF IDENTITY (1998)). *See also* Barrett, *supra* note 36, at 174.

[39] Mr. Meyer first advanced what he would later identify as the paladin theory of Federal decision making while clerking for the FCC's commissioner Andrew C. Barrett some twenty years ago, during the run-up to the Telecommunications Act of 1996, Pub.L. 104-104, 110 Stat. 56 (1996). The question then was whether the FCC had developed into its own semi-autonomous, decision-making self. *See* Barrett, *supra* note 36, at 168–169 ("But this alleged juridical flight from regulation is deceiving. Indeed, the time has come for American institutions to address the question of whether the Commission, and its peers, have evolved into complex decision-making bodies not unlike Article III courts."); *see also id.* at 171 ("Born of a legal regime based in delegation of powers (to independent agencies), and evincing broad, general mandates (in the form of legislative standards), the Communications Act of 1934 was emergency legislation rescuing a sector of the American economy from general market failure."). Pales, or palatines—effectively decision-making *marches*—are born of some institutional failure, whether market, political, or in capacity, leading to a variance in the relative ambits of *gubernaculum* and *jurisdictio*.

[40] *Compare* Ethan Yale, *Taxing Market Discount on Distressed Debt*, 32 VA. TAX REV. 703 (2013) (Professor Yale writes at the hearth, dealing with the interaction of statutory and common law principles in an area of law—taxation—where the majority of Federal decision makers administering the law are firm in their commitment to as little discretion as possible, and greater levels of certainty so as to not disturb the expectations of the taxing, or the taxed, as they order their affairs) *with* Kenneth A. Klukowski, *Severability Doctrine: How Much of a Statute Should Federal Courts Invalidate?*, 16 TEX. REV. L. & POL. 1, (2011) (citing Alfred Hayes, Jr., *Partial Unconstitutionality with Special Reference to the Corporation Tax*, 11 COLUM. L. REV. 120, 141 (1911) (discussing how in tax law, Article III courts have played the critical role in defining the ambit of taxation, crafting opinions which have curtailed discretion and thereby limiting the decision-making march); *see also* Richard R.W. Brooks & Carol M. Rose, SAVING THE NEIGHBORHOOD: RACIALLY RESTRICTIVE COVENANTS, LAW, AND SOCIAL NORMS (2013) (Professor Brooks' study examining change real property, one area of law that had been known for

situations where acts of a sovereign are ultra-march, or "beyond the Pale." This would be in the realm of outlawry as defined by a writ of *exegi facias*. A much-misused word, the concept has come to be synonymous with simple criminal behavior. By definition, however, it connotes being "beyond the law," whether administered at a hearth or in a march. This concept cuts through any number of areas of law, including international relations.[41]

Gubernaculum, termed "domination" by the theorist Max Weber, extends in both terms of time and place to that point at which there is a "probability that a command with a given specific content will be obeyed by a given group of persons." It is defined by the power relationships allowing an institution to claim a right to govern.[42]

---

certainty and that required change to meet changing social norms). For another hearth-to-march example, banking regulation underwent profound changes after 1982. *See generally* Peter D. Wimmer, *Are the Floodgates Now Open for the "Business of Banking" after NationsBank of North Carolina, N.A. v. Variable Annuity Life Insurance Co. (VALIC),* 15 ST. LOUIS U. PUB. L. REV. 505 (1996) (citing Professor Edward Symons, Jr., *The "Business of Banking" in Historical Perspective*, 51 GEO. WASH. L. REV. 676 (1983)). Pay close attention to how the Supreme Court chose among several theories in deciding the case. This is the federal decision making that moves issues from march to hearth and vice versa. For an early example of hearth-to-march decision making, *see* Barrett, *supra* note 36, at 168 ("The Court foreclosed the judiciary's last substantive ties to what was once a judicial power—economic regulation.").

[41] *See* Eliana I. Kalivretakis, *Are Nuclear Weapons Above the Law? A Look at the International Criminal Court and the Prohibited Weapons Category*, 15 EMORY INT'L L. REV. 683, 729 n.223 (2001) (citing Jonathon Granoff, *Nuclear Weapons, Ethics, Morals, and Law*, 2000 BYU L. REV. 1413, 1433 (2000) and Stephen J. Hadley*, Debate: Policy Considerations in Using Nuclear Weapons*, 8 DUKE J. COMP. & INT'L L. 23, 24–25 (1997)). *See also* Toby S. Goldbach, Book Review, *Theory and Practice of Harmonization*, 41 INT'L J. LEGAL INFO. 222, 226 n.9 (2013) (citing Toby Goldbach, Benjamin Brake & Peter Katzenstein, *The Movement of U.S. Criminal and Administrative Law: Processes of Transplanting and Translating*, 20 IND. J. GLOBAL LEGAL STUD. 141 (2013)) (discussing how law moves between sovereign jurisdictions).

[42] *See* MAX WEBER, ECONOMY AND SOCIETY 53 (Guenther Roth & Claus Wittich eds., Ephraim Fischoff et al. trans., 1978) ; *see also* Norman Uphoff*, Distinguishing Power, Authority & Legitimacy: Taking Max Weber at His Word by Using Resource-Exchange Analysis*, 22 POLITY 295, 302 (1989). These constitutional principles are broadly compatible with the economist's and common law lawyer's concepts of principal and agent. Agency law is rooted in the ecclesiastic critique of Roman law, which generally lacked the concept of agency. The civil, statist traditions—practiced by modern Romans—look to central planning, direct regulation, command and control, etc. as tools substituting for a march. Medieval and even Renaissance society struggled with distance in a manner that classical antiquity did

Institutional characteristics change over time, and even between decisions, individual decision makers may emphasize one characteristic over another in a different manner than they had in an earlier but similar manner. Opacity, for instance, which drives the need for secrecy, varies as national security conditions change. During the Cold War, near-complete scientific secrecy marked Russo–American relations. Today, China and the United States do develop some technologies together.[43]

The theoretical background above, while a little dense, is essential to understanding the unique nature of Intelligence Community whistleblowing. The *de facto* delegation of function (arguably, constitutional powers are shared while the functions are unique) that occurred in the ordering of Intelligence Community whistleblowing is more than mere administrative routine or simple social choice. It was a concession to functionalism predicated on the unique nature of the IC, a nature dominated by a system of secrecy.[44]

---

not. So the same canon laws creating delegation in the West and giving persuasive precedent to the King's attorneys ordering the march also probably informed the common law judges crafting agency law to empower the early Renaissance aristocracy and merchants in their commercial practices.

[43] Joel B. Eisen, *China's Greentech Programs and USTR Investigation*, 11 SUSTAINABLE DEV. L. & POL'Y 3, 7 n.143 (2011) (citing Hugh Gusterson, *Secrecy, Authorship and Nuclear Weapons Scientists, in* SECRECY AND KNOWLEDGE PRODUCTION 57, 69 (Judith Reppy ed., 1999) (discussing the "intense secretiveness of the Soviet state")).

[44] *But see* Barrett, *supra* note 36, at 175 (citing ALFRED C. AMAN, JR. & WILLIAM T. MAYTON, ADMINISTRATIVE LAW 31 (1993), which articulates the conventional wisdom underlying administrative delegation of powers as a choice between a primary social choice or a matter of administrative routine). *See also id.* at 177–78 ("When Henry Bruére, Director of the Bureau of Municipal Research, City of New York, reviewed that municipality's initial foray into regulation, he noted that independent agencies were the cautious solution to a problem attracting more crazed arguments for state ownership. Reform was cautious, deliberative and thoughtful") (citing Henry Bruére, *Public Utilities in New York*, 31 ANN. AMER. ACAD. POL. & SOC. SCI 535, 535 (1908); Bringham Daniels*, Agency as Principal*, 48 GA. L. REV. 335, 339, n.14 (2014) (citing Alan Brinkley, *The Challenge to Deliberative*, *in* NEW FEDERALIST PAPERS: ESSAYS IN DEFENSE OF THE CONSTITUTION 23, 25 (1997), which discusses how bureaucracies can act as a buffer between popular will and public action); THEODORE J. LOWI, THE END OF LIBERALISM 92–94 (2d ed. 1979) (criticizing Congress for broad delegations); DAVID SCHOENBROD, POWER WITHOUT RESPONSIBILITY: HOW CONGRESS ABUSES THE PEOPLE THROUGH DELEGATION 99–106, 135–52 (1993) (discussing how Congress secures political power through broad delegations); Terry M. Moe, *The Politics of Bureaucratic Structure*, *in* CAN THE GOVERNMENT GOVERN? 267, 327–29 (John E. Chubb & Paul E. Peterson eds., 1989) (discussing how presidential and Congressional control of

Whistleblowing is candid and transparent; the Intelligence Community is prudent and opaque. For these two Executive branch missions to coexist, they must be coordinated in a manner perhaps new and unique to the IC. At the heart of this coordination is the reconciliation of many governance functions, including oversight (both departmental and Congressional), counterintelligence security, and the whistleblowing itself.

III. CONTEXT FOR FEDERAL DECISION MAKING

The role of whistleblowers repeatedly has become an issue of public focus in recent years. In the aftermath of the first serious foreign attack on North American soil since the War of 1812, the Congressionally empanelled 9/11 Commission acknowledged public disclosure as "democracy's best oversight mechanism."[45] And *Time* even selected two whistleblowers as the Persons of the Year in 2002,[46] highlighting FBI Special Agent Coleen Rowley's disclosure of intelligence failures leading up to 9/11. In so doing, it exemplified the heightened awareness and scrutiny of government intelligence programs in the press and public eye.[47] In 2009 and 2012, protracted public discussions on the distinction between whistleblowing and leaking began after WikiLeaks and *Guardian* both released information regarding the national security policy and operations of the United States.[48]

---

agencies can sometimes conflict, and speculating "that the current administrative tangle may actually get worse over time"); Theodore J. Lowi, *Two Roads to Serfdom: Liberalism, Conservatism and Administrative Power*, 36 AM. U. L. REV. 295, 296 (1987) ("[T]he delegation of broad and undefined discretionary power from the legislature to the executive branch deranges virtually all constitutional relationships and prevents attainment of the constitutional goals of limitation on power, substantive calculability, and procedural calculability.").

[45] PROJECT ON GOVERNMENT OVERSIGHT, HOMELAND AND NATIONAL SECURITY WHISTLEBLOWER PROTECTIONS: THE UNFINISHED AGENDA (2005), *available at* http://www.pogo.org/our-work/reports/2005/wi-wp-20060428.html [hereinafter PROJECT ON GOVERNMENT OVERSIGHT].

[46] Richard Lacayo & Amanda Ripley, *Persons of the Year 2002: The Whistleblowers*, TIME, Dec. 30, 2002.

[47] *Id.*

[48] In general, "right to know" First Amendment theories have teetered in the balance since the 1980s. American jurisprudence could have developed these doctrines aggressively after the Watergate era (which includes the Church Committee's highlighting of Intelligence Community civil rights and foreign intelligence abuses). But that did not happen. Even the litigation over James Risen's sourcing, recently before the U.S. Supreme Court and denied certiorari, merely asked whether journalists have a privilege rooted in our First Amendment freedom of the press not to reveal sources, when those sources are under criminal prosecution. It was not reviewing whether sources contacting journalists have a public interest privilege when

The post-9/11 Federal game space was ideally suited for the emergence of whistleblowers within the nation's intelligence agencies. But protections for people like Special Agent Rowley who made Intelligence Community disclosures waned prior to 2012. Senator Charles Grassley testified, "Since September 11th, government agencies have placed a greater emphasis on secrecy and restricted information for security reasons," focusing less on protecting whistleblowers.[49] Here we see evidence of governing institutions making paladin choices between transparency and opacity, prudence and candor. Such an insular focus can encourage reprisal against whistleblowers. Between the 9/11 attacks in 2001 and the issuance of a report in 2005, the number of whistleblowers seeking protection from retaliation jumped by nearly fifty percent, spiking specifically for those reporting national security concerns.[50] Condoning retaliation negatively impacts government accountability by discouraging whistleblowers. Employees most often fail to make disclosures because they either believe no change will occur or they fear retaliation.[51] Disapproval of whistleblowers and a corresponding lack of oversight afflict the intelligence agencies disproportionately due to porous legal protections and a premium on secrecy. The issuance of Executive branch regulations PPD 19 and ICD 120 sought to remedy this management failure.

IV. THE INTELLIGENCE COMMUNITY AS PALATINE OR MARCH

Thus far, we reviewed ICW&SP's concept of operations in Section I. We then articulated in Section II an analytic lens—in the form of a paladin theory of Federal decision making—which explains why the Legislative and Executive branches chose a delegated decision-making structure when creating the Intelligence Community whistleblowing program. Section III provided a transitional review of the context in which this Federal decision making occurred. Now in Sections IV and V, we apply the paladin theory of Federal decision making to the creation of an Intelligence Community whistleblowing program.

---

disclosing unlawfully. *See generally* Rosanna A. Cavanagh, *James Risen's Litigation: A Turning Point for Press Freedoms*, NEW ENGLAND FIRST AMENDMENT COAL. (Feb. 3, 2014), http://nefirstamendment.org/james-risens-litigation-turning-point-press-freedoms/.

[49] *Compare* PROJECT ON GOVERNMENT OVERSIGHT, *supra* note 45, *with* William E. Lee, *Deep Background: Journalists, Sources, and the Perils of Leaking*, 57 AM. U. L. REV. 1453 (2008).

[50] *See* PROJECT ON GOVERNMENT OVERSIGHT, *supra* note 45, at 3.

[51] *See id.*

The law formerly provided few whistleblower protections to employees within the Intelligence Community. While the Executive branch transgressions of public trust in the 1950s, 1960s, and 1970s produced general legislative whistleblower reform through the Civil Service Reform[52] and Inspector General Acts of 1978,[53] the Military Whistleblower Protection Act of 1988,[54] the Whistleblower Protection Act of 1989,[55] and the Intelligence Community Whistleblower Protection Act of 1998,[56] none of these statutes provided a general, all-purpose whistleblowing program for the IC. And while sometimes groundbreaking, the protections afforded the Intelligence Community prior to October 2012 were often not exercised, or exercised in the truest paladin tradition, that is, when enforcement was in the interest of those entrusted with ordering the local game space within the agencies rather than in the interest of balancing transparency and opacity, prudence and candor. Employees generally depend largely on statutes for protection from reprisal, but Congress chose not to enact separate and effective rules for intelligence agencies.[57]

---

[52] Civil Service Reform Act of 1978, Pub. L. No. 95-454, ch. 71, 92 Stat. 1111 (1978) (codified at 5 U.S.C. §§ 7101–7106, 7111–7123, 7131–7135).

[53] Inspector General Act of 1978, Pub. L. No. 95−452, 92 Stat. 1101 (1978) (codified at 5 U.S.C. App. 3).

[54] Whistleblower Protection Act of 1989, Pub. L. No. 101-12, 103 Stat. 16 (1989) (codified as amended at 5 U.S.C. § 2301 et seq.). *See* 5 U.S.C. § 2302, in particular, and Title 5's associated whistleblowing case law, which are used to the furthest extent possible to conduct reviews pursuant to PPD-19 and ICD-120.

[55] Military Whistleblower Protection Act of 1988, 10 U.S.C. § 1034 (2012).

[56] Intelligence Community Whistleblower Protection Act of 1998, Pub. L. No. 105-272, tit. 7, 112 Stat. 2413 (1998) (codified at 5 U.S.C. App. 3 § 8H). But note, "[d]espite its title, the ICWPA does not provide statutory protection from reprisal for whistleblowing for employees of the intelligence community." *National Security Whistleblowers in the post–September 11th Era: Lost in a Labyrinth and Facing Subtle Retaliation: Hearing Before the H. Subcomm. on National Security, Emerging Threats, and International Relations of the H. Comm. on Gov't. Reform*, 109th Cong. 391–92 (2006) (statement of Thomas F. Gimble, Acting Inspector General, Office of the Inspector General, U.S. Dep't. of Def.), *available at* http://www.fas.org/irp/congress/2006_hr/021406gimble.pdf. It was the failure of this statute (or misnomer) that created the general mischief that required the signing of PPD-19 and ICD 120.

[57] Denied substantive statutory protection, intelligence community employees have nonetheless had access to a series of internal regulations, which at least on their face provide some degree of protection. Since 2005, the Office of the Inspector General, U.S. Department of Defense has used IG Act sections 7(a) and (c), as well as 8(h), to provide discretionary civilian whistleblower protection by internal policy memorandum. Indeed, an often overlooked provision is the whistleblower protection available through the DoD's intelligence oversight process and its Procedures 14 and 15, which have been in effect since 1982 and would have provided, in part, a

A. Statutory and Regulatory Regime

The uneven nature of Federal whistleblower protections is not a mistake of Congressional decision making. The varying statutes have been adopted piecemeal in response to very real concerns about specific cases: cases in which the status of the employee or contractor has varied. The Whistleblower Protection Act (WPA) provides remedies for reprisal against civilian Federal employees paid with Congressionally appropriated funds, but it exempts employees of intelligence and counterintelligence agencies. These employees may make disclosures through the Intelligence Community Whistleblower Protection Act (ICWPA), which provides no direct protection from reprisal.[58] The ICWPA was designed to provide an avenue to transmit classified complaints to the appropriate Congressional oversight committee, thereby protecting the classified information from unauthorized disclosure. In fact, the ICWPA even has a provision allowing CIA employees to report complaints of an "urgent concern" to the CIA inspector general in accordance with the Inspector General Act of 1978, as amended, 5 U.S.C.A. App. 3 Section 8H(C) or the CIA Act, as amended, 50 U.S.C.A. § 3517 (d)(5).

CIA employees and the employees of other Intelligence Community Elements may also report an "urgent concern" to the IC IG under its Title 50 statutory procedures, which are akin to the ICWPA, 50 U.S.C.A § 3303

---

process for Edward Snowden had he contacted the assistant to the secretary of defense for intelligence oversight (ATSD I/O) with his NSA surveillance concerns. *See* UNDER SEC'Y OF DEF. FOR POLICY, DOD 5240.1-R, DEPARTMENT OF DEFENSE PROCEDURES GOVERNING THE ACTIVITIES OF DOD INTELLIGENCE COMPONENTS THAT AFFECT UNITED STATES PERSONS ¶ C14.2.3.2 (1982) ("Ensure that no adverse action is taken against any employee because the employ reports activities pursuant to Procedure 15") [hereinafter DoD 5240.1-R]. Signed seven years before the Whistleblower Protection Act of 1989, this is one of the older regulations providing federal employee and contractor protection. *Existence* of the protection has never been in question. *Effectiveness* obviously needs to be assessed via duly authorized oversight procedures. Nonetheless rules have been on the books since at least the Reagan administration. Internal systems gained heighten priority after the U.S. Supreme Court's decision in *Garcetti v. Ceballos*, 547 U.S. 410 (2006), in which the Court moved away from the "*Pickering* balance" when assessing the First Amendment rights of public employees.

[58] But the Inspector General Act of 1978, Pub. L. No. 95−452, 92 Stat. 1101, and the National Security Act of 1947, Pub. L. No. 80-253, 61 Stat. 495 (1947) *do* provide reprisal protections for those filing through the ICWPA or its Title 50 equivalent, when that disclosure is through a presidentially appointed, Senate-confirmed (PASC) statutory inspector general.

(k)(5). This provides CIA employees with an option to report "urgent concerns" to another IG with authority to receive the complaint—an IG more removed from management influence due to the IC IG's direct report status to the Director of National Intelligence—rather than the Director, Central Intelligence Agency. Whether the complaint of "urgent concern" is received by the CIA IG or the IC IG, the CIA employee must follow the statutory procedures in order to make a lawful disclosure to the Congressional oversight committees.[59] The ICWPA was designed to provide an avenue to transmit classified complaints to the appropriate Congressional oversight committee, thereby protecting the classified information from unauthorized disclosure.

As the ICWPA is not an IC whistleblower protection act, the Intelligence community relies primarily on internal mechanisms―namely PPD-19, ICD 120, the External Review Panel (ERP),[60] and the local agency implementing regulations―to protect its employees serving as sources. The failure of Washington professionals, in general, to understand the external context impacting the ICWPA led to a decade's delay in providing general whistleblower protection in the Intelligence Community.[61] Making a disclosure is the first step in gaining protection. Individuals within the Intelligence Community, whether they are government employees or contractors, can make reports of fraud, waste, abuse, and violations of law through their management chains, all the way up to the head of an IC element, to their respective IG, and to the IC IG.

These disclosures may be internal or external. As disclosures must be lawful, external disclosures need to be to a lawful receiver of the disclo-

---

[59] Making an unlawful disclosure places one in a state of outlawry, beyond the protection of the laws and regulations protecting whistleblowers. This would be "beyond the Pale" or march. For a recent citation of de Bracton's *gubernaculum* and jurisdiction discussed *infra* note 31, see Larry Catá Backer, *Transnational Corporations' Outward Expression of Inward Self-Constitution: The Enforcement of Human Rights by Apple, Inc.,* 20 IND. J. GLOBAL LEGAL STUD. 805 (2013) (citing Larry Cata Backer, *Reifying Law-Government, Law and the Rule of Law in Governance Systems*, 26 PENN. ST. INT'L L. REV. 521, 522 (2008)). *Compare* Meyer & Volk, *supra* note 30, *with* Ruth Wedgewood, *The Uncertain Career of Executive Power*, 25 YALE J. INT'L L. 310, 313 n.16 (2000).

[60] INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY, IC IG EXTERNAL REVIEW PANEL PROCEDURES PURSUANT TO PRESIDENTIAL POLICY DIRECTIVE―19 (2013) [hereinafter IC IG EXTERNAL REVIEW PANEL].

[61] *See generally* WILLIAM D. POPKIN, MATERIALS ON LEGISLATION: POLITICAL LANGUAGE AND THE POLITICAL PROCESS 248–337 (5th ed. 2009) (discussing external context in the sense of statutory purpose and how it influences the meaning of a statute).

sure, such as Congress. If an IC employee wishes to report an "urgent concern" to Congress, he or she may do so through either the IC element's IG or through the IC IG under the ICWPA and related statutes, as mentioned above. These reports to the IG are also "protected disclosures," which means that employees and contractors are protected from reprisal actions for making such disclosures. Moreover, the IGs have a responsibility to report directly to Congress any instances of management officials refusing to cooperate with an IG review of such a matter that has been reported to the IGs. These provisions ensure that IC employees and contractors have a protected avenue to make reports of alleged wrongdoing to Congress without compromising sensitive and classified information or fearing retaliatory actions.[62]

1. *WPA and the Intelligence Exception*

The Whistleblower Protection Act, codified in part at 5 U.S.C. §§ 1211-22, generally protects non–Intelligence Community appropriated, Federal civilian employees who make disclosures and then face retaliatory actions by their superiors. Employees must make a protected disclosure under 5 U.S.C. § 2302(b)(8) in order to receive protection. Under this provision, otherwise-authorized managers may not "take or fail to take, or threaten to take or fail to take" personnel actions against employees or applicants because of any covered disclosure.[63] Covered disclosures include disclosing information that the individual "reasonably believes evidences [any] violation of any law, rule, or regulation, or gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety."[64]

In order for the disclosures to be covered under Title 5, they must relate information "not specifically prohibited by law and . . . not specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs," or else the individual must convey the information to the Special Counsel, the Inspector General, or a des-

---

[62] *See* Intelligence Community Whistleblower Protection Act of 1998 §§ 701–702, 5 U.S.C. App. 3 § 8H; 50 U.S.C. § 3517 (for CIA employees and contractors); 50 U.S.C. § 3033 (for the intelligence community at large). In addition to ICWPA and disclosures to statutory inspectors general, employees and contractors making disclosures of questionable activities under the intelligence oversight regulations (such as Department of Defense Procedures 14 & 15, which are contained in DOD 5240.1-R, *supra* note 57) also qualify as having made a "protected disclosure."

[63] 5 U.S.C. § 2302(b)(8).

[64] *Id.*

ignated employee.[65] As long as the disclosure falls outside this category of privileged information, it can be made to anyone, whereas formerly the employee had to convey the matter to someone outside her chain of command or the nature of the disclosure had to fall outside her work duties.[66] This restrictive requirement was removed by the Whistleblower Protection Enhancement Act of 2012.[67]

Title 5 does not protect Intelligence Community whistleblowers. But the regulatory protections provided to Intelligence Community employees incorporate Title 5 standards by reference.[68] Accordingly, Intelligence Community whistleblower protection is not pursuant to Title 5, but rather mirrors Title 5 to the furthest extent possible. In general under Title 5, if a supervisor takes a prohibited personnel action against an employee for the latter's perceived protected disclosure, the whistleblower can seek corrective action. The Office of Special Counsel (OSC) can investigate and the Merit Systems Protection Board (MSPB) can order corrective action,[69] which must include attorney's fees and may include "back pay and related benefits, medical costs incurred, travel expenses, and any other reasonable and foreseeable consequential changes."[70] The MSPB can also order a stay of any pending personnel action,[71] or can enforce disciplinary action against the retaliating supervisor.[72] The Court of Appeals for the Federal Circuit can review MSPB decisions.[73] PPD-19 and ICD 120 provide institutions parallel to the OSC and MSPB to review IC whistleblowing complaints.

PPD-19 and ICD 120 do not rely on the OSC and the MSPB to provide the above functions, but rather use the system of inspectors general to provide a functional equivalent. So it is important to remember that the general Federal whistleblower protections statutes do not aid the Intelligence Community employees of specified federal agencies conducting foreign intelligence/counterintelligence operations, because those agencies are exempted from statutory Title 5 protection. The WPA, for instance, does not apply to

---

[65] *Id.*
[66] *See* Huffman v. Office of Pers. Mgmt., 263 F.3d 1341 (Fed. Cir. 2001).
[67] Whistleblower Protection Enhancement Act of 2012, Pub. L. No. 112–199, § 101(b)(2)(C), 126 Stat. 1465, 1466 (2012).
[68] *See* PPD-19, *supra* note 19, at 2.
[69] 5 U.S.C.§§ 1214, 1221(a).
[70] *Id*. at § 1221(g).
[71] *Id*. at § 1221(c).
[72] *Id.* at § 1215(b).
[73] *Id.* at § 7703.

> the Federal Bureau of Investigation, the Central Intelligence Agency, the Defense Intelligence Agency, the National Imagery and Mapping Agency, the National Geospatial-Intelligence Agency, the National Security Agency, and, as determined by the President, any Executive agency or unit thereof the principal function of which is the conduct of foreign intelligence or counterintelligence activities.[74]

2. *Executive Branch Regulations*

Civilian employees of agencies exempted from Title 5 do not receive the WPA protections afforded other civilian whistleblowers, but they may use the ICWPA, its Title 50 equivalent,[75] the Inspector General Act, and departmental directives maintained to implement PPD-19 and ICD 120. The ICWPA and its Title 50 equivalent require employees within the intelligence community to follow a particular process for disclosure that is more constrained than disclosures under the WPA. Neither the ICWPA nor its Title 50 equivalent provides direct protection from reprisal. The Intelligence Community instead relies on internal mechanisms to protect its employees and leaves this area of Executive branch decision making marked by high administrative discretion. The Inspector General Act permits IGs to investigate alleged whistleblower retaliation and make findings. But to gain corrective action—as remedy for the whistleblower and discipline against the reprisor—IGs must forward findings to officials who may act, and oversight authorities must follow up on the referral to ensure action is taken.

Before the signing of PPD-19 and ICD 120, the Inspector General Act of 1978, the Central Intelligence Act of 1952, and the National Security Act of 1946, all as amended, provided some whistleblower protection to the Intelligence Community. According to the Inspector General Act and similar provisions in the other statutes, a manager may not take action "against any employee as a reprisal for making a complaint or disclosing information to the IG."[76] The Inspector General Act further states:

> [The IG] may receive and investigate complaints or information from an employee of the establishment concerning the possible existence of an activity constituting a *violation of law, rules, or regu-*

---

[74] *Id.* at § 2302(a)(2)(B)(ii).
[75] 50 U.S.C. § 3033(k)(5)(A).
[76] 5 U.S.C. App. 3 § 7(c).

> *lations*, or mismanagement, gross waste of funds, *abuse of authority* or a substantial and specific danger to the public health and safety.[77]

Given that a manager cannot retaliate against an employee for disclosing information to the IG, the IG can investigate a complaint that alleges reprisal because it violates that law and the manager has abused his or her authority. Despite this broad authority to investigate whistleblower reprisals, it provides no mechanism for enforcing protection of the whistleblowers or providing them a corrective remedy, much like the ICWPA. Effectiveness, therefore, is left to the process of IG report oversight by department heads or Congressional committees of jurisdiction.[78]

Prior to PPD 19, IGs had discretionary authority to investigate reprisals. Statutorily confirmed IGs are authorized "to make such investigations and reports relating to the administration of the programs and operations of the applicable establishment as are, in the judgment of the Inspector General, necessary or desirable."[79] But if the IG finds that an investigation is not "necessary or desirable," the ignored non-IC complainant was, and still is, left without recourse under this provision. The DoDIG established the Directorate, Civilian Reprisal Investigations in 2004 to give priority to "[c]ases originating in the intelligence community."[80] But CRI ceased operations in the spring of 2011. And despite this priority, even CRI could decline to investigate a case in the Intelligence Community. Other Executive branch departments with fewer Intelligence Community personnel did not contain a directorate devoted specifically to investigating intelligence community reprisals.

In deciding whether to investigate, an IG may be mindful of her relationship with the Executive branch department she oversees, the relation-

---

[77] *Id.* at § 7(a) (emphasis added).

[78] Assessing effectiveness requires some thought with respect to the metrics developed for a whistleblowing program. *See* A. J. Brown, D. Meyer, C. Wheeler & Jason Zuckerman. *Whistleblower Support in Practice: Towards an Integrated Research Model*, *in* INTERNATIONAL WHISTLEBLOWING RESEARCH HANDBOOK (A.J. Brown. David Lewis, Richard Moberly & Wim Vandekerckhove, eds, 2014). *See also* Maj. Jonathan B. Bell, Intelligence Community Whistleblowers and Opportunities for Reform: Why and How to Better Protect Secrets and Preserve Civil Liberties (June 16, 2014) (unpublished M.A. thesis, National Intelligence University) (on file with the author).

[79] 5 U.S.C. App. 3 § 6(a)(2).

[80] Memorandum for Civilian and Military Officers and Employees Assigned to the Office of the Inspector General of the Department of Defense (Jan. 7, 2005) (on file with author).

ship with the President who nominated her, or indeed, the Senate who confirmed her. Under the IG Act and its Intelligence Community equivalents, a statutory Office of the Inspector General is independent of "management," that is, of Executive branch department leadership within the department the IG serves. IGs are not, as zealous members of senior leadership sometimes mistakenly believe, "independent" of all management, including the Congress. All three institutions weigh heavily on an IG and her staff when vexing cases are under review for intake. The President appoints the IG, but the office is created within the Executive branch department overseen by the IG.[81] The IG must report to the head of the department and is subject to general supervision, although the department head generally cannot prevent or prohibit an IG investigation.[82] The IG maintains a relationship with its corresponding department, which may indirectly exert an influence on investigations, but the IG ultimately has freedom to investigate what she chooses when there is a very specific tasking from Congress, usually in legislation.

The IG's authority to investigate adheres only to the statutorily created IG. It does not extend to discretionary IGs created by individual department heads such as the Secretary of the Army. The Inspector General Act establishes an IG for each major non-Intelligence Community department in the Executive branch, including one each for the DoD and DOJ. In 2010, reforms to Title 50 created the first overarching Inspector General for the Intelligence Community, who answers to the United States Director of National Intelligence and Congressional committees of jurisdiction.

3. *Security Clearances*

Managers could formerly evade many whistleblower protection laws by denying or revoking security clearances. Employees still cannot appeal the merits of security clearance decisions to the MSPB or other courts.[83] Courts can only review procedural protections of a security clear-

---

[81] 5 U.S.C. App. 3 §§ 2-3.

[82] *See id.* at § 3. Heads of department do have what is called "Section 8" authority to bar an inspector general from acting on a particular matter. This is used sparingly and, in some agencies, not at all. *See* 5 U.S.C. App. § 8(b)(2). Given that these provisions typically require reporting to Congressional oversight authorities, use of Section 8 can raise a red flag to the Hill that a department head may require additional oversight.

[83] *See* Dep't of the Navy v. Egan, 484 U.S. 518 (1988); *see also* Hesse v. Dep't of State, 217 F.3d 1372, 1377 (Fed. Cir. 2000) (applying the *Egan* principle to a civilian whistleblower reprisal case).

ance decision,[84] but may not consider the substantive basis for the decision. To provide for substantive review, for instance, the DoDIG took positive steps to investigate security clearance decisions as early as 2004; but like all IG investigations, they are internal to the department and rely on oversight processes at the department or Congressional level for enforcement.[85]

Given the central nature of security clearances for Intelligence Community employment, supervisors and managers could formerly terminate employees indirectly through security actions. This unchecked tool for Executive branch officials was an easy way to retaliate against employees, as one source described:

> Taking away an employee's security clearance has become the weapon of choice for wrongdoers who retaliate. When a security clearance is revoked, the employee is effectively fired, since they are unable to do their job or pursue other job opportunities in their area of expertise. Currently, the employee is unable to appeal to an independent body to challenge the retaliation and internal hearings are Kafkaesque. Among the practices we have been made aware of in recent years: whistleblowers are not told the charges against them, they are not allowed to dispute those charges, or they are prevented from presenting their case before internal panels which decide.[86]

V. FROM WASTE TO PALATINE: GRANTING PROTECTION TO INTELLIGENCE AGENCY WHISTLEBLOWERS

As the Whistleblower Protection Enforcement Act was debated during the 111th and 112th Congresses, there was a perception in some quarters that the Intelligence Community lacked informed oversight because community employees were unwilling to disclose corruption. The then statutory and regulatory schema provided piecemeal protection for employees who faced retaliation for making disclosures. Few employees could understand,

---

[84] *See, e.g.,* Cheney v. DOJ, 479 F.3d 1343, 1352 (Fed. Cir. 2007) (holding that procedural requirements were not met because plaintiff was not given sufficient reasons for his suspension to be able to respond).

[85] PROJECT ON GOVERNMENT OVERSIGHT, *supra* note 45 at 11.

[86] *National Security Whistleblowers in the post–September 11th Era: Lost in a Labyrinth and Facing Subtle Retaliation: Hearing Before the H. Subcomm. on National Security, Emerging Threats, and International Relations of the H. Comm. on Gov't. Reform*, 109th Cong. (2006) (statement of Beth Daley, Senior Investigator, Project on Gov't Oversight), *available at* http://www.fas.org/irp/congress/2006_hr/whistle.html.

for instance, that Procedures 14 and 15 provided a means for protection. Even when the pieces were put together, the network of diluted laws usually left an employee without effective protection, although the framework for protection existed. Courts would simply dismiss an employee's reprisal claim against an intelligence agency, and the IG could give the employee no remedy.

A. The Legislation History of the 110th Congress

In the 110th Congress, each house of Congress passed a bill to reform whistleblower protection law.[87] Both bills allowed Article III courts to review security clearance decisions, permitted employees to disclose sensitive information to Congress, forbade the President from retroactively exempting an agency from the WPA, and limited the reach of secrecy agreements. The first run of what would become the Whistleblower Protection Enhancement Act (WPEA),[88] passed in the House of Representatives, outlined a procedure for employees to seek a remedy for whistleblower reprisal complaints and included access to the courts, should the IG not act. The Federal Employee Protection of Disclosures Act (FEPDA),[89] passed in the Senate, lacked the comprehensive review mechanism, but required agencies to inform employees of how to make proper disclosures.

1. *Shared Provisions of the WPEA and FEPDA*

Under either bill, employees in the Intelligence Community would have gained protection from abusive, security-action decisions taken in retaliation for making disclosures, thereby closing one of the most problematic statutory lacuna in the rubric's schema. The bills accomplished this by explicitly including security clearance decisions in the description of prohibited reprisals.[90] The FEPDA also checked judicial review of security clearances by barring the courts from reversing the government's security clearance determinations. But it permitted other corrective action to compensate.[91] Otherwise, under this new construction, Article III courts would have been able to review security clearance determinations the same way that they currently address direct terminations and other personnel actions.

---

[87] A bill was passed and signed by the president in the 112th Congress, namely the Whistleblower Protection Enhancement Act of 2012. *See* Etzioni, *supra* note 9, at 1179–1180.

[88] Whistleblower Protection Enhancement Act of 2007, H.R. 985, 110th Cong. (2007).

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

[90] H.R. 985 § 10(a); S. 274 § 1(e)(1).

[91] S. 274, § 1(e)(3).

Further, in the 110th Congress, employees would have gained the right to lawfully and directly disclose sensitive information outside of the agency. Employees would have been able to disclose not only to their respective IGs and authorized Executive officials, but also to authorized members of Congress.[92] Under the bills, authorized members of Congress in most instances consisted of members of the intelligence committees.[93] Under the 110th Congress's WPEA, an employee could disclose information that she reasonably believes evidences a "violation of any law, rule, or regulation; or gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety."[94] In the case of the FEPDA, the employee's evidence had to be more specific, but it could also fall into an additional category of "a false statement to Congress on an issue of material fact."[95] These provisions would allow for direct disclosures to Congress and match closely to the types of disclosures covered by the WPA.

The bills also would have clarified how the President determines agencies of the Intelligence Community for purposes of exemption from the WPA. Following MSPB litigation earlier in the decade, bureaucratic efforts to clarify this process had languished. The President or his delegate can determine, after a reprisal has occurred, that an agency's primary function is conducting intelligence activities, and that the agency may be exempt for that reprisal. This retroactive determination exempts the agency from the regular federal whistleblower protection provided by the WPA, even though the employee could not know that the agency was exempt when she made the disclosure. This became even more problematic after 9/11, when "intelligence activities" were being placed in agencies that historically had a limited relationship to the Intelligence Community. Under the proposed laws, the President would have had to make this determination before the alleged reprisal occurred.[96]

Courts have upheld secrecy or nondisclosure agreements between agencies and federal employees, but the proposed 110th Congress's reforms limited these agreements where they conflicted with the right to make responsible disclosures. The new laws would have banned agencies from creating total nondisclosure agreements, required that such agreements contain

---

[92] H.R. 985 § 10(a); S. 274 §1(b)(3).
[93] H.R. 985 § 10(a); S. 274 §1(b)(3).
[94] H.R. 985 § 10(a).
[95] S. 274 §1(b)(3).
[96] H.R. 985 § 6; S. 274, § 1(f).

provisions allowing for responsible disclosures, and construed agreements to allow for responsible disclosures even if absent from the written agreement.[97] Responsible disclosures were those that were permitted by the whistleblower statutes, and nondisclosure agreements would not infringe upon the rights provided in those statutes. In short, this legislative proposal provided protection of the whistleblower's right to disclose: a right that was curtailed when Article III courts read the enforcing secrecy agreements as absolute.[98]

2. *WPEA: Granting Corrective Action and Court Access*

The 110th Congress's WPEA offered to protect employees in the Intelligence Community by setting up a process to review reprisals against them.[99] The legislative proposal returned, in a variety of forms, in the 111th and 112th Congresses. The 111th Congress's Whistleblower Protection Enhancement Act of 2009, S. 372, was again authored by Senator Daniel K. Akaka (D-HI), passed by unanimous Senate consent on December 10, 2010 and unanimous House consent on December 22, 2010, but was not enacted before the end of the 111th Congress's second session. As the vote was without objection, no record exists of individual votes. As S.743, this legislation was reintroduced in the 112th Congress and eventually signed on November 27, 2012—exempting the Intelligence Community—as the Whistleblower Protection Enhancement Act of 2012.[100] The regulatory combination of PPD-19 and ICD 120 has now replaced those legislative initiatives with an Executive branch-–centric solution. But it is useful to recall—should PPD-19 and ICD 120 ultimately fail to deliver a system of Intelligence community whistleblowing—the state of Congressional reform during the sessions prior to President Obama's signing of PPD-19.

Under the now-abandoned legislation, once an Intelligence Community employee made a complaint of reprisal to an IG, that office was required to review the complaint and the agency head was required to make a determination.[101] Once a substantiated finding was made, the head of the agency was required to grant corrective action or issue an order denying relief to the employee.[102] If the head of the agency did not make a determination within 180 days, or else deny relief, the employee could have the

---

[97] H.R. 985 § 5; S. 274 §§ 1(k)(1), 1(e)(2)(C).
[98] *See* United States v. Marchetti, 466 F.2d 1309 (4th Cir. 1972).
[99] H.R. 985 § 10(a).
[100] Whistleblower Protection Enhancement Act of 2012, Pub. L. No. 112-199, 126 Stat. 1465 (2012).
[101] H.R. 985 § 10(a).
[102] *Id.*

complaint reviewed by an Article III court.[103] There the agency would have to openly defend its managers, unless successful in claiming the state secrets privilege.[104] If the agency invoked the state secrets privilege, however, two major consequences ensued under the reform legislation. First, the agency was required to issue a report to Congress.[105] Second, if the IG found "substantial confirmation," the court would rule in favor of the employee, although the bill did not define "substantial confirmation."[106] These procedures still started with internal investigations.

3. *Opposition to the Legislation*

In the 110th Congress, each bill passed overwhelmingly in respective chambers.[107] Congress was then required to write a compromise bill to pass through both houses[108] that would have required a careful balancing of interests to retain their strongest measures without losing votes. Despite strong bipartisan support for the legislation, Congress was acting under a veto threat from the Bush administration directed at both the WPEA and the FEPDA, stating "[i]f H.R. 985 were presented to the President, his senior advisors would recommend that he veto the bill."[109] This was an offshoot of the gridlock facing WPA reform after the *Huffman*[110] case in 2001. For what would become a decade-plus impasse, attempts to reform the WPA would

---

[103] *Id.*
[104] *Id.*
[105] *Id.*
[106] *Id.*
[107] Government Accountability Project, *Senate Approves Whistleblower Protection Legislation (*Dec. 18, 2007), *available at* http://yubanet.com/usa/Senate_Approves_Whistleblower_Protection_Legislati_73072_printer.php [hereinafter Government Accountability Project].
[108] *See id.*
[109] OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, STATEMENT OF ADMINISTRATIVE POLICY, H.R. 985—WHISTLEBLOWER PROTECTION ENHANCEMENT ACT OF 2007 (2007), *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/sap/110-1/hr985sap-h.pdf [hereinafter Statement of Administrative Policy]; *see also* Letter from Michael B. Mukasey, Attorney General, to Nancy Pelosi, Speaker, House of Representatives (Dec. 17, 2007), *available at* http://www.justice.gov/archive/ola/views-letters/110-1/12-17-mukasey-re-s274-fed-employee-act.pdf [hereinafter Mukasey].
[110] Huffman v. Office of Pers. Mgmt., 263 F.3d 1341 (Fed. Cir. 2001), *superseded by statute,* Whistleblower Protection Enhancement Act of 2012, Pub. L. No. 112–199, § 101(b)(2)(C), 126 Stat. 1465, 1466 (2012) (now desuetude following enactment of the WPEA). *See also* SISSELA BOK, SECRETS: ON THE ETHICS OF CONCEALMENT AND REVELATION (1983).

begin in each successive Congress and then fail in the waning weeks of each Congress.

The Executive branch has asserted that permitting employees to make sensitive disclosures directly to Congress creates a grave and unconstitutional[111] risk to national security. According to Attorney General Mukasey, only an official acting on the authority of the President should determine when to disclose classified information.[112] Intelligence employees surreptitiously deciding when to disclose Executive branch arcana violates this principle. This issue is not about individual employee preference, but rather one triggering separation of powers concerns between Executive control over *arcana imperii* and Legislative prerogative in gaining information as the agent of the Sovereign under the U.S. Constitution.[113] Limiting the scope of secrecy agreements poses the same problems by permitting disclosure of classified information.[114]

In a similar manner, the Executive branch posited that the President must control security clearance determinations as an exercise of his discretion in protecting national security. By reviewing security clearances and providing relief to plaintiffs based on them through the WPEA reform legislation, the courts would therefore encroach on the President's power to protect certain information.[115] These judicial reviews could thereby unconstitutionally[116] undermine the President's authority over security clearances.

Finally, the Executive branch opposed WPEA provisions giving intelligence employees access to the court system. These employees could then get two rulings on the same claim because judges can hear claims already denied by the IG. Also, by finding in an employee's favor when the government invokes the state secrets privilege, judges would "require the agency to choose between protecting national security information in court

---

[111] Attorney General Mukasey relies heavily on *Egan* in declaring both disclosures to Congress and judicial review of security clearances unconstitutional. *See* Mukasey, *supra* note 109. *Egan* itself states the proposition, however, that courts are reluctant to intrude upon the authority of the Executive in national security affairs "[u]nless Congress has specifically provided otherwise," which Congress has done in the WPEA and FEPDA. Egan, 484 U.S. at 530. It should also be noted that *Egan* is limited to the restriction on Article III courts; it does not restrict inspectors general, whose offices are part of the executive branch.

[112] Mukasey, *supra* note 109.

[113] *See id.*

[114] *See id.*

[115] *See id.*

[116] *See* H.R. 985, *supra* note 88.

or conceding lawsuits."[117] The Executive branch found this choice unacceptable and so opposed the WPEA provision permitting courts to take this action in some circumstances.[118] These Executive branch concerns were part of the friction impeding legislative reform between 2001 and 2011, especially after 9/11.

Faced with this check, Congress had three choices. First, the 110th, 111th, and 112th Congresses could have rounded the new act's language until the black letter was acceptable to the Executive branch. But given the number of reform provisions generating concerns among *both* Bush and Obama national security elites, accommodation may well have undone the reform consensus within the Legislative branch. Second, Congress could have waited for a new administration and hoped it would take a different stance on these issues. This is always a tough choice, as the former breadth of national security policy divergence between Democratic and Republican circles has narrowed significantly since 9/11. The final approach—passing a veto-proof bill—raised the legislative bar exceedingly high. It also required deft maneuvering to avoid the hold senators may place on bills. If the Senate and House of Representatives could have agreed to a strong compromise bill without upsetting the reformists, such approach would have been feasible. The House of Representatives did in fact pass the WPEA with a veto-proof majority, and the Senate passed the FEPDA by unanimous consent.[119] But those were not the final conferenced and reconciled bills.

In summary, the Whistleblower Protection Enhancement Act in the 110th and 111th Congresses would have provided whistleblower protection to Intelligence Community employees and contractors. As early as 2007, provisions were included to cover the revocation and suspension of security clearances when done in retaliation. The Executive branch opposed the legislation on the grounds that employees disclosing classified information to Congress without authorization jeopardize national security and impede the President's coordination function. Also of concern was the perceived threat the legislation posed to the assertion of the state secrets privilege at trial as well as the integrity of the security clearance decision-making process as an Executive branch function.[120]

---

[117] Statement of Administrative Policy, *supra* note 109.
[118] *See id.*
[119] *See* Government Accountability Project, *supra* note 107.
[120] *See*, *e.g.*, Papandrea, *supra* note 11, at 494–496 (citing OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, STATEMENT OF ADMINISTRATIVE POLICY, H.R. 985—WHISTLEBLOWER PROTECTION ENHANCEMENT ACT OF 2007 (2007)).

4. *Resulting Protections for IC Whistleblowers*

The 110th, 111th and 112th Congresses did not pass whistleblower reform legislation to protect sources within the Intelligence Community.[121] Mid-passage during the 111th Congress, the reformists came close to passing a reconciled bill until a hold was placed on the Senate bill. In the spring of 2011, work began on an executive branch solution to the impasse, which through several drafts became PPD-19, after it was signed on October 20, 2012. This occurred just before Congress passed a WPEA without the bill's Title 2, the Intelligence Community whistleblower reform legislation.

PPD-19's provisions can be summarized as follows. Once a protected disclosure is made under PPD-19,[122] the presidential directive provides an avenue to protect the whistleblower making the disclosure. PPD-19 requires each IC agency to establish:

> (1) policies and procedures prohibiting retaliation against employees who make protected disclosures,
>
> —and—
>
> (2) policies and procedures for these claims to be reviewed by the agency's IG, who will make a recommendation to the agency head on appropriate relief if retaliation is proven.

---

[121] Once a sovereign concedes being "of two minds" and unable to act, the resulting march creates a system of privileges and immunities that must be tightly regulated to preserve sovereignty at the hearth. *See* Thomas H. Burrell, *A Story of Privileges and Immunities: From Medieval Concept to the Colonies and United States Constitution*, 34 CAMPBELL L. REV. 7, 59 n.292 (2011) (citing NICHOLAS P. CANNY, THE ELIZABETHAN CONQUEST OF IRELAND: A PATTERN ESTABLISHED 1565–1576 49–52 (1976)). It is worth comparing this piece with Michael J. Glennon, *National Security and Double Government*, 5 HARV. NAT'L SEC. J. 1 (2014). In the European colonial expansion, the English common law was combined with royal prerogative—*jurisdictio* and *gubernaculum* coincident—in an act of violence against societies opposing the expansion. *See, e.g.*, Ezekiel Rediker, *Courts of Appeal and Colonialism in the British Caribbean: A Case for the Caribbean Court of Justice*, 35 MICH. J. INTL'L 213 (2013). To be sure, the violence is not necessarily irreversible. *See* Hefin Rees, *Awakening the Welsh Dragon: Will the Creation of the National Assembly for Wales Make a Significant Difference to the Constitutional Arrangements between England and Wales*, 23 SUFFOLK TRANSNAT'L L. REV. 459 (2000).

[122] PPD-19 generally does not apply to the FBI, which follows a different statutory regime. *See* PPD-19, *supra* note 19.

To the fullest extent possible, PPD-19 requires these IC agency policies and procedures to mirror those of the Whistleblower Protection Act (5 U.S.C. § 2302(b)(8)). The requirements of PPD-19 are currently being implemented. The latest milestone was the Director of National Intelligence's issuance of ICD 120 on March 20, 2014. Eighteen months after the President's signing of PPD-19, the 113th Congress began the process of codifying PPD-19. In doing so, Congress narrowed the scope of PPD-19 by setting, via statute, the evidentiary standard for assessing a reprisor's actions at the lower "preponderance" level. PPD-19 itself provided for Title 5 standards to "the furthest extent possible," permitting the use of the higher "clear and convincing" standard.[123]

If an employee has exhausted his or her remedies under the PPD-19 agency process, he or she may seek review by the External Review Panel, a body of three inspectors general chaired by the IC IG. The IC IG may make a recommendation to the agency head for appropriate action or may exercise *de novo* investigative jurisdiction over the matter appealed.[124]

Structurally, PPD-19 is divided into two core functional parts: Section A (providing whistleblower protection for IC members) and Section B (providing whistleblower protection for all Federal security clearance applicants and holders). The standards for assessing reprisal under Section A are provided by the President's citation to Title 5 of the United States Code. In contrast, Section B cites simply to Executive Order 12968, Access to Classified Information (Aug. 4, 1995), which does not have a whistleblower protection clause providing standards. PPD-19 Section B simply does not have a standard by which an investigator can conduct an investigation. Accordingly, the IC IG applies by extension the Title 5 standards, including associated case law, cited in PPD-19 Section A. All PPD-19 investigations pursuant to Sections A and B are thereby held to similar standards.[125] The general standards cited in Section B are outlined at Executive Order 12968 and require eligibility and access to classified information to be "clearly consistent

---

[123] Intelligence Authorization Act of 2014, Pub. L. No. 113-126, § 602(b), 128 Stat. 1390, 1416 (2014) (codified at 50 U.S.C. § 3341).

[124] *See* PPD-19, *supra* note 19, at pt. C.

[125] *See* UNDER SEC'Y OF DEF., U.S. DEP'T OF DEF., DTM 13-008, DOD IMPLEMENTATION OF PRESIDENTIAL POLICY DIRECTIVE 19 (2013). There is one statutorily-determined difference between the two PPD-19 sections, A and B. Through the Intelligence Authorization Act of 2014, Congress set the standard of proof in Section B investigation as by a preponderance of the evidence. Intelligence Authorization Act of 2014 § 602(b).

with the interests of national security."[126] Whistleblowing pursuant to PPD-19 is a component of the national security interest.

PPD-19 also prohibits agencies from taking an action to revoke or deny an employee's eligibility for access to classified information (i.e., the employee's security clearance) in retaliation for making a protected disclosure. The relevant executive orders implementing the eligibility system (E.O. 12968 for government employees) already include due process procedures for suspension and revocation of access to classified information. In addition to these due process procedures, PPD-19 requires all agencies to develop a review process that allows employees to appeal an action affecting eligibility for access to classified information if they allege that such action was made in retaliation for making a protected disclosure. As part of this additional review process, PPD-19 also requires a review by the agency's inspector general to determine whether PPD-19 has been violated and if so, to make recommendations for the agency to reconsider the employee's access to classified information. Employees who claim retaliations affecting security clearances may also take advantage of the external IG panel review discussed above.[127]

Contractors are not covered by the Whistleblower Protection Act of 1989, as amended, or Part A of PPD-19. However, the Intelligence Community Whistleblower Protection Act (ICWPA) of 1998 applies to IC contractors, providing them with a protected avenue for making reports of urgent concern to Congressional committees without compromising sensitive and classified information.[128] The ICWPA does not, however, provide pro-

---

[126] *See* Exec. Order No. 12,968, 60 Fed. Reg. 40,245 (Aug. 2, 1995) pt. 3.1.(b)–(d). For example, reporting of corruption within the federal government is required by Exec. Order No. 12,674, 54 Fed. Reg. 15,159 (Apr. 12, 1989). President Bush signed Executive Order 12674 on April 12, 1989 and Executive Order 12731 on October 17, 1990. Executive Order 12731 restated Executive Order 12674 and incorporated certain modifications. The new executive branch–wide standards of conduct regulation, the *Standards of Ethical Conduct for Employees of the Executive Branch*, became effective in 1993 and was codified in 5 C.F.R. pt. 2635. Where there are allegations that the national security interest has been compromised by reprisal against a source, Title 5 standards are applied to ascertain whether those reporting corruption are being reprised against for their reporting.

[127] *See* PPD-19, *supra* note 19, at pt. B.

[128] For the narrower category of disclosures that relate to intelligence oversight wrongdoing, a longer pedigree controls. With respect to employees and contractors concerned about the legality of the National Security Agency's warrantless electronic monitoring activities between 1982 and the present, the NSA IG would have been a good first point of disclosure. The NSA IG has well-developed hotline procedures and whistleblower protection directives. If a complainant found the NSA

tection for the discloser. Protection would have to be provided, if available under the circumstances, by another device such as the Inspector General Act of 1978, as amended.

Executive Order 10865, which establishes the Industrial Security Clearance Program, includes the due process requirements for the revocation of access to classified information for contractors, including providing the contractors with the right to a due process hearing. Part B of PPD-19 may also provide additional protections for contractors who claim retaliation. The Executive branch is evaluating the scope of that protection as they implement the requirements of PPD-19, which is currently in its implementation phase. Agencies are required to certify their compliance with the PPD

IG unresponsive, she or he could then contact the assistant to the secretary of defense for intelligence oversight (ATSD I/O). A complainant contacting the ATSD I/O, would then find that the ATSD I/O may inquire or investigate, but more often than not finds the level of oversight that can most efficiently investigate the allegations. This could very well be a local IG, such as NSA's, or an IG more remote from the allegations. So, if a complainant were to go to the ATSD I/O and allege reprisal that the ATSD I/O felt could not be investigated by the local IG, he or she could send the reprisal allegations to an IG not conflicted, such as the Defense Hotline. *See* OFFICE OF INSPECTOR GENERAL, DEP'T. OF DEF., http://www.dodig.mil/hotline/classifiedcomplaint.html. Once received as an intake, this higher-level review in lieu of a local review would first consult DoD 5240.1-R, *supra* note 57. These regulations contain a provision for disclosure called Procedure 15 which states that "[e]ach employee shall report any questionable activity to the General Counsel or Inspector General for the DoD intelligence component concerned, or to the General Counsel, DoD, or ATSD(IO)." DoD 5240.1-R, *supra* note 57, at ¶ C15.3.1.1. Once a disclosure is made under Procedure 15, the employee is protected. *Id* at ¶ C14.2.3.2. ("The Heads of DoD Components that constitute, or contain, DoD intelligence components shall . . . [e]nsure that no adverse action is taken against any employee because the employee reports activities pursuant to Procedure 15."). The last critical piece is whether "employee" for the purpose of DoD 5240.1-R includes contractors. This is the definitional question that has been heavily debated throughout much of 2013 and 2014, and the answer is in plain text, which defines employee as "[a] person employed by, assigned to, or acting for an agency within the intelligence community, including contractors and persons otherwise acting at the direction of such an agency." *Id* at ¶ DL1.1.10. Effective immediately, DoD 5240.1-R was signed by Attorney General William French Smith and Secretary of Defense Caspar Willard Weinberger on December 7, 1982, thereby giving intelligence community contractors whistleblower reprisal provisions available for their protection when disclosing on intelligence oversight matters such as alleged electronic surveillance on U.S. persons and other questionable activities. There is always a place for assessing *effectiveness*. But *existence* is not open to debate.

to the DNI, who will review the certifications and inform the President of compliance.

So the following statutory and policy provisions provide protections for IC whistleblowers: the Inspector General Act of 1978, as amended, allows Department of Defense intelligence component employees to report allegations of violation of laws, rules, or regulations, or mismanagement, gross waste of funds, abuse of authority, or a substantial and specific danger to the public health and safety to their respective IC element IG or the Department of Defense IG;[129] for employees of the Central Intelligence Agency, the CIA inspector general can accept disclosures, complaints, or information from any person concerning the existence of an activity within the CIA constituting a violation of laws, rules, or regulations, or mismanagement, gross waste of funds, abuse of authority, or a substantial and specific danger to the public health and safety;[130] and the National Security Act of 1947,[131] as amended, allows the IC IG to receive disclosures, complaints, or information from any person concerning the existence of an activity within the authorities and responsibilities of the Director of National Intelligence constituting a violation of laws, rules, or regulations, or mismanagement, gross waste of funds, abuse of authority, or a substantial and specific danger to the public health and safety. Further, this statute prohibits reprisal actions taken against employees making these kinds of disclosures to the IC IG, who may investigate any reprisal allegation in addition to the initial disclosure that the employee made.

The IC IG Forum members also may receive complaints from IC employees and contractors who wish to report "urgent concerns" to Congress. This allows whistleblowers an avenue to report classified complaints to the Congressional intelligence committees for action. And again, these disclosures are protected, and reprisal actions stemming from such disclosures are prohibited.[132] Though it should be noted, the Federal Acquisition

---

[129] *See* 5 U.S.C. App. 3 § 8G. This includes each inspector general for the Defense Intelligence Agency (DIA), the National Geospatial-Intelligence Agency (NGA), the National Reconnaissance Office (NRO), and the National Security Agency (NSA).

[130] *See* 50 U.S.C. § 3517 (e)(3).

[131] *See id.* at § 3033 (g)(3).

[132] *See* 5 U.S.C. § 8H, which is commonly referred to as the Intelligence Community Whistleblower Protection Act of 1998 (ICWPA) and covers DIA, NGA, NRO, and NSA employees and contractors. 50 U.S.C. § 3517(d)(5)(A), which is part of the Central Intelligence Agency Act of 1949, covers CIA employees and contractors. The IC IG statute, 50 U.S.C. § 3033, is mirrored after the ICWPA. The ICWPA, which does not provide intelligence community whistleblower protection,

Streamlining Act of 1994,[133] as implemented by the Federal Acquisition Regulations (FAR), formerly provided whistleblower protection to contractor employees for "all Government contracts."[134] That overarching protection has been curtailed and replaced by more narrowly focused systems of protection.

In general, IGs may receive reprisal complaints "relating to a substantial violation of law related to a contract (including the competition for or negotiation of a contract)." Note that the sole basis for protection is far more limited than the basis for reprisal protection under the National Security Act above, as this protective statute is available to IC contractors who disclose matters related and limited to only the contract under which they are working.[135] However, the IC IG may receive complaints from "any person," not just IC employees, regarding any violation of law, not just those violations relating to the contract. The IC IG statute prohibits reprisal actions against anyone making such disclosures to the IC IG, which allows for another more broadly scoped reprisal protection for IC contractors.[136] The Federal Acquisitions Regulation was amended in September 2013, stating that the regulation's whistleblower protections no longer implemented the FASA provisions in 10 USC § 2409 (affecting DoD, NASA, and the Coast Guard). These protections were to be implemented in the FAR supplements issued by those agencies (e.g., at DoD, the DFARS).[137]

---

would probably have been better entitled, "the protection of disclosures to Congress Act." For employees disclosing to the Congressional intelligence committees under these acts, protection is provided under the broader whistleblower protection provisions outlined in the respective IG acts stated above.

[133] Federal Acquisition Streamlining Act of 1994, Pub. L. No. 103-355, 108 Stat. 3243 (1994).

[134] Whistleblower Protections for Contractor Employees, 48 C.F.R. § 3.902 (1989). This section, previously entitled "Applicability," was removed in 2009.

[135] At present, there is a whistleblower protection pilot program as mandated by section 828, entitled "Pilot Program for Enhancement of Contractor Employee Whistleblower Protections." It was passed as part the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2013. *See* Pub. L. No. 112-239, § 828, 126 Stat. 1632, 1837 (2013) (Pub. L. 112-239, enacted January 2, 2013). Paragraph (a) of section 828 adds to title 41 a new section 4712 that contains the elements of the pilot program, which is in effect through January 1, 2017. *Id*. Under the pilot program, and under 10 U.S.C. § 2409, another whistleblower protection program, these protections exclude IC contractor employees.

[136] *See* 50 U.S.C. § 3033 (g)(3).

[137] 48 C.F.R. § 3.900 (2013) ("This subpart implements three different statutory whistleblower programs. This subpart does not implement 10 U.S.C. 2409, which is applicable only to DoD, NASA, and the Coast Guard.").

And finally, PPD-19 ensures that IC employees and individuals eligible for access to classified information can effectively report fraud, waste, and abuse while protecting classified information, without fear of retaliation for making such reports. This protection allows employees to make protected disclosures, regardless of category, to management officials, agency directors, and agency inspectors general. PPD-19 prohibits reprisal actions in the form of personnel actions (Section A) or security clearance decisions (Section B) against IC employees who make such disclosures, which in turn establishes an overarching system of IC whistleblower protection through an executive order. [138]

Further, PPD-19 requires an IG review of any reprisal allegation that violates PPD-19. Initial IG reviews are completed by agency IGs, who are also members of the IC IG Forum. If employees have exhausted their agency review process, including the IG review process, then they may appeal to the External Review Panel, led by the IC IG, for an appellate review. Hearing of an appeal or a *de novo* investigation in response to an appeal is discretionary on the part of the IC IG. For IC contractors, reprisal protections are granted under Section B of PPD-19 and only for the limited purposes of reviewing alleged reprisal through security clearance decision making. Prior to and in response to PPD-19, IC elements maintained local whistleblower protection regulations, which are now certified under the PPD-19 process. [139]

Accordingly, this patchwork of statutory and policy protections creates a system dependent on the skills, talents, and authority of the many inspectors general providing oversight to the Intelligence Community. These inspectors general may make findings and recommend corrective action. But they cannot order corrective action. In order for a wronged whistleblower to receive a remedy or for a wrongful responsible management offi-

---

[138] Since 1982, sources to defense intelligence community intelligence oversight (I/O) investigations and reviews have had protection under Procedures 14 & 15 of the regulations implementing the Foreign Intelligence Surveillance Act of 1978, as amended. The term "employees" under this act has been read to include contractors since at least 2004. Accordingly, these investigations would probably now be routed through the Department of Defense Office of the Inspector General, and reviewed under the provisions of PPD-19.

[139] Several IC elements already had whistleblower policies that provided reprisal protections for IC employees and contractors. PPD-19 enhanced those existing policies by creating a uniform prohibition on reprisal actions for making protected disclosures as well as requiring an IG review of reprisal allegations.

cial to be disciplined, the agency head (or her designee) that has personnel authority over both whistleblower and reprisor must take action.[140]

The President's decision to incorporate Title 5 by reference in PPD-19 permits use of Title 5's case law in the conduct of whistleblower reprisal investigations. Accordingly, this allows for use of critical doctrines such as those of "perceived whistleblowers," "constructive knowledge," and the three-part test for whether the agency would have taken the action absent the disclosure. The critical distinction to understand when assisting IC whistleblowers is that, unlike non-IC whistleblowers, the status of the employee or contractor is not the lead determinant in how to apply the law. Once you know you have an IC employee or contractor, what matters is really the *venue* of the disclosure, which the Legislature and the Executive branch have made the most important metric in classifying a case.[141]

Once the local agency review has been exhausted, the complainant may file for appeal to the ERP under PPD-19. The IC IG's acceptance of the appeal is discretionary.

In reviewing the appeal, the ERP will apply general acceptable standards of review to the reprisal allegations including, but not limited to "(i) Title 5, and applicable case law, in so far as possible; (ii) Council of Inspectors General on Integrity and Efficiency, *Quality Standards for Investigations* (2011), [and] (iii) Directives, instructions and other regulations of the originating agency."[142] Once the appeal is filed, the ICW&SP directorate will process the appeal.

VI. CONCLUSION

This article explored the interaction of law and geography as those disciplines are employed traditionally to order the world around us. The application of law to geography is what is known to law students as "real property," and it is a subject that a small minority of lawyers proceed to make their life's work. It is an easy construct to understand. But the

---

[140] Critics of an inspectors general–centric system of disclosure and reprisal investigation have cited conflict of interest as a major concern. *See, e.g.,* Vladeck, *supra* note 14.

[141] There has been a fair amount of confusion regarding the protection of IC contractors. Given the limits of the laws provided, IC contractors (and those disclosing on FISA matters in particular) have had substantially the same protections as non-contractors since 1982. "Existence" of the protections really cannot be debated but "effectiveness" is always a useful issue to review.

[142] IC IG EXTERNAL REVIEW PANEL, *supra* note 60, at pt. 7(A).

application of geography *to law* is a far harder concept to internalize. As the received English common law and later Royal administrative law were developing in both the Middle Ages and the Renaissance, the application of geography to law was perhaps more intuitive to a power elite living closer to the land than the modern federal bureaucrat. Concepts such as *gubernaculum* and *jurisdictio*, and the idea of the King's Writ running or not running, made sense to a people who found distance to be a challenge. Such concepts formed core tenets of medieval constitutional law.

And though our globalized polity collapses distance with technologies the medieval jurist would have found to be witchcraft, there is a good argument that some aspects of even modern governance instill the equivalent of "distance" even as that characteristic is mitigated in our day. Classification of information is one such characteristic. The need or desire to classify, and thereby promote aspects of prudence and opacity to achieve a Federal mission, places "distance" between the American sovereign and those agents executing the sovereign's intelligence and counterintelligence missions.

Having reviewed ICW&SP's concept of operations in Section I, we then articulated in Section II a paladin theory of Federal decision making, noting that when a sovereign's *jurisdictio* extends beyond the reach of the sovereign's utility, or ability to act, delegation is required to bridge the distance between *jurisdictio* and *gubernaculum*. That gap is an intellectual marchland, one determined by conditions unique to the particular nature of that Federal mission. For the Intelligence Community, it is secrecy and the nature of the clandestine and covert components of the intelligence and counterintelligence missions that create the march for the coequal mission of whistleblowing. Section III provided a transitional review of the context in which Federal decision making regarding whistleblowing has occurred. In Sections IV and V, we presented the record for Congress's limited actions on behalf of whistleblowing in the Intelligence Community, finishing with the observation that the 114th Congress began the process of codifying the march action that was PPD-19.

Through all of this discussion we have used principles providing the foundation of everyday decision making in the Republic's capital. These are a set of principles formed after, quite literally, centuries of European, European colonial, and American experience with the delegation of power from a sovereign to the agents of that sovereign. Where the run of the sovereign's will reflected in law is weak, the shared juridical tradition underlying decision making inside the Beltway provides for palatine systems of decision making. Under the paladin theory of Federal decision making, weak *gubernaculum* leads to delegation—delegation which then, in the field of whistle-

blowing, leads to specific choices between opacity and transparency, prudence and candor.

This is essentially what occurred after failure of legislative reform during the 111th Congress in the fall of 2010. The Executive branch created, at the President's discretion, a system of regulation in what we could call a *decision-making march*.[143] March systems are highly prudential, and not overly transparent. They are opaque and not always noted for their candor. In their creation, decision-making marches by necessity trigger concerns with sovereignty and who holds that status in any constitutional system.[144]

As we have noted, the intelligence community employee is *required* to blow the whistle under Executive Order 12674, *Principles of Ethical Conduct for Government Officers and Employees* (Apr. 12, 1989).[145] The order is obligatory and has been in effect since 1989. In the *Principles of Professional Ethics for the Intelligence Community*, "speaking truth to power"[146] is specifically delineated as a basic principle of the Intelligence Com-

---

[143] *See* BLACK'S LAW DICTIONARY 1118–19 (4th ed. 1951) (variety of entries following "March"); *id* at 1264 ("Palatine"). One must be careful to limit the metaphor. We are not inferring that the President has been granted royal authority; what we are stating is that in areas governing activity where the traditional workings of law are problematic (such as Intelligence collection and analysis), modern jurisprudence relies on forms similar to medieval decision making). Marches are not fixed. areas of law and economics long stable and subject to hearth-like regulatory controls can, due to technological innovation, become wonderfully unstable, foster entrepreneurship, and expand the national welfare. *See* Andrew C. Barrett, *Shifting Foundations: The Regulation of Telecommunications in an Era of Change*, 46 FED. COMM. L.J. 39 (1993). Cornell University's Professor Theodore J. Lowi coined the term "legiscide" to capture Congress's ill-disciplined delegation function; courts can do likewise, in a form of "juriscide." When both the Legislative and Judicial branches do this on the same subject matter and in deference to the Executive branch, you are likely to find the great chance of creating a decision-making *march* under the paladin theory. That is essentially what happened with the signing of PPD-19. *See* Barrett, *supra* note 36, at 171 n.22. The impact of creating a march, disconnected or remote from the juridical hearth, becomes clear when a march decision maker's exercise of discretion conflicts with a decision from the hearth itself. *See* Holly Doremus, *Scientific and Political Integrity in Environmental Policy*, 86 TEX. L. REV. 1601, 1603–09 (2008) (summarizing the failed Klammath biological opinion whistleblowing complaint).

[144] *See* Barrett, *supra* note 36, at 177 ("Where do *Schecter* and *Chevron* end? They end where questions of popular will begin.").

[145] Exec. Order No. 12,674, *supra* note 20, at pt. I, § 101(k).

[146] AMERICAN FRIENDS SERVICE COMMITTEE, SPEAK TRUTH TO POWER: A QUAKER SEARCH FOR ALTERNATIVES TO VIOLENCE (1955).

munity. PDD-19, *Protecting Whistleblowers with Access to Classified Information* (Oct. 10, 2012), establishes a framework for those whistleblowers speaking truth to power to effectively report waste, fraud, and abuse while simultaneously protecting classified information. All Intelligence Community employees are covered under both PPD-19's Section A (reprisal through adverse actions) and Section B (reprisal through any action affecting access to classified information). Contractors to the Intelligence Community are not covered under Section A, but do have Section B coverage.[147] This was the case on October 10, 2012, and that contractor protection was restated by the Director of National Intelligence in ICD 120, *Intelligence Community Whistleblower Protection* (March 20, 2014).[148]

The President adopted the policies and procedures used to adjudicate alleged violations of section (b)(8) of Title 5 "to the furthest extent possible." Accordingly, whistleblowing needs to be the disclosure of wrongdoing and not a policy dispute or an analytic dispute. And it needs to be made via some recipient capable of correcting the wrongdoing. Communication can be to an inspector general, an intelligence oversight official, a general counsel's office, a security office, or other entity. It can also be to Congressional committees of jurisdiction through the Intelligence Community Whistleblower Protection Act. The IC IG Hotline is available to facilitate this process.

So as the *Risen*[149] case slips from visibility, and those seeking to expand the journalist's privilege look for a new case to advance their cause, the Court will undertake, in the *McLean* appeal,[150] march decision making. An expansion of the journalist's privilege beyond its 1972 ambit would have been a move of whistleblower law from march to hearth, placing cases back at the American common weal's center in Article III courts. Instead, the Supreme Court seems to be taking up the more limited question of whether—following the delegation of national security whistleblowing issues to Executive branch officials with high levels of discretion—complainants should have access to fora such as the U.S. Office of Special Counsel, which make decisions ultimately appealable to the Court. If the Supreme Court decides against Special Agent McLean, they will have

---

[147] PPD-19, *supra* note 19, at pt. B (citing Exec. Order No. 12,968, 60 Fed. Reg. 40,245 (Aug. 2, 1995), which defines employees as including contractors at pt. 1, § 1.1(e)).
[148] ICD 120, *supra* note 16, at ¶ F.1.b.(1).
[149] 724 F.3d 482 (4th Cir. 2013), *cert. denied*, 82 U.S.L.W. 3530 (U.S. June 2, 2014) (No. 13-1009).
[150] 714 F.3d 1301 (Fed. Cir. 2013), *cert. granted*, 82 U.S.L.W. 3470 (U.S. May 19, 2014) (No. 13-894).

perhaps recognized that national security concerns over transparency, opacity, prudence, and candor require such matters to be decided under a paladin theory of Federal decision making.

What are the implications of these potential decisions? Stepping back from the sometimes-discordant Beltway dialogue over whistleblowing, achieving a balance between the flow of information regarding wrongdoing within the Federal government and the secrecy necessary to execute the intelligence and counterintelligence missions is important for more than operational reasons. Unlike any other act of self-governance, whistleblowing triggers visceral and raw emotions within some members of the power elite. The phrase "power elite" makes many Americans uncomfortable; we do not want to recognize that it exists or to study its characteristics and culture. Research common and prevalent in the 1950s, 1960s, and 1970s lost its relevance once the Baby Boomers came to power. It was almost as if, once the Baby Boomers came of age, there was agreement that an elite no longer existed to be studied.

Whistleblowing exposes the lie in that thinking. Disclosing bares the actions of the elite from within and forces correction, in many cases, from within. This creates no small amount of internal tension. But when a decision is made by an insider to escalate and move without, the elite will respond in spades. And how you define *within* and *without* delineates your constitutional ideology. If you make, for instance, an inspector general the "other" to be opposed, you are taking a position on your accountability within the American system of governance. Make the Congress "the other" to be opposed, and you are making a statement about your relationship to the American sovereign. It takes a fair amount of training and discipline to form a professional governing cadre reserved enough to weather a whistleblowing incident without seeking reprisal as a means to discipline the allegedly disloyal employee. The Federal government has yet to achieve such a level of discipline and training, and many federal officials even reject the necessity of doing so. This state of professionalism (or lack thereof) inside the Beltway creates "distance," too.

To help explain these modern equivalents of medieval "distance" in contemporary American governance, the authors developed and applied a paladin theory as they worked through whistleblower cases within the Executive branch. The paladin theory of Federal decision making draws on Professor McIlwain's characterization of Henri de Bracton's work. In *Federal No. 84*, Alexander Hamilton worked from principles not unlike those

Professor McIlwain resurrected[151] in 1947 from the works of the medieval jurist:

> It is improper—say the objectors—to confer such large powers, as are proposed, upon the national government, because the seat of that government *must of necessity be too remote* from many of the States to admit of a proper knowledge on the part of the constituent, of *the conduct of the representative body*. This is confined to the citizens on the spot. They must therefore *depend on the information of intelligent men*, in whom they confide; and how must these men obtain their information? Evidently from the complexion of public measures, from the public prints, from correspondences with their representatives, and *with other persons who reside at the place of their deliberations*.[152]

Here in the *Federalist* is Bracton and McIlwain's immutable concern with geography and decision making,[153] and the solution Hamilton relies upon is *whistleblowing*. Federalist No. 84 was published in three articles during the

---

[151] *See* MCILWAIN, *supra* note 30.

[152] THE FEDERALIST NO. 84 (Alexander Hamilton) (emphasis added). In this text, "the representative body" is the hearth; "many of the States" would be the march. *Compare* THE FEDERALIST NO. 14 (James Madison) (defining the hearth by stating "[a]s the natural limit of a democracy is that distance from the central point which will just permit the most remote citizens to assemble . . . so the natural limit of a republic is that distance from the centre which will barely allow the representatives to meet . . ."), *with* THE FEDERALIST NO. 17 (Alexander Hamilton) (defining the march by stating, "[i]t is a known fact in human nature, that its affections are commonly weak in proportion to the distance or diffusiveness of the object."). *Compare* GRAHAM ROBB, THE DISCOVERY OF MIDDLE EARTH: MAPPING THE LOST WORLD OF THE CELTS (2013) (purporting to have located the French and derivative British centres based on an application of the Ptolemaic system of *klimata*). Robb attempts to extend the system to Ireland. But it may be that a cultural marchland—a barrier preventing such an extension—separated the three societies. An Irish centre is, however, explored in MICHAEL DAMES, IRELAND: A SACRED JOURNEY (2000).

[153] Paladin decision making is not, in an age of instant technological communication, as much a factor of *geography* as it is a function of *capacity*. Law, for the most part, is memory from the hearth. Because we remember and we are just, we decide cases similarly but not identically. The bureaucracy seems to possess greater discretion than is permitted at the hearth in order to address new and unforeseen circumstances which memory can hinder. This is the nature of march decision making. It can also be a source of whim or violence. *See* Ryan Calo, *Code, Nudge or Notice*, 99 IOWA L. REV. 773, 797 (2014) (citing Robert M. Cover, *Violence and the Word*, 95 YALE L.J. 1601 (1986)).

summer of 1788, as New York debated adopting the Federal Constitution (1789). The first American statute promoting whistleblowing was signed a decade before; the first American intelligence agency had been in operation for thirteen years. Thus, the interaction of law and geography has been present in American decision making from the beginning.

Prior to the signing of the Declaration of Independence (1776), the Continental Congress created the Committee of Correspondence in 1775, three years before it enacted the first whistleblowing legislation for the American confederation. The committee was to gain, in part, the aid of foreign intelligence assets, including the sharing of information about British colonial policy. At the start of the hostilities, the committee seized and combed mail for vital intelligence information. Renamed the Committee of Secret Correspondence, and later the Committee of Foreign Affairs, it even employed trusted sympathizers in Britain to feed American leaders intelligence information. After establishing protocol for obtaining information, the committee established a network of couriers to disperse information to battlefield commanders and key government officials. All this leadership came from a legislature.

Two hundred and thirty-eight years later, Congress was poised to enact a Whistleblower Protection Enhancement Act, sweeping in its scope and depth. The reform initiative in the 110th Congress was truly historic. But there was no legislative reform. The popular will was not sufficient to support reform. And even under those proposed laws, problems would have persisted in protecting Intelligence Community employees from retaliation. The WPEA and FEPDA did not fully accomplish the goal of closing lacuna within the patchwork of regulations and laws providing Intelligence Community whistleblower protection while respecting the interests of Executive power and national security. There was a disconnect between the need for whistleblower protection and the will to so protect. Distance grew between the American sovereign and a problem needing to be resolved. Thus, in an act of march decision making, the President executed.