A Public Accountability Defense For National Security Leakers and Whistleblowers

A Public Accountability Defense for National Security Leakers and Whistleblowers

*Yochai Benkler**

In June 2013 Glenn Greenwald, Laura Poitras, and Barton Gellman began to publish stories in *The Guardian* and *The Washington Post* based on arguably the most significant national security leak in American history.[1] By leaking a large cache of classified documents to these reporters, Edward Snowden launched the most extensive public reassessment of surveillance practices by the American security establishment since the mid-1970s.[2] Within six months, nineteen bills had been introduced in Congress to substantially reform the National Security Agency's ("NSA") bulk collection program and its oversight process;[3] a federal judge had held that one of the major disclosed programs violated the Fourth Amendment;[4] a special President's Review Group ("PRG"), appointed by the President, had issued a report that called for extensive reforms of NSA bulk collection and abandonment of some of the disclosed practices;[5] and the Privacy and Civil Liberties Oversight Board ("PCLOB") found that one of the disclosed programs significantly implicated constitutional rights and was likely unconstitutional.[6] The public debate and calls for reform across all three branches of government overwhelmingly support the proposition that the leaks exposed lax democratic accountability of the national security establishment as well as

* Jack N. and Lillian R. Berkman Professor of Entrepreneurial Legal Studies, Harvard Law School, Faculty Co-Director, Berkman Center for Internet and Society, Harvard University. My thanks to Bruce Ackerman, Jack Balkin, Gabriella Blum, Jack Goldsmith, Aziz Huq, Orin Kerr, and Bruce Schneier for productive comments, and to Claire Johnson, Francesca Procaccini, and Michelle Sohn for excellent research.

[1] *See* Barton Gellman & Laura Poitras, *U.S. Mines Internet Firms' Data, Documents Show*, WASH. POST, June 6, 2013, at A1; Glenn Greenwald, *US Orders Phone Firm to Hand Over Data on Millions of Calls: Top Secret Court Ruling Demands 'Ongoing, Daily' Data From Verizon*, THE GUARDIAN (London), June 6, 2013, at 1.

[2] For a review of the offending practices and major reforms, see *Continued Oversight of the Foreign Intelligence Surveillance Act: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. (2013) (statement of Laura K. Donohue, Acting Director, Georgetown Center on National Security and the Law).

[3] Michelle Richardson & Robyn Greene, *NSA Legislation Since the Leaks Began*, AMERICAN CIVIL LIBERTIES UNION BLOG (Aug. 15, 2013, 10:48 AM), https://www.aclu.org/blog/national-security/nsa-legislation-leaks-began.

[4] Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013).

[5] *See* RICHARD A. CLARKE ET AL., LIBERTY AND SECURITY IN A CHANGING WORLD (2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf [hereinafter PRG REPORT].

[6] PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 103-37 (2014), *available at* http://www.pclob.gov/meetings-and-events/2014meetingsevents/23-january-2014-public-meeting [hereinafter PCLOB REPORT] (although the PCLOB also found that the government lawyers were entitled to rely on precedent for the opposite proposition as long as the Supreme Court did not directly hold on the matter).

practices widely viewed as threatening to fundamental rights of privacy and association. Nonetheless, the Justice Department pursued a criminal indictment against the man whose disclosures catalyzed the public debate. That prosecutorial persistence reflects a broader shift in the use of criminal law to suppress national security leaks in the post-9/11 state of emergency. That shift by the executive branch, in turn, requires congressional response in the form of a new criminal law defense,[7] the Public Accountability Defense I outline here.

The past decade has seen an increase in accountability leaks: unauthorized national security leaks and whistleblowing that challenge systemic practices, alongside aggressive criminal prosecution of leakers more generally. Most prominent among these have been leaks exposing the original "President's Surveillance Program" (known as "PSP" or "warrantless wiretapping"),[8] AT&T's complicity in facilitating bulk electronic surveillance,[9] and ultimately Snowden's leaks. Private Chelsea (then Bradley) Manning's disclosures to Wikileaks covered a broader range of topics and dominated newspapers throughout the world for weeks.[10] The Obama Administration, in turn, has brought more criminal prosecutions against leakers than all prior administrations combined,[11] and Private Manning's thirty-five-year sentence was substantially more severe than any prior sentence imposed for leaks to the press.[12] One possible explanation is that leaks *in general* have increased in number as a result of background technological change: digitization makes leaking documents easier and the prosecutions simply respond to the technologically-driven increase in leaks.[13] If this thesis is correct, then the increase in prosecutions is a "natural" response to a background change in leaking practice. There is, however, no robust evidence that the number of

---

[7] As will become clear, the defense calls for legislation aimed to counter systemic imperfections in the imperviousness of the national security establishment to public scrutiny. It is not based on any claimed speech rights of government employees. *See* Garcetti v. Ceballos, 547 U.S. 410, 426 (2006) (rejecting a First Amendment claim by a government employee who suffered retaliation for criticizing prosecutorial abuse he observed); United States v. Snepp, 444 U.S. 507, 526 (1980) (CIA agent's First Amendment rights not violated by requirement to submit books for review by Agency).

[8] *See* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Court Order*, N.Y. TIMES, Dec. 16, 2005, at A1; Michael Isikoff, *The Whistleblower Who Exposed Warrantless Wiretaps*, NEWSWEEK (Dec. 12, 2008, 7:00 PM), http://www.newsweek.com/whistleblower-who-exposed-warrantless-wiretaps-82805.

[9] *See* John Markoff & Scott Shane, *Documents Show Links Between AT&T and Agency in Eavesdropping Case*, N.Y. TIMES, Apr. 13, 2006, at A1.

[10] *See generally* David Leigh & Luke Harding, WIKILEAKS: INSIDE JULIAN ASSANGE'S WAR ON SECRECY (2011); Yochai Benkler, *A Free Irresponsible Press: Wikileaks and the Battle Over the Soul of the Networked Fourth Estate*, 46 HARV. C.R.-C.L. L. REV. 311 (2011).

[11] *See* David Carr, *Blurred Line Between Espionage and Truth*, N.Y. TIMES, Feb. 26, 2012, at B1.

[12] Justin Mazzola, *Chelsea Manning: Which One Doesn't Belong*, LIVEWIRE (Nov. 20, 2013), http://livewire.amnesty.org/2013/11/20/chelsea-manning-which-one-doesnt-belong/. For analysis of the other cases, *see infra* Part IV.

[13] *See* JACK GOLDSMITH, POWER AND CONSTRAINT: THE ACCOUNTABLE PRESIDENCY AFTER 9/11 73–76 (2012).

national security leaks has increased in the past decade or so.[14] Moreover, the technological thesis does not fit the fact that of the sixteen national security leak and whistleblowing cases of the past decade, only two—Manning and Snowden—were facilitated by the Internet and computers.[15] What does appear to have increased, however, is the number of national security leaks that purport to expose systemic abuse or a systemic need for accountability. This increase mirrors a similar spike during the legitimacy crisis created by the Vietnam War. Twelve to fourteen of the sixteen cases,[16] including Manning and Snowden, better fit a "legitimacy crisis" explanation for increased leaking concerning systemic failure.[17] The post-9/11 War on Terror and its attendant torture, rendition, indefinite detention, civilian collateral damage, and illegal domestic spying created a crisis of conscience for some insiders in the national security establishment. A consideration of the actual cases of the past decade suggests that it is this loss of legitimacy of decisions that likely underlies the increase in these kinds of systemic leaks. Technology certainly does play a role. It introduced the special challenges of bulk leaks, characterized by the Snowden and Manning cases, it has made detection and prosecution of leakers easier, and it has offered an alternative range of techniques outside the government to improve the ability to diagnose from the outside what is happening, as was the case with the disclosure of the secret prisons.[18] But the evidence does not support a thesis that there has been a general increase in leaks, nor does it support the idea that the relatively large number of leaks concerning arguably illegitimate action was primarily caused by a technological change.

If legitimacy crisis, rather than technological change, is the primary driver of the increase since 2002 of the particular class of leaks that is most important in a democracy, then the present prosecutorial deviation from a long tradition of using informal rather than criminal sanctions[19] represents a substantial threat to democracy. In particular, it threatens public accountability for violations of human and civil rights, abuses of emergency powers,

---

[14] *See* David E. Pozen, *The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information*, 127 HARV. L. REV. 512, 528–30 (2013) (surveying existing evidence).

[15] *See infra* Part IV. The Abu Ghraib photos were, of course, technologically mediated. But while these came to stand for broader abuses, they did not constitute a leak about a policy or practice as much as a self-destructive leak by the lower-level practitioners.

[16] *See infra* Part IV. These include Radack of the Department of Justice ("DOJ") on the Lindh prosecution; NSA whistleblowers Binney, Wiebe, Loomis, Roark, and Drake; AT&T leaker Klein; DOJ and CIA leakers of the PSP, Tamm and Tice, alongside Snowden and Manning. The unclear cases include Kirakou, depending on whether his prosecution is interpreted as retaliatory for disclosure of waterboarding, and Leibowitz, where there is disagreement about the contents of the disclosures. Of the remaining three cases prosecuted: Kim and Sterling appear to be garden variety leakers of the long-standing Washington model, swept up in the present leak investigation mood, while the Lawrence leak to the American Israeli Public Affairs Committee ("AIPAC"), often discussed together with the others, is more in the realm of espionage for allies than press leaks.

[17] *See* GOLDSMITH, *supra* note 13, at 71–72.

[18] *See id.* at 75.

[19] *See* Pozen, *supra* note 14, at 515.

and unchecked expansion of the national security establishment itself. Seen in that light, aggressive prosecutions are merely a symptom of the self-same post-9/11 national security overreach that instigated the legitimacy crisis: they manifest the government's need to shield its controversial actions from public scrutiny and debate.

Criminal liability for leaking and publishing classified materials is usually discussed in terms of a conflict between high-level values: security and democracy.[20] Here, I propose that the high-level abstraction obscures the fact that "national security" is, first and foremost, a system of organizations and institutions, subject to all the imperfections and failures of all other organizations. Considering that the Senate Select Committee on Intelligence ("SSCI") excoriated the CIA for groupthink failures in the lead up to the invasion of Iraq,[21] and again for its failures and dissembling in conducting its torture interrogation program,[22] it would be naïve beyond credulity to believe that the CIA, NSA, FBI, and Pentagon are immune to the failure dynamics that pervade every other large organization, from state bureaucracies to telecommunications providers, from automobile manufacturers to universities. When organizations that have such vast powers over life and death as well as human and civil rights, the risks of error, incompetence, and malfeasance are immeasurably greater than they are for these other, more workaday organizations. The Maginot Line did not make France more secure from Germany and neither torture nor the invasion of Iraq, with its enormous human, economic, and strategic costs, made America safer from terrorism, weapons of mass destruction, or rogue regimes. A mechanism for identifying and disrupting the organizational dynamics that lead to such strategic errors is necessary for any system of government, and in a democracy that mechanism is the principle of civilian control: fundamental questions of war and peace require public understanding and public decision.

Secrecy insulates self-reinforcing internal organizational dynamics from external correction. In countering this tendency, not all leaks are of the same fabric. "War story"-type leaks that make an administration look good or are aimed to shape public opinion in favor of an already-adopted strategy or to manipulate support for one agency over another, trial balloons, and so forth, are legion.[23] While these offer the public color and texture from inside the government and are valuable to the press, they do not offer a productive counterweight to internal systemic failures and errors. Some leaks, however, provide a critical mechanism for piercing the national security system's

---

[20] *See* Benjamin Wittes, *Against a Crude Balance: Platform Security and the Hostile Symbiosis Between Liberty and Security*, BROOKINGS INST. (Sept. 21, 2001), http://www.brookings.edu/research/papers/2011/09/21-platform-security-wittes.

[21] *See* SENATE SELECT COMM. ON INTELLIGENCE, REPORT OF THE 108TH CONGRESS, U.S. INTELLIGENCE COMMUNITY'S PREWAR INTELLIGENCE ASSESSMENTS ON IRAQ, S. REP. NO. 108-301, at 4–7 (2004).

[22] *See* 160 CONG. REC. S1487-91 (daily ed. Mar. 11, 2014) (statement of Sen. Dianne Feinstein).

[23] *See* Pozen, *supra* note 14, at 565–73, for a typology of the normal, "run-of-the-mill" leaks and "pleaks."

echo-chamber, countering self-reinforcing information cascades, groupthink, and cognitive biases that necessarily pervade any closed communications system. It is this type of leak, which exposes and challenges core systemic behaviors, that has increased in this past decade, as it did in the early 1970s. These leaks are primarily driven by conscience, and demand accountability for systemic error, incompetence, or malfeasance. Their critical checking function derives from the fact that conscience is uncorrelated with well-behaved organizational processes. Like an electric fuse, accountability leaks, as we might call them, blow when the internal dynamics of the system reach the breaking point of an individual with knowledge, but without authority. They are therefore hard to predict, and function like surprise inspections that keep a system honest.[24] By doing so, these leaks serve both democracy and security. This failsafe view of whistleblowing is hardly unique to national security. American law in general embraces whistleblowing as a critical mechanism to address the kinds of destructive organizational dynamics that lead to error, incompetence, and abuse. In healthcare, financial, food and drug, or consumer product industries; in state and federal agencies, throughout the organizational ecosystem, whistleblowers are protected from retaliation and often provided with financial incentives to expose wrongs they have seen and subject the organizations in which they work to public or official scrutiny.[25] Whistleblowing is seen as a central pillar to address government corruption and failure throughout the world.[26] Unless one believes that the national security establishment has a magical exemption from the dynamics that lead all other large scale organizations to error, then whistleblowing must be available as a critical arrow in the quiver of any democracy that seeks to contain the tragic consequences that follow when national security organizations make significant errors or engage in illegality or systemic abuse.

Aggressive prosecution of national security whistleblowers and accountability leaks threatens to undermine the checking function that whistleblowing provides. To address this threat, I propose that Congress adopt a new Public Accountability Defense as a general criminal defense, on

---

[24] I purposefully avoid the term "whistleblowing," although "accountability leaks" aim at that kind of leak, because the regulatory processes for internal whistleblowing threaten to cabin the debate to what would be legal under the existing whistleblower protection regime. Another way of reading "accountability leaks" would be to simply say "whistleblowing," but read this term capaciously, rather than merely limiting it to the existing legal definitions.

[25] *See, e.g.*, Whistleblower Protection Act of 1989, Pub. L. No. 101-12, 103 Stat. 16 (1989); *Other Workplace Standards: Whistleblower and Retaliation Protections*, DEP'T OF LABOR, http://www.dol.gov/compliance/guide/whistle.htm (last accessed Feb. 12, 2014). The Department of Health and Human Services provides substantial financial incentives to individuals who expose Medicare and Medicaid fraud. *See* 5 U.S.C. § 2302(b)(8)(A) (2012); *HHS Would Increase Rewards for Reporting Fraud to Nearly $10 Million,* DEP'T OF HEALTH & HUMAN SERVS. (Apr. 24, 2013), http://www.hhs.gov/news/press/2013pres/04/20130424a.html.

[26] See *e.g.*, TRANSPARENCY INTERNATIONAL, INTERNATIONAL PRINCIPLES FOR WHISTLEBLOWING LEGISLATION (November 2013), *available at* http://www.transparency.org/whatwedo/pub/international_principles_for_whistleblower_legislation.

the model of the necessity defense.[27] The defense would be available to individuals who violate a law on the reasonable belief that by doing so they will expose to public scrutiny substantial violations of law or substantial systemic error, incompetence, or malfeasance even where it falls short of formal illegality. It is most important to the leakers themselves, but would also be available to journalists and others who participate in disseminating the leaked information. It would provide a defense not only against specific criminal provisions protecting classified materials, but also against any charge brought for actions arising out of the same set of facts involved in the leak. Part III outlines the details. The basic model requires: (a) reasonable belief that exposure discloses a substantial violation of law or substantial systemic error, incompetence, or malfeasance, (b) mitigation to avoid causing imminent, articulable, substantial harm that outweighs the benefit of disclosure, and (c) communication to a channel likely to result in actual exposure to the public. The defense introduces a presumption of reasonableness where disclosed government actions can reasonably be characterized as grave violations of human rights, as substantial violations of civil rights or the constitutional order, as surveillance practices, or as decisions or abuses concerning other major life-threatening acts (primarily in war and public health).[28] The significance of the disclosed violations is the most important factor, and could dominate the outcome even where other elements, in particular harm mitigation, are weaker. Like any criminal defense, the proposal retains most of the deterrent effect of criminalization and places the risk of unavailability of the defense on the defendant. Moreover, full whistleblower protection would require more robust protections to avoid "punishment by process,"[29] most importantly a private right of action against abusive prosecutors and an attenuation of the prosecutors' qualified immunity, but these broader remedies are beyond the scope of this article. While incomplete, a formalized defense would nevertheless help restore an understanding upset by recent leak prosecutions: that where a person takes substantial personal risk reasonably calculated to inform the public about substantial abuses of government power, the state should correct itself, not the person who blew the whistle. The structure of the defense, in particular the requirement that the judge in the criminal case have an opportunity to pass on the legality or abusiveness of the exposed practices, should offer some deterrent to prosecutions of whistleblowers who expose practices that in fact raise substantial legal questions or systemic abuse.

---

[27] Model Penal Code Section 3.02(1).

[28] I base this list on the OPEN JUSTICE SOC'Y INITIATIVE, GLOBAL PRINCIPLES ON NATIONAL SECURITY AND THE RIGHT TO INFORMATION (TSHWANE PRINCIPLES) (2013), *available at* http://www.opensocietyfoundations.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles, which, although tailored to questions of classification, freedom of information law, and whistleblowing, offers a carefully considered standard against which to measure other proposals in the field.

[29] MALCOLM FEELEY, THE PROCESS IS THE PUNISHMENT (1992).

Part I outlines the critical system-correction role that leaks play in regulating information flow between the national security system and other systems in democratic society, once one understands the "security/democracy" tension in terms of the interaction of fallible institutional-organizational systems. Part II illustrates the theoretical framework with a description of the bulk data collection programs since September 11, 2001 and the ways in which leaks complemented highly imperfect formal oversight in providing correction. Part III describes the proposed Public Accountability Defense. Part IV examines twenty-two instances of leaks that resulted in prosecution or constituted whistleblowing or accountability leaks, from World War II to Snowden, suggesting that my proposal mostly comports with historical resolution of past events, although these past resolutions have been haphazard, rather than intentional.

I. Bureaucracy and Democracy, Secrecy and Security

A. The National Security Bureaucracy and Public Opinion: A Systems Approach

The question of secrecy and transparency in matters of national security is usually treated as a tension between security and democracy.[30] Discussion at that level of abstraction obscures more than it reveals, because national security and public accountability operate as practical social systems, not as values or broad interests divorced from the practices they describe. Both security and democracy are social practices instantiated in particular organizations and institutions[31] that form a system. By "system" I mean routinized interactions among organizations and institutions, objects and processes, technical platforms, and conceptual frameworks that provide agents with affordances and constraints. Systems set the parameters that shape the available observations of the state of the world, the range of possible actions, the valuations of competing actions and outcomes, and the outcomes of different actions in the practical domain in which they operate.[32] "Secrecy" and

---

[30] *See generally* Wittes, *supra* note 20.

[31] I loosely follow the distinction made by Douglass North, Institutions, Institutional Change, and Economic Performance (1991), but use a definition that follows the understanding of organizational sociology. By "organizations" I mean a set of routinized interactions among individuals, objects, and processes that coordinate the habits and practices of a defined set of individuals toward defined outcomes. A school, General Motors, the Pentagon, or the CIA is an organization. By "institutions" I mean more-or-less formalized instructions for the interaction among agents and organizations. Laws and regulations, well-understood norms, technical standards, are all "institutions." For intuitive reading, "organizations" should be read to mean a normal English understanding of the term, and "institutions" should be read as laws, norms, or their equivalents.

[32] The approach is related to the work of Niklas Luhmann and his school of thought. *See generally* Niklas Luhmann, The Differentiation of Society (1982). Exploration of the differences must await a later paper. In general, my focus here differs from a Luhmannian approach in that it (1) focuses on the ways in which systems overlap, interpenetrate, and colonize each other; (2) sees individuals as agents able to nudge, tug, and navigate within and

"transparency" are terms that describe the way one class of individuals and organizations shape the information flow both within and across the boundaries of the systems they occupy so as to pursue certain goals, exert power over individuals and organizations (shaping their beliefs, preferences, constraints, actions, and outcomes), both within the system and in neighboring systems, and resist the efforts of others to exert power over them.

The practical translation of this systems conception to national security is simple. "National security" is the system made up of state bureaucracies (the Pentagon, CIA, NSA, National Security Council ("NSC"), etc.) and market bureaucracies (Boeing, Lockheed Martin, Booz Allen Hamilton, Halliburton). Moreover, as Aziz Huq has explored in great detail with regard to the state actors, each of these discrete agencies and actors is itself a contingent, complex outgrowth of its own history and represents a discrete force in a constellation of forces, rather than a well-behaved "unit" in a coherent, well-controlled system.[33] This system deploys various ideas or concepts, like "national security" or "secrecy," to pursue goals and acquire resources (about four percent of GDP, or one-sixth of federal spending[34]), and a labor force of about one percent of the population of the United States who work inside the Department of Defense ("DOD")[35] with a similar number working on the market side of the system.[36] It uses secrecy to segment information flows about its structure and functions to allow it to project power in other systems and resist their incursions. Debates over secrecy and democracy involve disagreements over whether the actual information segmentation practices of the national security system act primarily to project power into what we consider "legitimate" targets—its parallels in other countries or non-state armed groups—or into systems we want to insulate from the power of the national security system: public opinion and the constitutional order. The actual leak cases of the past half century reveal that the secrecy protected in those cases was intended to project power into the American public sphere, although always defended as protecting power projection onto legitimate targets.

---

between systems in pursuit of goals, principles, and purposes in whose definition they have a normatively-significantly role (that is, they are autonomous, albeit situated, agents); and (3) is oriented toward normative evaluation.

[33] Aziz Huq, *Structural Constitutionalism as Counterterrorism*, 100 CAL. L. REV. 887, 904–18 (2012).

[34] *See* OFFICE OF MGMT. & BUDGET, HISTORICAL TABLES, TABLE 3.1: OUTLAYS BY SUPERFUNCTION AND FUNCTION 1940–2018, *available at* http://www.whitehouse.gov/sites/default/files/omb/budget/fy2015/assets/hist03z1.xls. Other tables *available at* http://www.whitehouse.gov/omb/budget/HISTORICALS.

[35] *DOD 101: An Introductory Overview of the Department of Defense*, U.S. DEP'T OF DEFENSE, http://www.defense.gov/about/dod101.aspx (last visited Apr. 17, 2014).

[36] Jennifer Rizzo, *Defense Cuts: The Jobs Numbers Game,* CNN (Sep. 22, 2011, 10:44 AM), http://security.blogs.cnn.com/2011/09/22/defense-cuts-the-jobs-numbers-game/.

B. Leaks as Corrective for Organizational, Informational, and Cognitive Imperfection

Once we abandon "national security" as an abstract concept and replace it with the actual system of organizations and institutions inhabited by human beings within and outside government, the question of leaks and whistleblowing becomes a question of system design. In particular, the question becomes designing the information flow mechanism between the national security system and at least two other systems: the constitutional order (those parts of Congress, the Judiciary, and the Presidency that are not part of the national security system) and public opinion.

Across a wide range of government agencies and private companies, the basic model of whistleblowing sees the individual insider as a critical corrective to the dynamics of organizations.[37] The model sees organizations as prone to error, incompetence, and abuse. Organizations control their own information flows to other systems so as to avoid the other systems exerting power to shape the practices arrived at through the internal dynamics of the organization. Whistleblowers create an alternative information channel. Whistleblowers are an important design element because their decision to open a new channel is uncorrelated with the internal practices, habits, and routines of the organization that caused the wrong. Whistleblowing, including leaking to the press to harness the system of public opinion, breaks through the managed information flows and provides external systems with the information they need to act on practices that the managed information flows underwrote.

The national security establishment has long been an exception to whistleblower protection, in particular whistleblowing in external channels that activate public opinion. Whistleblower protection came late to national security;[38] it does not cover civilian contractors, it limits external disclosure to Congress, and even then it gives national security agency heads the opportunity to resist disclosure.[39] In other words, for national security, current law protects secrecy at the expense of external review, even at the cost of securing bureaucratic independence from democratic accountability. The facially obvious reason is that revealing information that the national security establishment deems secret can have negative consequences such that the benefits of disclosure, generally thought worthwhile in less life-critical contexts than national security, do not in this context outweigh the costs of error, incompetence, and malfeasance within the system. Once stated in this form, the obvious counterargument emerges. To paraphrase Clemenceau, national security is too important to be left to national security insiders.[40]

---

[37] *See supra* note 25.

[38] *See* Intelligence Community Whistleblower Protection Act of 1998, 5 U.S.C. app. 3 § 8H (2012).

[39] *See id.* at § 8H(d)(2).

[40] John Hampden Jackson, CLEMENCEAU AND THE THIRD REPUBLIC 228 (1946).

If national security is so critical, then illegality, error, incompetence, and malfeasance are all the more important to identify and correct. The generals who designed and implemented the Maginot Line were all patriots; J. Edgar Hoover, legendary founding director of the FBI, was a stalwart of the national security establishment. The former led to the collapse of France in the Second World War.[41] The latter built a system of domestic spying and influence so powerful that it remained untouched during his life but was dismantled and utterly repudiated within a few years of his death, while his reign at the FBI became a standard reference point for abuse of power in America.[42] These are extreme but not exceptional historical examples. The national security establishment has no magical exemption from the dynamics that characterize all large organizations. Therefore there is no reason to believe that the damages of disclosure will systematically outweigh organizational failures and abuses, only that both sides of the equation may have very large values. The history of actual national security leaks, certainly those that resulted in substantial public exposure described in Part IV, overwhelmingly supports the contrary conclusion.

The literature on organizational, information, and cognitive imperfection is vast. Diverse lines of work in economics emphasize the tension between individual self-interest of agents and the organizational goal as a whole. New institutionalists are concerned with shirking and organizational costs,[43] while rational choice scholars are concerned with capture problems on the public organization side,[44] and principal-agent problems on the private side.[45] In any of its versions, economics suggests that national security organizations will be subject to influence by industry players who seek decisions that will line their pockets, that revolving door concerns will push high-level decision makers to adopt positions that fit industry needs, and that, at all levels of the security bureaucracy, individuals will try to cover their failures, make decisions that advance their own careers independent of what is best for the country, or try to expand their personal power and fiefdoms independently of whether doing so serves the broad organizational mandate or national interest. Recognizing these dynamics does not require a special distrust of military or national security establishments. It merely requires that we recognize that corporals and captains, colonels and generals, agents and deputy directors are people too, people operating in a large bureaucracy just like so many other employees, mid-level managers, and executives elsewhere in public service or the private sector. Economics, organizational sociology, management studies, and public administration all

---

[41] *See generally* H.W. KAUFMANN & J.E. KAUFMANN, FORTRESS FRANCE: THE MAGINOT LINE AND FRENCH DEFENSES IN WORLD WAR II (2006).

[42] *See The Truth About J. Edgar Hoover*, TIME, Dec. 22, 1975, at 18.

[43] *See generally* OLIVER E. WILLIAMSON, THE ECONOMIC INSTITUTIONS OF CAPITALISM (1986).

[44] *See generally* George Stigler, *The Theory of Economic Regulation*, 2 BELL J. ECON. & MGMT. STUD. 3 (1971).

[45] *See generally* Michael C. Jensen & Kevin J. Murphy, *Performance Pay and Top-Management Incentives*, 98 J. POL. ECON. 225 (1990).

include work that explores the failures introduced by practices, habits, and routines that prevent learning about the conditions in the world and adjustment in the face of change and uncertainty, and they all study approaches to overcome these failures or improve performance that are relevant in the national security sector.[46]

Literature on information dynamics and cognitive bias reinforces the idea that closed organizations will go awry systematically and predictably.[47] Substantial work establishes that groups tend to feed back their own beliefs into themselves, reinforce majority positions, and fail to challenge consensus beliefs—a process falling under the moniker groupthink.[48] Cass Sunstein described, for example, how the SSCI specifically saw groupthink as a central attribute of the CIA's failure in evaluating the threat of weapons of mass destruction in Iraq, a failure that contributed to the U.S. invasion of Iraq.[49] Aziz Huq surveyed the literature that explores the cognitive dynamics that emphasize security, predictability, control, and a resistance to opposition and uncertainty associated specifically with fear of terrorism.[50] These dynamics are exacerbated in hierarchical systems because advancement in these organizations requires that superiors not be antagonized. The "fundamental rules of bureaucratic life"[51] are at their core concerned with information flows: insulating bosses from criticism and information that would threaten to destabilize their judgment in front of subordinates. Even more fundamentally, error and biased interpretation of specific observations, background facts, and baseline presumptions are all subject to the dynamics of motivated reasoning.[52] That is, our most basic cognitive processes drive us to interpret the world and our observations to fit our existing understanding of the world. Finally, individuals in the national security system oversample threats and are involved in a system dedicated to avoid large unknown losses. Extensive work on the availability heuristic, loss aversion, and probability neglect suggests that insiders to the national security establishment will overstate the threats against which they are defending and the threat associated with

---

[46] *See* Charles Sabel & Jonathan Zeitlin, *Experimentalist Government*, *in* THE OXFORD HANDBOOK OF GOVERNANCE 168–87 (David Levi-Faur ed., 2011); *see generally* Paul DiMaggio & Walter Powell, *The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields*, 48 AM. SOC. REV. 147 (1983); Charles Sabel & William Simon, *Minimalism and Experimentalism in Administrative State*, 100 GEO. L.J. 53 (2011).

[47] *See* Cass Sunstein, *Group Judgments: Statistical Means, Deliberation, and Information Markets*, 80 N.Y.U. L. REV. 962, 964–67 (2005).

[48] *See, e.g.*, IRVING L. JANIS, GROUPTHINK 174–75 (2nd ed. 1983).

[49] Sunstein, *supra* note 47, at 965–66.

[50] *See* Huq, *supra* note 33, at 934–40.

[51] ROBERT JACKELL, MORAL MAZES: THE WORLD OF CORPORATE MANAGERS 115 (2009) ("(1) You never go around your boss. (2) You tell your boss what he wants to hear, even when your boss claims that he wants dissenting views. (3) If your boss wants something dropped, you drop it. (4) You are sensitive to your boss's wishes so that you anticipate what he wants; you don't force him, in other words, to act as a boss. (5) Your job is not to report something that your boss does not want reported, but rather to cover it up. You do your job and you keep your mouth shut.").

[52] *See generally* Dan Simon, *A Third View of the Black Box: Cognitive Coherence in Legal Decision Making*, 71 U. CHI. L. REV. 511 (2004).

leaks.[53] When a system whose insularity and secrecy disable external criticism, combined with individual cognitive and group information dynamics that contribute to poor diagnosis of the state of the world, substantial errors are inevitable. When this system is as large and complex as the national security system, and when the stakes of errors are so high, these dynamics reliably lead to periodic tragedy, abuse, or both.

Moreover, there are certain characteristics that make the national security system even more susceptible to the standard set of organizational decision-making errors, and less susceptible to correction.[54] Secrecy is pervasive in the national security system and prevents even internal sub-divisions from knowing enough to offer alternative views. It is linked to long and uncertain causal chains that make identifying the error or predicting its unintended consequences all the more difficult. The outcomes are not regular and smooth, such that outsiders and insiders can observe an external indicator such as a stock price, inflation rate, or employment statistics, to raise the alarm about a policy going wrong before it results in catastrophe or major abuse.[55] And finally, the mystique and cultural importance of patriotism make critique much harder to interpose, and much easier to ignore, than in more mundane areas that do not benefit from such strong emotional presumptions of worthiness. Mission critical organizations understand this and try to implement mechanisms to counteract the effect. From morbidity and mortality conferences in hospitals[56] to near-miss assessments on aircraft carriers,[57] organizations that must retain secrecy and confidentiality create internal models that encourage critical examination and mimic open criticism. Red teams in the military (like the Devil's Advocate in canonization) are among the canonical examples of mechanisms oriented to achieve that goal. The point is not that there is something inherently and particularly wrong about the military or national security systems as such. The point is that, effective as these internal efforts may be in many cases, they cannot truly escape the dynamics that lead to error. Open criticism from outsiders is also imperfect. But the sources of imperfection in open system criticism are uncorrelated with those of the internal dynamics, and it is that independence between the sources and forms of imperfection that creates the benefits of layering both internal and external systems—nowhere more so than in decisions of life and death.

Once we reject the implausible assumption that the particular organizations charged with delivering on national security are exempt from the dynamics that characterize all other organizations in all other sectors, and all other collective sense-making processes, then the question we face with na-

---

[53] *See generally* Cass Sunstein, *Fear and Liberty*, 71 SOC. RESEARCH: INT'L Q. 967 (2004).

[54] I owe these insights to Aziz Huq.

[55] Huq, *supra* note 33, at 930–34.

[56] *See generally* Jay Orlander and Graeme Fincke, *Morbidity and Mortality Conference*, 18 J. INTERN. MED. 656 (2003).

[57] *See* Charles F. Sabel, *A Real Time Revolution in Routines*, *in* THE FIRM AS A COLLABORATIVE COMMUNITY (Charles Heckscher & Paul Adler eds., 2006).

tional security leaks and whistleblowing is never abstract but always concrete. How much more error, incompetence, and malfeasance will we see in the critical area of national security by reducing whistleblowing through aggressive criminal enforcement of the Espionage Act,[58] the Computer Fraud and Abuse Act,[59] and other related laws, as compared to how much damage is national security likely to suffer from occasional major leaks if we create a well-structured defense for national security whistleblowers, and more generally if we bring national security whistleblower protection law more in line with whistleblower protection elsewhere in American law?

The problem with secrecy and security in a democracy runs deeper than correcting discrete errors or redressing instances of malfeasance. Secrecy goes to the heart of how "security" is defined. In particular it shapes whether security is defined along the contours of internally derived definitions of needs, beliefs, and actions within the national security system, or whether what counts as security is defined by public opinion.

Security is not a self-defining concept. The set of practices and routines we are willing to consider as security is the core decision that defines where "security" ends and "repression" begins. Bruce Schneier quipped colorfully that we could prevent all future plane bombings and hijackings: "simply ground all the aircraft."[60] If we encountered some other continental republic making such a choice we wouldn't call them "secure," we would call them "paranoid" or "defeated." We could prevent almost all future terrorist attacks on U.S. soil if we required every person to carry an internal passport and require clearance of all their movements by an antiterrorism unit, arresting any person observed in a place or time for which they were not pre-cleared. We would not call such a society "secure," we would call it "repressive." Secrecy of national security measures prevents democracy from playing precisely the role for which it was designed: managing hard choices about what to do and how much of it, to protect what, at what cost, to which other values.[61]

In a democracy, open debate and contestation provide a critical corrective to the destructive information and social dynamics of insulated organizations. Secrecy is never appropriate to insulate the current set of organizational practices of the national security system from democratic challenge regarding the basic external set of questions of what practices constitute security, and what constitutes repression or defeat. The level of risk we want to live with, the practices we are willing to endorse as a society in the name of security, and the level and forms of power we are willing to concentrate and locate within organizations charged with protecting national

---

[58] 18 U.S.C. § 793 (1996).

[59] 18 U.S.C. § 1030 (2008).

[60] BRUCE SCHNEIER, BEYOND FEAR: THINKING SENSIBLY ABOUT SECURITY IN AN UNCERTAIN WORLD 17 (2006).

[61] *See* Gene Spafford, *Security Through Obscurity*, CTR. FOR EDUC. & RESEARCH IN INFO. ASSURANCE & SEC. (Sept. 3, 2008), http://www.cerias.purdue.edu/site/blog/post/security_through_obscurity/ (explaining the origin of the term and qualifying its scope).

security—given the broad normative commitment to the set of values shared across a wide range of democratic societies in the early twenty-first century—lie at the very heart of the definition of security. This security function is merely a manifestation of the more general point: open society is a culture and set of institutions that harness the error correction, experimentation, and learning practices necessary for a society to adapt continuously to a highly uncertain, complex, ever-changing environment.

C. "But What About Plain Old Security?": Lessons From Computer Security

Even if we understand that the national security establishment can make mistakes, there remains the argument that secrecy is vital to security; that the price of transparency is too high. The argument gains force from the fact that understanding how security is enhanced by secrecy is intuitively trivial. A military unit is on its way to execute an attack on an enemy, and someone tips off the enemy who escapes or ambushes the troops. This is classic "transports on the way" secrecy that could be subject to prior restraint under the *Pentagon Papers* case.[62] Only one case of leaking to the press has ever involved a risk of this type: the case of Morton Seligman, who leaked decoded Japanese naval dispatches in the midst of World War II, and whose publication after Midway could have disclosed that the United States had broken Japanese naval codes.[63] This is the threat most legitimately interjected against leaks, but in all but that one World War II case, it has been pat hyperbole in criticisms of press leaks. Private Manning's disclosures to Wikileaks, for example, were denounced as likely to cause deaths, a claim that the Pentagon was not willing to repeat when asked for a formal assessment by the Senate Armed Services Committee.[64] Claims of secrecy of this sort normally assert power in the relationship between the national security system and the public opinion system.

Understanding how secrecy can *undermine* security requires more work. A brief diversion into computer security will help. Computer security is among the most complex systems-security challenges we face today. Yet the standard understanding, popularized through the term "no security through obscurity,"[65] is that secrecy is an imperfect and often self-defeating source of security. One of the most basic "general information security principles" is: "Open Design—System security should not depend on the

---

[62] *See* New York Times v. United States, 403 U.S. 713, 714 (1971).

[63] *See* Lawrence B. Brennan, *Spilling the Secret – Captain Morton T. Seligman, U.S. Navy (Retired), U.S. Naval Academy Class of 1919*, UNIVERSAL SHIP CANCELLATION SOCIETY LOG, Jan. 2013, *available at* http://www.uscs.org/society-archives/uscs-log-society-journal/. The Japanese Navy never made the connection, and the risk never materialized. *Id.*

[64] See Benkler, *supra* note 10, at 324 (describing claims about the effects of the leaks and Secretary Gates's response to Senator Levin's request for confirmation).

[65] *See* Spafford, *supra* note 61.

secrecy of the implementation or its components,"[66] a principle recognized since the early days of computer security.[67] This doesn't mean that secrecy offers no security, but that "the fewer secrets a system has, the more secure it is."[68]

Secrecy involves three distinct weaknesses. First, secrets are hard to keep. The more a system depends on secrecy as opposed to robust design, and the more its characteristics must be known to more people so they can work with it, the more susceptible it is to failure because it leans too heavily on that relatively weak link. Second, when secrets cover many facets of what makes a security system work, they tend to be interdependent and hard to change without changing the whole system. This makes security systems "brittle." They break when the secret is disclosed. A system with few secrets and few dependencies can change the information revealed to negate the revelation. If a password is revealed, it can be changed. If the core design is weak and its defense depends on secrecy, once the secret is out, the system is vulnerable. Ask Darth Vader.

The third problem with secrecy is its most important for our purposes: secrets undermine error correction. No system is perfect. None is perfectly designed in the first place, and systems, particularly complex systems that interact with an uncertain and changing environment, become less perfect as time passes: conditions change, threats change, and unanticipated interactions among components emerge. Error detection, resilience, healing, and experimentation with alternative solutions are critical to a well-functioning system. Secrecy severely limits the range and diversity of sources of insight for diagnosis and solution.

The point about error detection has broader implications for the relationship between the national security system and public opinion. Open, democratic societies are not weaker for their openness; they are stronger for it.[69] There are certainly inconvenient truths; backroom deals that have to be done, diplomatic channels that must be kept open. Public opinion can be fickle, leaders must sometimes take a longer view than present public sentiment will allow, and perfect transparency can be no panacea unless one imagines a utopia in which all members of the public are rational, well-informed, and patient. So yes, there are always troop movements that must be kept secret and much, much more. But there is also ambition and narrow-mindedness, interest, groupthink, and the yes-man mentality of the bureaucratic mindset. What has made open societies successful is their ability to learn, experiment, and adapt in a persistently uncertain and changing envi-

---

[66] KAREN SCARFONE ET AL., NAT'L INST. FOR STANDARDS & TECH., SPECIAL PUBLICATION 800-123, GUIDE TO GENERAL SERVER SECURITY 2–4 (2008), *available at* http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf.

[67] *See generally* Jerome H. Saltzer & Michael D. Schroeder, *The Protection of Information in Computer Systems*, 63 PROC. INST. ELECTRICAL & ELECTRONIC ENGINEERS 1278 (1975), *available at* https://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=1451869.

[68] SCHNEIER, *supra* note 60, at 128.

[69] *See generally* PAUL STARR, FREEDOM'S POWER: THE HISTORY AND PROMISE OF LIBERALISM (2008) (a historical survey of the relative strength of open societies).

ronment. On a much grander scale than computer security, secrecy undermines the most basic features by which open societies learn, question, and adapt; these are the very foundations of security in democratic society, and are congruent with, rather than in conflict with, the foundations of liberty in these societies.[70] It would be a mistake to imagine that the Counter Intelligence Program ("COINTELPRO"), the secret domestic spying program that the FBI ran against domestic dissenters (including leaders and activists in the civil rights and antiwar movements[71]) made America stronger and more secure at a cost to freedom and democracy. COINTELPRO made Americans less secure and less free, and less able to engage in the kind of criticism that helps us learn to distinguish between real, core threats to the lives and well-being of Americans and manufactured threats tailored to fit the views of those who sought to disrupt dissent.

II. Bulk Surveillance After 9/11: A Case Study in the Limitations of Closed Systems and the Role of Leaks in Enabling the Open System of Public Opinion as a Check on Power

The trajectory of the bulk surveillance system, in particular telephony metadata, over the dozen years from its implementation in October 2001 until early 2014 provides a lesson in the risks and failures of even well-designed closed systems like the post-Watergate delegated oversight system.[72] In particular, it shows how classification is wielded by actors in the national security system to defeat agents who inhabit the democratic oversight and independent review systems, the systemic limitations of "proper channels" accountability once these proper channels are severed from the ability to receive public criticism and harness public opinion to counter the

[70] This approach shares a basic commitment to the possibility of external evaluation of moral and practical "correctness" of collective actions with epistemic views of democracy. *See generally* David Estlund, *Beyond Fairness and Deliberation*, *in* Deliberative Democracy: Essays on Reason and Politics (James Bohman & William Rehg eds., 1997); Joshua Cohen, *An Epistemic Conception of Democracy*, 97 Ethics 26 (1986); Jules Coleman & John Ferejohn, *Democracy and Social Choice*, 97 Ethics 6 (1986). As will become clear, my commitment to living with endemic imperfection and uncertainty requires a more thoroughgoing tentativeness about the epistemic quality of the processes than Estlund's, and my emphasis on public opinion goes well beyond the problem of voting central to Cohen, Coleman, and Ferejohn. It most closely approximates Dewey's experimentalist view of democracy. *See* Charles Sabel, *Dewey, Democracy and Democratic Experimentalism* 9 Contemp. Pragmatism 35, 38–44 (2012).

[71] S. Rep. No. 94-755, at 10–12 (1976), *available at* http://www.intelligence.senate.gov/pdfs94th/94755_II.pdf.

[72] By "delegated oversight" I refer to the system put in place by the post-Watergate reforms, *see generally* Donohue, *supra* note 2, which took select members of Congress as part of select committees, select judges, as part of the Foreign Intelligence Surveillance Court ("FISC"), and select executive branch organs, like the agency Inspectors General or the Privacy and Civil Liberties Oversight Board ("PCLOB") and delegated to them authority to fulfill in secret tasks usually filled by all members of Congress and the Judiciary in processes open to public observation and criticism.

power of the national security system over matters understood as within its sphere, and the critical role that individual dissenters played as a corrective to the failures of the national security bureaucracy by rewiring the information flows between the systems.

A. The PSP from October 2001 Until 2007

Perhaps technological change to a ubiquitously networked, computationally-impregnated society and economy would have driven us to bulk surveillance without the attack on the World Trade Center.[73] Certainly, private companies implement pervasive surveillance on their own systems to improve marketing, and other countries, like China or Russia, are developing parallel practices facing different threat models and adhering to different conceptions of government power. But for purposes of understanding the particular story of how bulk surveillance developed in the American constitutional and political context, one must turn to the weeks after September 11, 2001.[74] Faced with the most devastating attack on U.S. soil since Pearl Harbor, the Bush Administration charged the NSA with creating a system that would allow early detection and prevention of future attacks. In response, the NSA developed, and the President authorized, the PSP,[75] one component of which was later disclosed and criticized as the "warrantless wiretapping" program.

Because that program required cooperation from telecommunications firms, the Administration sought Attorney General ("AG") sign-off on the legality of collecting telephone records in bulk without warrants. Approval by the AG would provide a mark of legitimacy and coax private companies to comply without court order. As part of this process, the Office of Legal Counsel ("OLC") had to provide independent analysis of the programs proposed. This first opportunity for oversight, internal to the Administration, was anchored in the historical professional independence of OLC. In this

---

[73] By "surveillance" I mean the collection of information about patterns of behavior that can be converted into effective action vis-a-vis the subject of the information. There is some debate as to whether information collected and stored without a human reading the material counts as surveillance. By my practical definition, whether the information is human-read or not only matters if the system requires human reading in order to have effects; if a marketing algorithm that targets ads (or more subversively, nudge-type messages) at me based on prior usage patterns, without ever being touched by a human being, that is surveillance because it shapes my perception and outcomes through the application of prior observation to present or future capabilities, opportunities, or configuration I inhabit; if meta-data or for that matter even only phone book data, if cross-referenced with other kinds of data, can lead to effective action upon the subject, that is surveillance. As machine processing becomes better, and automatic alteration of the information environment of subjects can get integrated better with machine processed data, the range of practices covered by the term "surveillance" becomes broader.

[74] *See generally* INSPECTORS GEN. OF THE DEP'T OF DEF., DEP'T OF JUSTICE, CENT. INTELLIGENCE AGENCY, NAT'L SEC. AGENCY, AND THE OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM (2009), *available at* http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/report_071309.pdf [hereinafter FIVE IGS REPORT].

[75] *Id.* at 5.

case, the Administration short-circuited that independence by permitting only one OLC lawyer, John Yoo, to be read into the programs: to receive enough information about them to form an opinion. This meant that only this particular individual could certify the constitutionality and legality of the program, and no one else in the hierarchical and peer review systems of OLC or the Department of Justice ("DOJ") could see facts that would allow them to challenge that conclusion. The opinion that resulted from this rump process was sufficiently weakly reasoned that as soon as Yoo left DOJ, his successors began processes to disclaim it. But for the first two years, secrecy insulated the PSP from this core internal, executive branch check. The failure of that system in those first two years does not mean it can never work. Indeed, the story of the conflict among then-head of OLC, Jack Goldsmith, Deputy AG James Comey, hospital-bed-bound AG John Ashcroft, and the White House over DOJ's refusal to continue to approve the programs after Yoo left is an exemplary tale of professional integrity playing its checking function.[76] The point is that the White House was able to use classification to rewire another system—the intersection of professional norms in the legal profession, and the organizational culture of OLC—in order to circumvent its designed checking function. As the DOJ resisted warrantless wiretapping, its functionality was preserved in part by components in the FBI, formally under the control of the AG, by dramatically increased use of National Security Letters. This practice was later found by the DOJ's Inspector General to have violated the Electronic Communications Privacy Act[77] and the pertinent Attorney General's guidelines.[78] Few parts of the story so clearly illustrate that the "systems" cross formal organizational boundaries. They are functional-sociological entities, not codified organizational relationships, and the counter-terrorism components of the FBI acted within the national security system, circumventing parts of the DOJ that function as elements of the constitutional order system.

Congressionally delegated oversight also existed during this period. On October 25, 2001, the White House reported to the Chairman and Ranking Member of the House Permanent Select Committee, and their counterparts on the SSCI.[79] They apparently raised no objections.[80] Given that the program was later determined to be illegal and its continuation required substantial changes to the law, that approval *sub silentio* should be treated as failed oversight, rather than as successful oversight and approval. In March 2004, after OLC and DOJ began to object to the program, the Administration again briefed a subset of the relevant congressional leadership, "the Gang of Eight."[81] According to later reports by Attorney General Gonzales,

---

[76] *Id.* at 20–26.
[77] 18 U.S.C. § 2510 *et. seq.*
[78] Inspector Gen., Dep't of Justice, A Review of the Federal Bureau of Investigation's Use of Exigent Letters and other Informal Requests for Telephone Records 2 (2010).
[79] Five IGs Report, *supra* note 74, at 16.
[80] *Id.*
[81] *Id.* at 23.

no one raised objections.[82] According to Congresswoman Nancy Pelosi, she did.[83] Whether or not private objections were raised, it was not until early 2007, almost six years after launch and three years after the internal DOJ objections, that the program was abandoned and replaced by new legislation. In the years since then, the NSA has offered several briefings to a broader set of congressional representatives.[84] But from public statements by congressional representatives, these briefings occur in special secure rooms, members are not permitted to take notes, and the overwhelming majority of members do not have staff with the clearance or training to understand the implications of technical descriptions.[85] The result is oversight theater: public enactment of the appearance of oversight, rather than real accountability. Operational secrecy similarly kept the Foreign Intelligence Surveillance Court ("FISC") on board but in the dark. Until early 2006, only the chief judge of the FISC was read into the program.[86] Reading a single judge into a program, while stating that it is absolutely critical to national security and without the normal process of evidence presentation and skeptical challenge makes the judicial notification a charade.

The early stages of the PSP provide a crisp example because there is little debate that at least that part of the program was illegal. Throughout the first years of operation, the White House used operational secrecy to shape the oversight process in ways that insulated the illegal program from effective challenge. It short-circuited the professional mechanisms intended to provide internal independent review within the executive branch, and it permitted the administration to severely constrain the access and possible effectiveness of the two other branches. The program was only shut down in early 2007, three years after the personnel changes within the DOJ precipitated its critique, and the FISC was only incorporated into the process in 2006. These changes followed soon after *The New York Times* reported on the program in December 2005, based on leaks by DOJ lawyer Thomas Tamm[87] and the April 2006 revelations by AT&T engineer Mark Klein of the

---

[82] *Id.* at 23, n.16.

[83] *Id.*

[84] *See* Letter from M. Faith Burton, Acting Assistant Att'y Gen., to Chairmen of the Senate and House Judiciary Comms. & Senate and House Intelligence Comms. (Mar. 5, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Mar 5 2009 Cover Letter to Chairman of Intel and Judiciary Committees.pdf; Letter from Ronald Weich, Assistant Att'y Gen., to Chairmen of the Senate and House Judiciary Comms. & Senate and House Intelligence Comms. (Sept. 3, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Sep%203%202009%20Cover%20letter%20to%20Chairman%20of%20the%20Intelligence%20and%20Judiciary%20Committees.pdf.

[85] *See* Alan Grayson, Op-Ed., *Congressional Oversight of the NSA Is a Joke. I Should Know, I'm in Congress*, THE GUARDIAN (Oct. 25, 2013, 7:45 AM), http://www.theguardian.com/commentisfree/2013/oct/25/nsa-no-congress-oversight; Justin Amash, Congressman, Lunch Keynote Address at the Cato Institute Conference: NSA Surveillance: What We Know; What to Do About It (Oct. 9, 2013), *available at* http://www.cato.org/events/nsa-surveillance-what-we-know-what-do-about-it.

[86] FIVE IGS REPORT, *supra* note 74, at 17.

[87] James Risen & Eric Lichtblau, *Spying Program Snared U.S. Calls*, N.Y. TIMES, Dec. 21, 2005, at A1.

deep tapping that AT&T enabled the NSA to perform.[88] Causal claims are difficult to prove, but timing strongly suggests that public exposure played a significant role in assuring that the most blatantly illegal aspects of the program were abandoned or fixed legislatively.

B. NSA Bulk Surveillance Since 2007

Materials leaked by Snowden or declassified in response to the criticism that followed suggest a similar pattern. First, as Judge Leon's December 16, 2013 opinion in *Klayman v. Obama*[89] makes clear, the telephony metadata program under Section 215 of the USA PATRIOT Act[90] may well violate the Fourth Amendment.[91] And yet, from May 2006, when the FISC began to approve bulk collection orders, until August 2013, apparently in response to the public outcry over the Snowden revelations, the FISC appears never to have considered the program's constitutionality. Moreover, the August 2013 opinion[92] did not even mention the most pertinent Supreme Court precedent: *United States v. Jones*.[93] That failure evidences systemic failure of the secret, ex parte, delegated judicial oversight model. No properly briefed judge writing an opinion for publication would have produced an opinion with such a glaring hole. Indeed, Judge Pauley's opinion in *ACLU v. Clapper* reaches the same conclusion as did the August 2013 FISC opinion, but with the benefit of proper briefing and anticipating publication, the opinion does indeed do the obvious: considers (and rejects) the *Jones*-based argument.[94] My point, therefore, is not that the telephony metadata program is necessarily unconstitutional or that it is impossible to write a competent opinion upholding it. The point is that for seven years the FISC did not bother to consider the question, and when it did, its opinion was one-sided and weak by comparison to opinions issued at the same time by other courts following the normal process of open court and published opinions.

The weakness of the FISC's analysis is underscored by the January 23, 2014 report by the PCLOB.[95] The report explained in detail why the telephony meta-data program could not be interpreted as coming under the precedent of *Smith v. Maryland*,[96] and in light of the opinions of five of the Justices in *United States v. Jones* likely violated Fourth Amendment under existing jurisprudence.[97] The timing of that report, however, strengthens the argument that internal mechanisms alone cannot assure proper oversight.

---

[88] *See generally* Markoff & Shane, *supra* note 9.
[89] 957 F. Supp. 2d 1 (D.D.C. 2013).
[90] Pub. L. No. 107-56, 115 Stat. 272 (2001), codified at 50 U.S.C. § 1861.
[91] *Klayman*, 957 F. Supp. at 9.
[92] *See In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things, No. BR 13-109 (FISA Ct. Aug. 2013), *available at* http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf.
[93] *See generally* United States v. Jones, 132 S. Ct. 945 (2012).
[94] ACLU v. Clapper, 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013).
[95] *See generally* PCLOB Report, *supra* note 6.
[96] 442 U.S. 735 (1979).
[97] *See* PCLOB Report, *supra* note 6, at 114–28.

The PCLOB was created in 2007 as a weak body[98] (only the chair is salaried and authorized to expend funds, while the other four members are volunteers).[99] It became operational in late May of 2013, days before the Snowden revelations.[100] At least four and a half years of the almost six-year delay were due to delayed nominations by both Presidents Bush and Obama.[101] These delays suggest that an administration interested in creating the appearance of oversight, rather than its actuality, can significantly hamper executive branch oversight.

While FISC judges did not consider constitutionality, they did work closely with the NSA to prevent abuses. The minimal staffing of the FISC, the technical complexities, the absence of opposing counsel, and the diversity and robustness of the programs that the intelligence community uses nonetheless limited the court's effectiveness. The secrecy and absence of public pressure puts the judges in a difficult if not impossible situation. Nowhere is this clearer than in opinions that found that the parameters they had set for collection, such as prohibiting the acquisition of wholly domestic communications, had been violated systematically.[102] In one opinion, Judge Walton stated that "[t]he minimization procedures proposed by the government in each successive application and approved and adopted as binding orders by the FISC have been so frequently and systematically violated that it can fairly be said that this critical element of the overall BR regime has never functioned effectively."[103]

The same dynamic characterized congressional oversight. For several years Senators Ron Wyden and Mark Udall, members of the SSCI, issued oblique warnings that the Administration's interpretation of the PATRIOT Act would shock the American people.[104] Their role inside the committee permitted them access to the information that allowed them to form their opinion, but the secrecy prevented them from mobilizing public support. Moreover, as the collection provisions came up for periodic reauthorization, the NSA and the Office of the Director of National Intelligence offered all members of Congress briefings that, read in hindsight, disclosed the fact of

---

[98] *See* Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 256 (2007).

[99] PRG REPORT, *supra* note 5, at 193–200.

[100] PCLOB REPORT, *supra* note 6, at 3–4.

[101] *See id.* at 4 (timing of the nominations and votes is blacked out); GARRETT HATCH, CONG. RESEARCH SERV., RL34385, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD: NEW INDEPENDENT AGENCY STATUS 2 (2012), *available at* https://www.fas.org/sgp/crs/misc/RL34385.pdf.

[102] Memorandum Opinion, No. [REDACTED] (FISA Ct. Oct. 3, 2011), *available at* https://www.aclu.org/files/assets/fisc_opinion_10.3.2011.pdf.

[103] *In re* Production of Tangible Things From [REDACTED], No. BR 08-13, 10–11 (FISA Ct. Mar. 2, 2009), *available at* http://www.documentcloud.org/documents/785205-pub-march-2-2009-order-from-fisc.html. When the court says "BR" it is referring to "Business Records," which is to say the materials produced under Section 215.

[104] *See* Letter from Senator Mark Udall & Senator Ron Wyden to Eric Holder, Att'y Gen. (Mar. 15, 2012), *available at* https://www.documentcloud.org/documents/325953-85512347-senators-ron-wyden-mark-udall-letter-to.html.

broad-based metadata collection.[105] Perhaps because the briefings were under conditions that prevented adequate staffing, perhaps because there was no electoral "angle" for members of Congress who could not reveal the nature of their objections publicly, the reality is that for years Congress did nothing to contain or reform the bulk collection programs. This inaction stands in stark contrast to the hive-like activity in Congress since the Snowden disclosures: nineteen bills have been introduced, and a Senate Judiciary Committee inquiry exposed that the telephony metadata program had not, as the directors of the NSA and National Intelligence publicly claimed, foiled fifty-four terrorist plots; to the contrary, the 215 program was responsible for, at most, one case, involving the transfer of $8500 to Al Shabaab by a Somali immigrant,[106] a finding later confirmed by the President's Review Group ("PRG").[107]

The stark discontinuity from years of inaction by any of the three branches' internal oversight processes to frenzied activity in all three makes clear that only the public disclosures and the outrage that followed them, and nothing else, were at the root of the reform. Claims to the contrary strain credulity.

Part of what the story tells us is that transparency is not merely a parallel mechanism of accountability alongside other models. It is the foundational driver of the successful operation of each of the other systems as well. Congressional oversight works when members know that the public will know and judge their actions. Judicial review works well in open court, but is hobbled by secrecy that denies judges the benefits of peer review and public accountability. And internal executive branch review also functions differently when insiders act in the dark, with no opportunity to recruit either public opinion or allies elsewhere in the Administration among those without privileged information access to push back on illegal or grossly mistaken policies.

III. A Public Accountability Defense

Leaks are widely used by insiders in both executive and legislative branches to manage public opinion.[108] Their unauthorized character lends

---

[105] *See* Letter from M. Faith Burton, *supra* note 84; Letter from Ronald Weich, *supra* note 84.

[106] *Compare Four Declassified Examples*, U.S. H.R. Permanent Select Comm. on Intelligence (last visited Mar. 16, 2014), *available at* http://intelligence.house.gov/1-four-declassified-examples-more-50-attacks-20-countries-thwarted-nsa-collection-under-fisa-section#overlay-context=highlights-june-18-open-hearing-fisa-program, *with Strengthening Privacy Rights and National Security: Oversight of FISA (Foreign Intelligence Surveillance Act) Surveillance Programs: Hearing Before the S. Judiciary Comm.*, 113th Cong. (2013) (statement of John Inglis, Deputy Dir., Nat'l Sec. Agency), *available at* http://icontherecord.tumblr.com/post/57811913209/hearing-of-the-senate-judiciary-committee-on (conceding that there was only one example "that comes close to a but-for example and that's the case of Basaaly Moalin").

[107] PRG Report, *supra* note 5, at 104.

[108] *See generally* Pozen, *supra* note 14.

them credibility, and the long tradition of forbearance in prosecutions helps maintain that credibility: if most leaks were prosecuted, leaks not prosecuted would come to be seen as sanctioned, and lose their credibility as tools for shaping public opinion.[109] Most normal leaks still are not prosecuted, and play a small role in securing public accountability. The defense I propose here is not concerned with these kinds of leaks. Instead, I focus on accountability leaks: those that expose substantial instances of illegality or gross incompetence or error in certain classes of particularly important matters associated with the activities of the national security system. These kinds of accountability leaks have been rare, appearing in two periods of significant crisis: first at the confluence of the Vietnam War and the Cold War with the anti-war and civil rights movements, and now again in response to some of the more extreme post-9/11 tactics and strategies. While rare, they represent instances where leaks have played a substantial role in undermining threats from the national security establishment to the constitutional order of the United States.

Accountability leaks are a critical safety valve for such moments. Unlike normal leaks, which preserve a space for leaking useful to leaders in the national security system and therefore enjoy a certain laxity in enforcement,[110] accountability leaks that expose systemic illegality, incompetence, error, or malfeasance challenge the system they expose in ways that make the leakers the target of heightened enforcement. Because the personal risk to the leaker in such critical leaks is high and will remain so even assuming adoption of a defense, national security accountability leaks to the press will continue to be rare. While human motivation is complex, and leaks of conscience are likely to come from individuals who already have a highly prosocial motivational structure, leakers are unlikely to be systematically impervious to the threat of aggressive prosecutions. Therefore, a defense likely will lower the threshold of a decision to leak, but only to a degree. Accountability leaks will only occur when the incongruity between what the system is doing and what conscience dictates to individual insiders is so great that they become willing to take that risk, and a defense would somewhat shrink the necessary magnitude of that incongruity. Because individuals are diverse in beliefs and sensitivity to the dictates of conscience, the exact locus of such a breach is highly uncertain, and most importantly, uncorrelated with where that individual is located in the decision-making process. It is this fact—that conscience is uncorrelated with well-behaved oversight—that gives leaks their unique pressure-valve role. Internal mechanisms may feel like they are working well to insiders because of the internal error dynamics of groups, even when they are, in fact, failing. Where the internal oversight mechanisms are functioning well, the pressure on the pressure valve will remain low. When those internal mechanisms fail, but insid-

---

[109] *Id.* at 562.
[110] *See id.*

ers continue to see them as succeeding (as they did with the surveillance and torture programs) the pressure valve of conscience is most likely to come into play. The fact that leaks are unpredictable from the perspective of insiders requires those insiders to operate on the assumption that if they do something sufficiently wrong, there is a nontrivial probability that someone, somewhere, will decide to leak it. The PRG expressed the restraining force of this mechanism as the "Front Page Rule."[111] The ungovernability of the combination of leaker and press makes it less manageable than the regular oversight system, and more susceptible to different forms of failure than the failures that caused the legitimacy crisis. That imperfection, in turn, is the reason it is appropriate to continue to maintain the baseline criminal sanctions, albeit moderated by the defense.

For decades, the systemic role of leaks was respected by the rarity of prosecutions. The recent slew of criminal prosecutions has upset that balance, and probably reflects the fact that the national security establishment adopted extremely controversial practices in the wake of the September 11 attacks, measures that flunked the "Front Page Rule" as soon as they were exposed. We have extensively discussed bulk surveillance. The CIA has been fighting tooth and nail to keep details of the SSCI damning review of its now-abandoned torture program secret,[112] and public exposure of the secret prisons system also led to abandonment of the practices and significant limitation of rendition programs.[113] The greater the incongruity between what the national security system has developed and what public opinion is willing to accept,[114] the greater the national security establishment's need to prevent the public from becoming informed. The prosecutorial deviation from past practices is best explained as an expression of the mounting urgency felt inside the national security system to prevent public exposure. The defense I propose is intended to reverse that prosecutorial deviation.

The proposal offers a framework to provide a criminal defense or sentencing mitigation factor, and is calibrated to protect individuals who release information of significant public benefit, and, where feasible, only the information necessary to inform the public of truly harmful government action. It is not intended to protect the much more common, run-of-the-mill national security leak that simply tells the story of this unit or that, this mission or the

---

[111] PRG Report, *supra* note 5, at 170. Note that a "Front Page" rule is Machiavellian, not normative: reasons of state can dictate immoral acts. The constraint is merely whether they can be framed so that, if made public, they will not cause a legitimacy crisis that would risk reversal and loss of power.

[112] Spencer Ackerman, *CIA and Senators in Bitter Dispute Over Capitol Hill Spying Claims*, The Guardian (March 5, 2014, 8:57 PM), http://www.theguardian.com/world/2014/mar/06/cia-and-senators-in-bitter-slanging-match-over-capitol-hill-spying-claims.

[113] Goldsmith, *supra* note 13, at 75.

[114] By "public opinion" I mean the actual pattern of opinions held by the public, accepting the outsized role of media elites, persuasion, and demagoguery. My position neither assumes nor depends on an ideal public, or a public that has gone through deliberative processes that make it more rational. *See generally* Bruce Ackerman & James Fishkin, Deliberation Day (2005).

other, or otherwise glorifies or vilifies actors in the national security system. By maintaining the general criminal prohibition while tying it to a defense and sentencing mitigation factor, the legal framework would still retain substantial risk for the person exposing the wrongdoing. By providing objective criteria for prosecutors as they evaluate whether to prosecute, for judges and juries as they decide cases, and for judges as they consider sentencing, the framework offers a person considering a leak a basis on which to form a belief, given their knowledge of the contents of the leak, about the likelihood of successful assertion.

The defense would cover individuals who violate a criminal provision to expose to public scrutiny substantial violations of law or systemic error, incompetence, or malfeasance. The emphasis of the defense would be on the government behavior disclosed, rather than on the motivation of the person disclosing. It requires only that the belief that the disclosure would expose substantial violations be reasonable, not that the government behavior disclosed is ultimately found to have in fact constituted a substantial violation of law or systemic error, incompetence, or malfeasance (for economy, I will refer to these as "systemic failure"). The defense is premised on the proposition that the leaker serves a public role, so the defense is public and systemic, rather than individual-rights based. As with qualified immunity for public servants, it is important that the defense be available for reasonable belief that the materials exposed show the pertinent kinds of violations, not that the actions disclosed are ultimately adjudged illegal. This belief element is objective, not subjective. If the matters revealed in the disclosure could not reasonably be seen as exposing substantial violations of law or systemic failure, the defense should not be available. For example, Samuel Morison, who leaked satellite photos of the construction of a Soviet aircraft carrier to *Jane's Defence Weekly*, claimed that he acted to persuade the American public to increase defense spending.[115] The claim of subjective belief is not the critical factor; rather, it is the implausibility of the claim that releasing the photos exposes substantial illegality or systemic failure on the part of the United States government in decisions about the level of defense spending in the early 1980s. The defense covers only disclosures through a channel reasonably likely to lead to public dissemination. There is no reason to protect leaks to a private party, much less to a foreign government, allied or enemy, not reasonably designed to lead to public disclosure. Thus, the case of Lawrence Franklin,[116] who gave information to AIPAC ("the American Israeli Public Affairs Committee ") for the benefit of Israel, would not be covered under this defense.

---

[115] Philip Weiss, *The Quiet Coup:* U.S. v. Morrison: *A Victory for Secret Government*, HARPER'S, Sept. 1989, at 54, 58, *available at* http://harpers.org/archive/1989/09/the-quiet-coup/.

[116] David Johnston, *Former Military Analyst Gets Prison Term for Passing Information*, N.Y. TIMES, Jan. 20, 2006, at A1.

The defendant must establish that (a) the disclosed actions were reasonably seen as illegal or constituted systemic error, incompetence, or malfeasance, (b) the disclosure used reasonable means to mitigate harms from the disclosure, and (c) the disclosure is to a channel reasonably aimed at public disclosure.

Much of the discussion below will go to the first showing the defendant must make—that the disclosed actions can reasonably be seen as illegal or systemic failure. A word is warranted about mitigation, in particular mitigation of bulk disclosures. Some disclosures can in fact cause substantial harm, even where they disclose wrongdoing. A leaker can mitigate the harm by limiting disclosure to information pertaining to the wrongdoing, by limiting and redacting disclosed documents to the minimum necessary, or by limiting the disclosure to a moment when it will no longer cause significant, articulable harm. A leaker can also mitigate by disclosing to an organization that has a capacity or history of managing sensitive documents responsibly. The latter technique will be the primary mitigation approach in cases of bulk leaking, like those of Snowden and Manning. These are likely to become more significant because, with digital storage, grabbing "everything" is often faster and harder to detect than grabbing only selected files that evidence wrongdoing. Because of the difficulty of securing and searching such bulk caches, this mitigation requirement will tend to favor traditional media outlets with the resources and experience to do so. In the second decade of the twenty-first century, this bias in the defense is hardly uncontroversial.

A major controversy in the Manning case concerned the role of Wikileaks. I have elsewhere discussed in depth why Wikileaks and other members of the networked fourth estate cannot be treated as second-class citizens under the First Amendment.[117] It is important to recognize, however, that equal status as speakers under the First Amendment does not automatically preclude the public accountability defense from favoring disclosure to recipients with the organizational and institutional capacity to minimize the operational damage disclosure could cause. Certainly, dumping all the materials online in a single unedited site would fulfill the "channel aimed at disclosing to the public" arm of the defense, but doing so would offer no meaningful mitigation. Disclosing to an established major media site is not more protected as a matter of the First Amendment but may be more appropriate for availability of the public accountability defense. If the leaker limits the documents disclosed, and properly redacts prior to publication, then the outlet chosen will be less important as to mitigation; but where the materials are leaked in bulk, that choice matters. As for Manning's choice of Wikileaks, I testified at the court martial that both the public perception of Wikileaks at the time of the leak and Wikileaks's ex-post alliance with traditional newspapers to redact and release the materials supported a finding that Wikileaks was a channel that a reasonable leaker in early 2010

[117] *See generally* Benkler, *supra* note 10.

would see as an outlet able to mitigate the harms.[118] One need not agree with my interpretation of the facts as they stood in early 2010 to recognize that some actors in the networked fourth estate will have established a reputation, or a set of well-understood practices that achieve mitigation in ways that are not inferior to those used by traditional media, or will work in collaboration with those media to mitigate the harms. Disclosure through such actors should be treated as no less evidence of proper mitigation than disclosure through *The New York Times* or *The Guardian*.

Once the defendant shows that the disclosed actions are reasonably characterized as violations, and that disclosure was reasonably designed to mitigate the harms, the burden shifts to the government to show by clear and convincing evidence that the harm is (a) specific, imminent, and substantial, and (b) outweighs reasonably expected benefits from the disclosure. The burden shifting recognizes that the government is more likely to possess the relevant facts about harm. The heightened burden reflects recognition that officials have tended to make broad claims of harm that do not withstand scrutiny.[119] Certain harms should simply be excluded from consideration—most obviously, where harm is from exposure of the wrongdoing. For example, where the information discloses gross human rights violations, and the damage of the disclosure is harm to the reputation of the United States, even to the extent of inflaming violent reaction among victims' nations, that harm should be inadmissible to refute the defense. The Abu Ghraib photos or the CIA torture program are obvious examples. Otherwise, the defense would paradoxically become less available as the behavior disclosed entailed more shocking and criminal conduct. Furthermore, where the harm is general, as opposed to imminent and specifically articulable, it should be accorded little weight. For example, in the case of the embassy cables disclosure, a general harm to frank communications within the State Department's system, or embarrassment in the relations of the United States with nations generally, are too general and vague to count as imminent, articulable harm. By contrast, exposure of names of specific individuals who are put at articulable risk by the disclosure is such harm.

Because the defense is intended as a systemic pressure valve to counter destructive internal dynamics, rather than an individual civil liberty of the leaker, the nature of the disclosed actions plays the dominant role in determining whether to excuse the individual's illegal acts. The more clearly

---

[118] I made the case for this claim in my testimony at the Manning trial, *see* United States v. Manning, Court Martial, (Fort Myer, VA, July 10, 2013), *available at* https://pressfreedomfoundation.org/sites/default/files/07-10-13-AM-session.pdf, https://pressfreedomfoundation.org/sites/default/files/REVISED-July-10-afternoon.pdf. The later disclosure of the full cache of embassy cables, one year later, was an organizational glitch not fundamentally different from what happened to the United States government itself when the measures it put in place to prevent a leak failed.

[119] *See*, *e.g.*, Benkler, *supra* note 10, at 324 (discussing Admiral McMullen's initial claims about the harm done, followed by Secretary Gates' more muted formal letter to Congress once evidence was demanded).

wrongful the action disclosed is, the more readily the defense should be available, even where other factors of the defense are weaker. The *Tshwane Global Principles* document,[120] developed by NGOs concerned with freedom of information and national security, offers a valuable list of core areas where the public interest in disclosure is particularly salient. Where the information pertains to these, the reasonableness of the public interest side of the equation should be presumptively satisfied and could only be outweighed by clear and convincing evidence that disclosure caused articulable imminent danger of the highest order, and even then, if the harm is reasonably mitigated, such as by delayed disclosure or redaction, disclosure should be excused:

- Substantial violations of human rights and domestic civil rights, and grave violations of international humanitarian law.
- Significant manipulations of public opinion, misstatements, or improper considerations in decisions to use military force or acquire weapons of mass destruction. While the risk of imminent harm from poorly timed release is clear, so too is the risk of gross error. It is precisely in deciding on the use of military force that groupthink and organizational failure in the national security and military establishments can have their most tragic consequences, and where informing the public sphere may offer the most critical counterweight to the internal dynamics of bureaucracies on the path to war.
- Secret laws or rules that govern use of national security or policing powers in ways that threaten life, limb, and liberty. This would cover, for example, OLC memoranda that systematically shape the legal framework governing executive branch actions with these critical effects. Secret law has no place in governing these kinds of threats away from any mechanism for public debate. Moreover, law or rules are generally most removed from operational needs, and of their nature cover patterns of practice involving civilian control over national security systems. Systematically, therefore, their secrecy is more likely to undermine oversight and public debate than to evade countermeasures by legitimate national security adversaries.
- Disclosure of the existence of a secret military, intelligence, or policing unit whose actions systematically involve one of the other categories of protected disclosure. While secrecy of some units is sometimes legitimate and necessary, public oversight is impossible over an agency whose existence is unknown.
- Surveillance programs and instances of abusive surveillance. Surveillance is so corrosive to individual freedom and democratic opin-

[120] *See generally* Open Society Founds., The Global Principles on National Security and the Right to Information (Tshwane Principles) (2013), *available at* http://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf.

ion formation, association, and expression that its existence and contours should always be subject to public scrutiny. The defense would cover both disclosures of programs, where they are illegal, unconstitutional, or represent systemic failure, and individual surveillance instances where a reasonable person would think that the surveillance constitutes an abuse (such as the FBI's wiretapping of Martin Luther King, Jr.).

- Disclosure narrowly focused on evidence of discrete constitutional or substantial statutory violations by parts of the national security establishment.

The presumptive categories are not intended to be exclusive. Where behavior does not fall within these presumptive categories, a judge hearing the defense will make a determination of reasonableness of the disclosure. Given the general baseline commitment of judges to their professional training and the rule of law, it is unlikely that, in the normal course, judges would find leaks that did not fall within the statutorily prescribed domains to be reasonable. Partly in aid of anchoring that determination, the statute should include certain kinds of public corrective action whose existence will serve as conclusive proof that their disclosure was in the public interest, or significant efforts to introduce corrective action that will shift the burden of proof that disclosure was not in the public interest. These include:

- Judicial finding that the exposed practice violates the Constitution or the law. An initial judicial determination later reversed will establish a presumption that the belief that the information should be disclosed was reasonable when taken.
- Congressional action. Passage of a law conclusively establishes reasonableness; introduction of bills not passed shifts the burden of proof to the government to show by clear and convincing evidence that the information should not have been publicly disclosed.
- Executive branch action. Significant change in the disclosed practices establishes the reasonableness of the belief. Significant reports or executive branch watchdog or review processes that find the disclosed practices must be changed will establish a presumption of reasonableness with regard to the initial disclosure.[121]
- Public opinion. Evidence showing that significant swaths of public opinions view the disclosed practices as illegal or requiring substantial change will create a presumption of reasonableness. This might be established by well-designed media studies, by the presence of

[121] This obviously creates a perverse incentive for the executive not to study the disclosures. The intuition behind this arm of the proof is that (a) the executive branch is sufficiently complex that different sub-systems within it will not necessarily be able to control each other, despite the formal unitary organizational structure of the executive, and that (b) executive branch correction will, in any case, usually occur only where public opinion demands it with sufficient force such that the marginal impact on the defense in a case against the leaker will likely be insufficient to control the action.

> petitions of sufficient scale, or by clear, professionally conducted opinion polls. Here I mean not a hypothetically informed public opinion, but the highly imperfect system of public opinion as it is constituted. While imperfect and subject to manipulation and fashions, its imperfections are different than those that plague the systems that make up the three branches of government, and the public accountability defense is specifically intended to undermine efforts to disable public opinion and the public sphere from exerting control over the national security system.

Cases involving accountability leak prosecutions will, of necessity, depend overwhelmingly on evidence that concerns classified materials. Passage of the defense will require some revision of the Classified Information Procedures Act.[122] In particular, materials publicly disclosed retain their classification, and a revised procedure should permit courts to accept into evidence all documents shown to be already in the public domain (such as where they are published online by a newspaper or other organization), and all descriptions of documents that disclose no more than was disclosed in descriptions that are in the public domain. While the classification power remains in the hands of the executive, the prejudice to the government's interest in maintaining secrecy of already publicly available documents is minimal, while the prejudice to the defense of inability to rely openly and publicly on materials central to the defense is substantial. Moreover, many aspects of the defense will require the court's consideration of disclosed materials that have not been declassified or disclosed. The systemic failures we observe in delegated oversight make it is impossible to accept deference to the government's judgments in these cases. Instead, the judge in the case must be able to assess the evidence both of the reasonableness of the wrongdoing and of the likelihood of harm. While *in camera* proceedings may be appropriate for some aspects of a case, these should be kept to a minimum. In particular, proceedings should be kept public unless the judge determines that no reasonable person could deem the disclosures as falling under the defense, or the government shows significant, substantial, imminent harm from holding open proceedings. Assuring this procedural aspect will be the primary protection of leakers from "punishment by process," because it is only the fear that the government's actions themselves will be assessed by an independent judge, in an adversarial process in public court, that would prevent prosecutors from bringing aggressive prosecutions that will cost defendants hundreds of thousands of dollars, years of fear, and ultimately demeaning plea bargains (even if there was no wrongdoing, as the case of Thomas Drake amply demonstrates).[123] Finally, the defense should clarify that in the absence of clear and convincing evidence by the government of imminent, articulable harm, the normal remedy for the government's insis-

---

[122] 18 U.S.C. app. 3 §§ 1–16 (1980).

[123] *See infra* text accompanying notes 148–51.

tence on keeping relevant materials classified should result in dismissal of the charges, rather than a lesser sanction.[124]

IV. The Defense and Past Practice

As a formal legal matter, the defense is a radical departure from existing law. However, the history of national security leaks suggests that the defense would cohere with actual practices and shared historical understandings of the public role those leaks played. A review of these cases seen through the lens of the public accountability defense offers context and confidence that its application in fact would represent a rebalancing relative to the recent prosecutorial deviation.

- 1942. *Morton Seligman* leaked decoded Navy messages of the Japanese order of battle to a reporter, whose publication could have exposed the fact that the United States had cracked the Japanese naval codes.[125] There was no disclosure of government wrongdoing, and the disclosure could have disabled a critical war-making capability—reading foreign enemy codes in a hot war. The defense would not be available. Seligman was not prosecuted. He was, however, left ashore and denied promotion.[126]
- 1970. *Christopher Pyle* disclosed in writing and congressional testimony the existence of a U.S. Army domestic intelligence program aimed at antiwar and civil rights activists.[127] The fact of domestic surveillance falls under the violations of civil rights, surveillance, and illegality. The revelations led to investigation by the Senate Judiciary Committee under Chairman Sam Ervin, who also hired Pyle to work on the subject for the Committee.[128] On the major attributes of illegality, abuse of civil liberties, and objective external indicia of public interest, Pyle's is an easy case. He was not prosecuted.

---

[124] *See* 18 U.S.C. app. 3 § 6(e)(2) (1980) (providing that where evidence is subject to non-disclosure, the court will dismiss the indictment, or, if dismissal does not serve justice, dismiss specified counts, find against the United States on issues to which the classified information pertains, or strike or preclude testimony covered by the non-disclosure determination). In the text, I propose that dismissal, rather than the provided lesser sanctions, should be the strong presumptive norm in cases of whistleblower prosecution, and that Congress should make that categorical determination when it fashions the public accountability defense.

[125] *See generally* Brennan, *supra* note 63.

[126] *Id.*

[127] *See* Christopher H. Pyle, *CONUS Intelligence: The Army Watches Civilian Politics*, Wash. Monthly, Jan. 1970, at 4; Christopher Pyle, *Conus Revisted, The Army Covers Up*, Wash. Monthly, July 1970, at 49.

[128] *See Christopher Pyle, Whistleblower Who Sparked Church Hearings of 1970s, on Military Spying of Olympia Peace Activists*, Democracy Now! (July 29, 2009), http://www.democracynow.org/2009/7/29/pyle.

- 1970. *Perry Fellwock* was the first major NSA leaker.[129] In an interview to *Ramparts* magazine he disclosed that the NSA existed and conducted extensive signals intelligence on the Soviet Union, that the agency had information sharing arrangements with other nations, and that it systematically recorded and searched phone calls into or out of the United States.[130] Fellwock was a less obvious candidate for the defense. Most of the revelations did not disclose clear wrongdoing, but the core disclosures did include two among the heightened public interest concerns: disclosure of the existence of a major military or intelligence body requiring oversight (the NSA) and disclosure of surveillance affecting broad swaths of the population. The former is an important category because one cannot perform oversight over a body one does not know exists, although the disclosures described no particular abuses; the latter because the question of how much electronic surveillance to employ is a matter of critical significance in any democracy. Disclosure was relatively narrowly circumscribed. What was disclosed was primarily the existence of a longstanding program, rather than particular operational details creating a present risk of harm, suggesting that the harm would be of the type that can be absorbed for sufficiently significant disclosures. Objective indicia that the disclosures covered matters reasonably considered meriting public scrutiny include that Fellwock's disclosures were part of the materials that the Ervin and Church Committees considered, and with regard to communications from the United States abroad, one can see the passage of FISA as in part responsive to these disclosures.[131] The defense, while less clear than in the case of Pyle, would apply; Fellwock was never prosecuted.
- 1971. *Daniel Ellsberg and Anthony Russo* present the paradigm case of defensible whistleblowing. Disclosing edited versions of the Pentagon Papers, Ellsberg offered materials that went to the heart of a core public interest—decisions about war-making—and was tailored to avoid specific articulable harm while fostering public accountability.[132] Disclosure to *The New York Times* was clearly calculated to reach the public.[133] As far as objective indicia are concerned, here the case would fall in the category of broad media coverage and

---

[129] Natasha Lennard, *The Original NSA Whistleblower: Snowden is a Patriot*, SALON (Nov 12, 2013, 4:42 PM), http://www.salon.com/2013/11/12/the_original_nsa_whistleblower_snowden_is_a_patriot/.

[130] *See generally* David Horowitz, *U.S. Electronic Espionage: A Memoir,* 11 RAMPARTS 35 (1972).

[131] *See generally* PATRICK RADDEN KEEFE, CHATTER: UNCOVERING THE ECHELON SURVEILLANCE NETWORK AND THE SECRET WORLD OF GLOBAL EAVESDROPPING (2005).

[132] *See* Daniel Ellsberg, *Secrecy and National Security Whistleblowing*, HUFFINGTON POST (Jan. 13, 2013), http://www.huffingtonpost.com/daniel-ellsberg/secrecy-and-national-secu_b_2469058.html.

[133] *Id.*

proof of impact on public debate (which in the fullness of historical time is unchallengeable, but may have provided significant barriers of proof were it to be proven as an element in the defense). Ellsberg was prosecuted, but the case was ultimately dismissed for prosecutorial misconduct.[134] In the broader historical narrative of the American collective memory, Ellsberg remains the paradigm case of a leaker whose acts should not have been prosecuted, and whose prosecutors and investigators are remembered as the primary offenders. Russo helped Ellsberg, was indicted with him, and his indictment was dismissed in the same process.[135]

- 1984. *Samuel Morison* disclosed satellite images of a Soviet aircraft carrier to *Jane's*.[136] This was an easy case for denying the defense: the disclosure did not fall into the major concerns of public interest, nor was it followed by any significant public acts of reform. Morison was convicted and sentenced to two years in prison.[137] He was later pardoned by President Clinton, largely on Senator Daniel Patrick Moynihan's concern that the Espionage Act had been applied erratically and inconsistently, with Morison's conviction being the sole conviction in its first eight decades.[138] Morison's two-year sentence suggests a proper departure point for sentences where disclosure does not meet the requirements of the defense, and the ultimate pardon suggests that even where the defense does not apply directly, the broad systemic considerations of assuring accountability through a well-informed investigative press may override considerations of national security and counsel against criminal prosecution in the absence of clear, articulable harm.
- 2002. *Jesselyn Radack,* a former DOJ attorney, disclosed information to the press that suggested that the prosecution of John Walker Lindh (the "American Taliban") was tainted by violations of Lindh's right to counsel, and that the prosecution removed documents—emails from her to interrogators—that would have established those violations at Lindh's trial.[139] The documents were not classified, though the DOJ claimed they were covered by attorney-client privi-

---

[134] *See Generally* Martin Arnold, *Pentagon Papers Charges are Dismissed; Judge Byrne Frees Ellsberg and Russo, Assails 'Improper Government Conduct'*, N.Y TIMES, May 12, 1973, at A1, *available at* https://www.nytimes.com/learning/general/onthisday/big/0511.html#article.

[135] *Id.*

[136] Stephen Engelberg, *Spy Photos' Sale Leads to Arrest*, N.Y. TIMES, October 3, 1984, at A8.

[137] Michael Wright & Caroline Rand Herron, *The Nation; Two Years for Morrison*, N.Y. TIMES, Dec. 8, 1985, at E4, *available at* http://www.nytimes.com/1985/12/08/weekinreview/the-nation-two-years-for-morison.html.

[138] Letter from Daniel Patrick Moynihan, U.S. Senator, to William Clinton, U.S. President, *available at* http://www.fas.org/sgp/news/2001/04/moynihan.html.

[139] Jane Mayer, *Lost in the Jihad*, NEW YORKER (March 10, 2003), http://www.newyorker.com/archive/2003/03/10/030310fa_fact2?currentPage=1.

lege.[140] The context—the first prosecution surrounding the Afghanistan war, and violations of individual constitutional rights in a tribunal held *in camera* for national security purposes—locates it closer to the concerns of this article. Radack was subjected to criminal investigations, pressure on employers that caused her to lose jobs, and efforts to have her disbarred.[141] The public accountability defense would have applied to her actions had she been charged, since the violations were of civil rights, and the harm was merely that the violations would have been exposed to a proper court. Its practical irrelevance to the sustained pressure on Radack, which did not take the form of a prosecution, underscores the fact that the government has substantial powers to intimidate bearers of inconvenient truths, even in the presence of a criminal defense.[142] Addressing these kinds of concerns would require not only expansion of the Federal Whistleblower Protection Act to national security, but also more toothsome remedies, perhaps through a federal tort, for abusive retaliation by any means.

- 2003. *Lawrence Franklin* conveyed classified documents about U.S. policy toward Iran to employees of AIPAC. Franklin is an easy case where the defense would not be available because his disclosures were not to a channel reasonably likely to inform the public. His initial thirteen-year sentence was later reduced to ten months of house arrest.[143]
- 2004. *Thomas Tamm and Russ Tice*, separately, were sources of the *New York Times* disclosures of the PSP.[144] These provide easy cases for eligibility of the defense. They narrowly disclosed, to a channel clearly calculated to inform the public, the existence of a program later found to be illegal and in violation of basic constitutional rights prohibitions on warrantless searches. Neither was prosecuted.[145]
- 2004. *William Binney, Kirk Wiebe, Ed Loomis, and Diane Roark* were three NSA employees and a congressional staffer (Roark) to the

---

[140] Radack v. United States Dep't of Justice, 402 F. Supp. 2d 99, 103 (D.D.C. 2005).

[141] *See* Frank Lindh, *America's 'Detainee 001' – the Persecution of John Walker Lindh*, THE GUARDIAN, (July 9, 2011), http://www.theguardian.com/world/2011/jul/10/john-walker-lindh-american-taliban-father.

[142] Jesselyn Radack, *A Whistle-Blower's Inside View of the Homeland Security Nominee*, L.A. TIMES (Feb 4, 2005), http://articles.latimes.com/2005/feb/04/opinion/oe-radack4. *See generally* JESSELYN RADACK, TRAITOR: THE WHISTLEBLOWER AND THE "AMERICAN TALIBAN" (2012).

[143] Nathan Guttman, *Once Labeled an AIPAC Spy, Larry Franklin Tells His Story*, JEWISH DAILY FORWARD (July 1, 2009), http://forward.com/articles/108778/once-labeled-an-aipac-spy-larry-franklin-tells-his/.

[144] Brian Ross, *NSA Whistleblower Alleges Illegal Spying*, ABC NEWS (Jan. 10, 2006), http://abcnews.go.com/WNT/Investigation/story?id=1491889; *Govt. Looks for Leaker on Warrantless Wiretaps*, NEWSWEEK (Aug. 12, 2007), http://www.newsweek.com/govt-looks-leaker-warrantless-wiretaps-99001?tid=relatedcl.

[145] Josh Gerstein, *Wiretapping Leak Probe Dropped*, POLITICO (Apr. 26, 2011, 8:00 PM), http://www.politico.com/news/stories/0411/53718.html.

then-Chair of the House Intelligence Committee. All four were involved in classic, *internal* whistleblowing (except in contacting a congressional staffer, albeit one privileged to be part of the oversight process): raising objections that the communications surveillance system the NSA bought, Trailblazer, was substantially more expensive and less respectful of civil rights than an in-house system developed by Binney, ThinThread.[146] Both NSA and DOD Inspectors General ultimately agreed that Trailblazer was an expensive failure. The four disclosed nothing to the press, and pursued a concern later validated, but were subject to aggressive and disruptive investigation, their homes were raided, and they were named as unindicted co-conspirators in the Drake indictment.[147] Their cases offer an important example of abusive investigation and punishment by process.

- 2004/2005. *Thomas Drake* was an NSA employee in several leadership positions, who had supported Binney et al. in the concerns they voiced and was a major source for the DOD Inspector General's report on Trailblazer.[148] Frustrated with the lack of effect of the internal paths that he, Binney, Wiebe, and Loomis had taken, Drake discussed fraud and waste at the NSA with a *Baltimore Sun* reporter, without disclosing any classified information.[149] Drake was indicted under the Espionage Act, charged with ten counts (each carrying a ten-year sentence),[150] and he ultimately pled guilty to retention of national security information, though the prosecution could show no disclosures of classified materials.[151] Like Radack's mistreatment, the Drake prosecution, which dragged on for several years and placed him under threat of substantial penalties, is a crisp example of abuse of prosecution as punishment for whistleblowing. The breadth and vagueness of the Espionage Act or the Computer Fraud and Abuse Act make it possible to bring a prosecution carrying grave consequences against someone who brought matters of public concern to the public without disclosing any classified information. This kind of *in terrorem* process requires a remedy, perhaps by limiting the qualified immunity prosecutors and investigators normally enjoy,

---

[146] Jane Mayer, *The Secret Sharer*, NEW YORKER (May 23, 2011), http://www.newyorker.com/reporting/2011/05/23/110523fa_fact_mayer?currentPage=all.

[147] *NSA Whistleblower Kirk Wiebe Details Gov't Retaliation After Helping Expose "Gross Mismanagement,"* DEMOCRACY NOW! (Dec 19, 2013), http://www.democracynow.org/2013/12/19/nsa_whistleblower_kirk_wiebe_details_govt.

[148] *See* Mayer, *supra* note 146.

[149] Siobhan Gorman, *System Error*, BALT. SUN (Jan 29, 2006), http://articles.baltimoresun.com/2006-01-29/news/0601280286_1_intelligence-experts-11-intelligence-trailblazer; *see also* Mayer, *supra* note 146.

[150] Scott Shane, *Former N.S.A. Official Charged in Leaks Case*, N.Y. TIMES (Apr. 15, 2010), http://www.nytimes.com/2010/04/16/us/16indict.html?_r=0.

[151] *See* Reuters, *Ex-Official for N.S.A. Accepts Deal in Leak Case,* N.Y. TIMES, Jun. 11, 2011, at A14.

but is unlikely to be resolved adequately within the confines of the criminal defense discussed here.

- 2006. *Mark Klein*, a retired AT&T employee, disclosed to *The New York Times*[152] that AT&T had voluntarily complied with NSA requests to monitor Internet communications that pass through AT&T's facilities in a major switching facility in San Francisco.[153] Klein's disclosures played a central role, alongside Tamm and Tice, in exposing the PSP.[154] Klein did not have security clearance and the documents he disclosed were unclassified technical documents whose national security meaning became apparent only in the context of their use in connection with the installation of a secret room within the AT&T facility.
- 2006. *Jeffery Sterling* leaked details of a successful CIA operation to feed defective information to Iran's nuclear weapons program; it presented no obvious insight into any plausible violation of law or systemic failure.[155] While useful to the media, the failure to disclose actions that a reasonable person would consider a violation of law or systemic failure would make the public accountability defense unavailable.[156]
- 2009. *Shamai Leibowitz* presents a complex case. Leibowitz was an FBI translator. He leaked transcripts of intercepted calls to a regularly publishing blogger. Details are scarce because the materials were never published.[157] Leibowitz claimed that his disclosures were intended to expose FBI illegal acts,[158] "very similar to what Edward Snowden has reported about the NSA."[159] The blogger told *New York Times* reporter Scott Shane that Leibowitz leaked Israeli embassy intercepts, and was trying to expose Israel's aggressive efforts to shape American public opinion and policy, in particular toward a

---

[152] *See generally* Markoff & Shane, *supra* note 9.

[153] *See generally* Affidavit of Mark Klein, Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006) (No. 06-CV-0676), *available at* https://www.eff.org/document/klein-declaration.

[154] *See The NSA Whistleblower*, ABC NEWS (March 7, 2007), http://abcnews.go.com/Nightline/video?id=2930944.

[155] Greg Miller, *Former CIA Officer Jeffrey A. Sterling Charged in Leak Probe*, WASH. POST (Jan. 6, 2011), http://www.washingtonpost.com/wp-dyn/content/article/2011/01/06/AR2011010604001.html.

[156] Public debate surrounding the events had to do with the fact that investigators issued a subpoena to James Risen, the *New York Times* reporter to whom Sterling leaked, and thereby threatened reporters, not only the leaker.

[157] Scott Shane, *Leak Offers Look at Efforts by U.S. to Spy on Israel*, N.Y. TIMES, Sept. 5, 2011, at A1.

[158] *See* Shamai Leibowitz, *Blowback From the White House's Vindictive War on Whistleblowers*, THE GUARDIAN (July 5, 2013, 8:30 AM), http://www.theguardian.com/commentisfree/2013/jul/05/blowback-white-house-whistleblowers.

[159] Shamai Leibowitz, *Edward Snowden and the Crackdown That Backfired*, LEIBOWITZ BLOG (June 24, 2013), http://www.shamaileibowitz.com/2013/06/edward-snowden-man-of-conscience.html.

strike on Iran's nuclear capabilities.[160] Leibowitz denied this outright,[161] but was constrained by his plea agreement from providing further details.[162] Contemplating the risk of long imprisonment, Leibowitz pled guilty to a lesser offense and was sentenced to twenty months imprisonment.[163]

Remarkably, the judge apparently had "no idea" what documents Leibowitz had leaked, and why they had compromised security.[164] If the documents in fact were, as the recipient claimed, about aggressive and misguided moves by the government of Israel, then an American court cannot recognize these as providing a defense to violation of American secrecy laws. If, however, the documents disclosed, as Leibowitz claims, illegal and unconstitutional phone taps by the FBI, then his case would fall squarely within the public accountability defense.[165]

This case underscores the important effect the defense could have on moderating the prosecution's considerations as to whether to bring a case in the first place. If the public accountability defense had been available, prosecutors would have had to contend with the possibility that, if they prosecuted the case and it involved documents that disclosed illegality, the defendant could assert the defense and a federal judge who was not part of the FISC would consider the legality of the agency's action.[166] Systematically, the more clearly illegal or wrongful the official behavior disclosed, the higher the risk to the national security establishment from such an independent judicial review, and the less likely a prosecution. That systematic effect is a

---

[160] *See* Shane, supra note 157; *see also* Richard Silverstein, *Why I Published US Intelligence Secrets About Israel's Anti-Iran Campaign*, TRUTHOUT (Oct. 14, 2011, 11:25 AM), http://www.truth-out.org/news/item/3499:why-i-published-us-intelligence-secrets-about-israels-antiiran-campaign.

[161] *See* Leibowitz, *supra* note 159.

[162] Maria Gold, *Former FBI Employee Sentenced for Leaking Classified Papers*, WASH. POST (May 25, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/05/24/AR2010052403795.html ("As part of the arrangement, he agreed to file no requests for documents concerning the investigation and to 'never disclose,' except to those who are authorized by the government, any classified or sensitive information he learned while working for the FBI.").

[163] Stephen Aftergood, *Jail Sentence Imposed in Leak Case,* SECRECY NEWS (May 25, 2010), http://blogs.fas.org/secrecy/2010/05/jail_leak/.

[164] Shane, *supra* note 157 ("'All I know is that it's a serious case,' Judge Alexander Williams Jr., of United States District Court in Maryland, said at the sentencing in May 2010. 'I don't know what was divulged other than some documents, and how it compromised things, I have no idea.'").

[165] The fact that disclosure was to a blogger, rather than a traditional journalist, is not dispositive. The blog appears to be regularly published, and a reasonable channel for public communication, even if it failed to publish in this instance. Moreover, the fact that the documents were never published argues against a finding that disclosing the documents to that blog was tantamount to dumping the documents online unedited and unredacted.

[166] This would require a more general review of the use of classified evidence in criminal trials.

desirable effect of the defense, given the enormous costs to leakers associated with being indicted, even for leakers who would ultimately win on the defense.

- 2009. *Stephen Kim* was a State Department employee who leaked the existence of a conversation suggesting that North Korea was about to test a nuclear bomb.[167] While the subject is of critical public interest, there was no suggestion of illegality or systemic failure in the U.S. government's decision to keep the information secret. Moreover, disclosure was not aimed to, nor was it likely to lead to, a significant change in American law or policy in a way that corrects internal systemic errors. The harm was mostly retrospective, and in this regard likely minimal, which would militate against prosecution, but the public accountability defense on its own terms would be either entirely unavailable or very weak. In January of 2014, Kim pled guilty and agreed to serve a thirteen-month prison term.[168]

  The primary public debate in the case surrounded the fact that prosecutors characterized James Rosen, the Fox News reporter to whom Kim had leaked, as having behaved "much like an intelligence officer would run an [sic] clandestine intelligence source,"[169] and asserted under oath that "there is probable cause to believe that the Reporter has committed a violation of 18 U.S.C. Sec. 793 (part of the Espionage Act), at the very least, either as an aider, abettor, or co-conspirator of Mr. Kim."[170] While my discussion throughout this paper has focused on the leakers themselves, who have been the subject of prosecutions to date, the systemic justifications of the defense require that it be available to the public outlets of the leaked materials as well—the reporters, news outlets, and, because their relative political weakness makes them more politically-palatable targets, outlets in the networked fourth estate in particular. In other words, the defense must be available on its own systemic terms, by statute, over and above any First Amendment claims the public speakers who disseminate the information may have.[171]
- 2007/2012. *John Kiriakou* presents a compound case. The leak for which he was prosecuted was an unintentional disclosure of the iden-

---

[167] Charlie Savage, *Ex-Contractor at State Dept. Pleads Guilty in Leak Case*, N.Y. TIMES, Feb. 7, 2014, at A10.

[168] Josh Gerstein, *Stephen Kim Pleads Guilty in Fox News Leak Case*, POLITICO (Feb. 7, 2014, 2:25 PM), http://www.politico.com/story/2014/02/stephen-kim-james-risen-state-department-fox-news-103265.html.

[169] *See* Application for Search Warrant ¶ 39, *In re* Search of E-mail Account [REDACTED]@gmail.com on Computer Servers Operated by Google, Inc., No. 10-MJ-00291-AK (D.D.C. Nov. 7, 2011), *available at* http://apps.washingtonpost.com/g/page/local/affidavit-for-search-warrant/162/.

[170] *Id.* at ¶ 40.

[171] For a discussion of the limited protection the First Amendment offers journalists against criminal prosecution, the role of constitutional culture, rather than constitutional law, and the risks this poses for the networked fourth estate, see Benkler, *supra* note 10, at 363–65.

tity of a CIA agent,[172] the kind of information least likely to fit the defense because it places an individual at risk while exposing no violations of law or systemic failure. Kiriakou was sentenced to thirty months imprisonment for this disclosure.[173] However, there is some possibility that Kiriakou was singled out for prosecution because he had earlier leaked details about the CIA's infamous torture program, disclosures for which he was not prosecuted.[174] It should be clear that disclosure of torture, a program that so clearly violates fundamental human rights, goes to the very heart of a public accountability defense. Should a leaker offer details that substantiate the presence, scope, or responsibility for such systematic violation of as basic a human right as the prohibition on torture, the leaker should enjoy full immunity under almost any circumstances. Perhaps, in an extreme case where disclosure directly endangered, in the immediate future, actual, identifiable lives, culpability could attach. But disclosure of systematic torture is perhaps the clearest example of a leak that will almost certainly be protected. The Kirakou case therefore suggests that where the government is pursuing an action on an unrelated disclosure, itself illegal, the court must take into consideration the totality of the disclosures; and where the actual charge, even if true, is found to be pretextual or peripheral to the core disclosure, the defendant should be eligible for the defense.

- 2010. *Chelsea (Bradley) Manning* was responsible for leaking several hundred thousand reports (so called "war logs") from units in Iraq and Afghanistan, and 250,000 State Department embassy cables to Wikileaks.[175] Several potential violations of human rights or laws of war were disclosed by some of the war logs, alone or in combination. A helicopter gun camera video showed a gunship attacking a civilian van offering aid to individuals injured by an earlier attack from the same gunship.[176] This second strike injured two children who were in the van and apparently killed a Reuters reporter who

---

[172] Scott Shane, *Ex-Officer Is First From C.I.A. to Face Prison for a Leak*, N.Y. TIMES (Jan 5, 2013), http://www.nytimes.com/2013/01/06/us/former-cia-officer-is-the-first-to-face-prison-for-a-classified-leak.html?pagewanted=all.

[173] *Id.*

[174] *See, e.g.*, John Kiriakou, *I Got 30 Months in Prison. Why Does Leon Panetta Get a Pass?*, L.A. TIMES (March 9, 2014), http://articles.latimes.com/2014/mar/09/opinion/la-oe-kiriakou-panetta-whistleblower-20140309; Associated Press, *CIA 'Whistleblower' John Kiriakou Jailed for Two Years for Identity Leak*, THE GUARDIAN (Oct 23, 2012), http://www.theguardian.com/world/2012/oct/23/cia-whistleblower-john-kiriakou-leak.

[175] *See* Scott Shane & Andrew Lehren, *Leaked Cables Offer Raw Look at U.S. Diplomacy*, N.Y. TIMES, Nov. 29, 2010, at A1.

[176] *See Collateral Murder*, COLLATERAL MURDER (April 5, 2010), http://www.collateralmurder.com.

had been injured in the initial volley.[177] Later parts of the video showed the same gunship crew in a separate engagement, again shooting a second missile as civilians are visibly climbing the rubble to aid injured survivors of a first missile they had shot.[178] The war logs showed that civilian casualties in Iraq were substantially higher than those publicly reported by the Pentagon,[179] and disclosed the existence of Task Force 373, a targeted assassination squad;[180] the logs also showed that U.S. forces knew of torture by the Iraqi security services and did not systematically protest or prevent these from continuing, even where the U.S. forces had the power to do so.[181] The embassy cables, by contrast, disclosed potential violations by the governments of other countries,[182] but not by the State Department or the U.S. government itself. As an initial matter, then, some of the materials Private Manning released would make her eligible for the defense. The scope and breadth of the disclosure, coupled with the fact that the majority of the documents did not disclose gross violations, suggest that, at least in its full version, the defense would be inappropriate. Had Manning selected only those materials that evidenced core wrongs and released those, the defense would have applied. Because the materials—although broad—included matters of special public concern, and because they were clearly intended to be made public, the Manning case presents a particularly crisp instance where the defense would better operate as a sentencing mitigation factor rather than a complete defense. Considering the sentences in the cases of Morison, Leibowitz, Kiriakou, and Kim (much less Franklin), Manning's thirty-five-year sentence was overwhelmingly excessive by comparison to any prior leak to the media.[183]

---

[177] *See Leaked U.S. Video Shows Deaths of Reuters' Iraqi Staffers*, REUTERS (Apr. 5, 2010, 8:39 PM), http://www.reuters.com/article/2010/04/06/us-iraq-usa-journalists-idUSTRE6344FW20100406.

[178] *See* Benkler, *supra* note 10, at 51.

[179] David Leigh, *Iraq War Logs Reveal 15,000 Previously Unlisted Civilian Deaths*, THE GUARDIAN (Oct. 22, 2010, 4:32 PM), http://www.theguardian.com/world/2010/oct/22/true-civilian-body-count-iraq.

[180] C. J. Chivers et al., *The Afghan Struggle: A Secret Archive*, N.Y. TIMES, July 26, 2010, at A1 ("Secret commando units like Task Force 373—a classified group of Army and Navy special operatives—work from a 'capture/kill list' of about 70 top insurgent commanders. These missions, which have been stepped up under the Obama administration, claim notable successes, but have sometimes gone wrong, killing civilians and stoking Afghan resentment.").

[181] David Leigh & Maggie O'Kane, *Iraq War Logs: US Turned Over Captives to Iraqi Torture Squads*, THE GUARDIAN (Oct. 24, 2010, 3:46 PM), http://www.theguardian.com/world/2010/oct/24/iraq-war-logs-us-iraqi-torture?guni=Article:in%20body%20link.

[182] *See U.S. Embassy Cables Interactive Database*, THE GUARDIAN (Nov. 28, 2010, 1:10 PM), http://www.theguardian.com/world/interactive/2010/nov/28/us-embassy-cables-wikileaks.

[183] *See* Andy Greenberg, *Sentenced to 35 Years, Bradley Manning Faces Longest-Ever U.S. Prison Term For Leak to Media*, FORBES (Aug. 21, 2013, 11:49 AM), http://www.forbes.

How would *Edward Snowden* fare under the public accountability defense? Most of Snowden's disclosures fall squarely within the defense, but some exposed details that likely impeded legitimate programs.

The disclosures included four distinct classes. First, programs known in public as "Bullrun" aimed at weakening cybersecurity for everyone, by undermining basic security standards-setting processes to simplify acquisition and analysis of bulk data.[184] Second, documents disclosed the existence and some details of several bulk collection programs under a range of legal authorities: Executive Order 12333 acquisition of data considered purely foreign,[185] FISA 702 collection of all data other than data completely within the United States or of individuals known to be U.S. persons,[186] and PATRIOT Act 215 collection of business records, in particular telephony metadata, wholly within the United States.[187] Third, disclosures offered substantial insight into the secret oversight process, in particular, the FISC process.[188] Fourth, documents disclosed intelligence practices that involve targeting specific computers, publicly known as Tailored Access Operations ("TAO").[189]

Disclosure of the telephony metadata collection program is the most defensible of the Snowden disclosures. As Judge Leon in *Klayman*,[190] the majority of the PCLOB,[191] and at least one member of the President's Review Group[192] stated, the telephony bulk collection program likely violates

---

com/sites/andygreenberg/2013/08/21/sentenced-to-35-years-bradley-manning-faces-longest-ever-u-s-prison-term-for-leak-to-media/.

[184] *See, e.g.*, Jeff Larson, *Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security*, ProPublica (Sept. 5, 2013, 3:08 PM), http://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption.

[185] *See, e.g.*, Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide*, *Snowden Documents Say*, Wash. Post (Oct. 30, 2013), http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

[186] *See, e.g.*, Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data From Nine U.S. Internet Companies in Broad Secret Program*, Wash. Post (June 6, 2013), http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?hpid=z1.

[187] *See, e.g.*, Glen Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, The Guardian (June 5, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[188] *See*, *e.g.*, Barton Gellman, *NSA Broke Privacy Rules Thousands of Times Per Year, Audit Finds*, Wash. Post (Aug. 15, 2013), http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html.

[189] *See*, *e.g.*, *Inside TAO: Documents Reveal Top NSA Hacking Unit*, Der Spiegel (Dec. 29, 2013, 9:18 AM), http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html.

[190] Klayman v. Obama, 957 F. Supp. 2d 1, 9 (D.D.C. 2013).

[191] *See* PCLOB Report, *supra* note 6.

[192] *See Continued Oversight of the Foreign Intelligence Surveillance Act: Hearing Before the S. Comm. on the Judiciary*, 113th Cong., Oct. 2, 2013 (Testimony of Keith Alexander, Director, National Security Agency); Geoffrey Stone, *The NSA's Telephone Metadata Program Is Unconstitutional*, Huffington Post (Jan. 9, 2014), http://www.huffingtonpost.com/geoffrey-r-stone/the-nsas-telephone-meta-d_b_4571523.html.

the Fourth Amendment. Moreover, a substantial number of members of Congress have joined efforts to amend the PATRIOT Act to prohibit this practice.[193] External objective evidence that the exposed conduct was wrongful is readily established, and the magnitude and ubiquity of the response strongly support availability of the defense in this case.[194]

Section 702 data collection differs primarily in that it refers to collection of communications predominately external to the United States and therefore not covered by the Fourth Amendment.[195] Nonetheless, these collection efforts sweep in significant numbers of protected communications, as well as millions of communications of innocent non-U.S. citizens, who are protected by human rights, if not American civil rights.[196] There should therefore be a presumption of reasonableness for their disclosure. Unlike the telephony metadata program, the PRG report suggests that 702 data did play a role in preventing terrorism, and exposure may lead to reduction of the program's capabilities.[197] While this harm exists, it appears to be longer-term reduction in efficacy, rather than articulable, immediate operational harm that would clearly outweigh the benefits, given the significance of the disclosure. Even if the 702 collection is legal, it is the kind of decision, affecting Americans and innocent civilians in other nations, that merits public debate and a democratic decision. The 12333 programs are fully foreign but fall under the broader sense of systemic failure. Most famously the "Muscular" program involved hacking foreign-located data centers of Google and Yahoo! and obtaining communications, including communications of U.S. users.[198] The harm of disclosure, as with 702 programs, will likely require changed procedures to assure protection of rights, which is not a cognizable harm, and longer-term adaptation of techniques to recover lost effectiveness. While certainly relevant, such harms are too remote and gradual to outweigh the benefit of exposing a program with such far-reaching implications for rights at home and abroad.

Exposure of court orders and the limitations of the oversight system plainly fall at the core of proper disclosure. The documents exposed the limitations of the delegated oversight system introduced in the post-Watergate era. Myriad legislative reforms and executive branch proposals confirm

---

[193] *See* Dan Roberts, *Patriot Act Author Prepares Bill to Put NSA Bulk Collection 'Out of Business'*, THE GUARDIAN (Oct. 10, 2013, 3:57 PM), http://www.theguardian.com/world/2013/oct/10/nsa-surveillance-patriot-act-author-bill.

[194] *See Snowden's Disclosure Prompts Global Debate Over Privacy Versus National Security*, PRI'S THE WORLD (July 18, 2013, 6:45 AM), http://www.pri.org/stories/2013-07-18/snowdens-disclosure-prompts-global-debate-over-privacy-versus-national-security.

[195] Foreign Intelligence Surveillance Act of 1978 Amendments of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (2008).

[196] *See* Elizabeth Goitein, *The NSA's Backdoor Search Loophole*, BOS. REV. (Nov. 14, 2013), http://www.bostonreview.net/blog/elizabeth-goitein-nsa-backdoor-search-loophole-freedom-act.

[197] *See* PRG REPORT, *supra* note 5.

[198] *See* Gellman & Soltani, *supra* note 185.

that the leaked documents exposed significant flaws in judicial review of NSA surveillance, flaws that the American public through its representatives seeks to correct. These facts create a presumption of reasonableness of disclosure.

The Bullrun disclosures are the least widely understood, and represent the category of violations of systemic failure, not illegality. The NSA undermined standards-setting and product-design processes, intervening in market and non-profit activities to achieve an outcome of profound public consequence.[199] Effectively, the NSA made a decision that its intelligence function was so important that it was worth making the Internet less safe for everyone, from everyone, in order to make it less impregnable to NSA spying.[200] Like a decision to ground all air traffic to avoid terrorism, that decision cannot be made without public debate. It goes to the heart of how a society defines security. The most explicit acceptance of this critique has been the PRG report. The report recommended that no part of the U.S. government should undermine encryption standards or subvert generally available commercial software,[201] and more fundamentally, recommended a reorganization of the NSA that would separate parts of the agency responsible for communications security, which would form a separate unit in the Pentagon, from signals intelligence, and both would be separate from the United States Cyber Command.[202] These organizational changes appear crafted to avoid repetition of the kind of myopia represented by Bullrun, in which signals intelligence dominated communications security, cybersecurity, and both market and social innovation processes. The fact that the independent review group found the program to be one that required substantial change is the kind of evidence that can show that disclosure was reasonable when made.

Unless one completely abandons espionage as a tool, however, TAO represents the kind of operation that most closely resembles individualized search; has the least negative impact on democracy, individual dignity, or autonomy on a societal level; and is expensive enough to increase our confidence that it will be aimed at legitimate targets. Disclosure of TAO is therefore least likely to expose abuse or violations of law or systemic failure, while also being most likely to cause operational harms. The question it poses for us is whether the harm caused by these disclosures to these programs is large enough to deny Snowden the defense, given the significance of the other disclosures.

---

[199] *See* James Ball et al., *Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security*, THE GUARDIAN (Sept. 5, 2013), http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

[200] *See Secret Documents Reveal N.S.A. Campaign Against Encryption*, N.Y. TIMES (Sept. 5, 2013), http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html.

[201] *See* PRG REPORT, *supra* note 5, at 36 (Recommendation 29).

[202] *See id.* at 34 (Recommendations 23–25).

To summarize, disclosure of the telephony metadata program and the limitations of the FISC is clearly protected. Disclosures of Bullrun, 702 collection, and Muscular also should enjoy the defense. Disclosure of TAO alone, however, would likely not have properly come under the defense. Given the breadth and depth of public concern over the former aspects of the program and the extensive, multi-branch condemnation of so many aspects of the disclosed programs and oversight system, Snowden presents a case where the overall significance of the disclosures is not only reasonable, but also overcomes claims of harm, once the harms claimed are properly reduced to losses in articulable operational terms, rather than general necessity to recalibrate surveillance measures. The defense would be rendered meaningless, however, if prosecutors were free to cherry pick the least defensible disclosures, charge offenses based on them alone, and limit introduction of the entirety of the disclosure. To prevent prosecutors from manipulating cases to nullify the defense, courts must permit defendants to introduce other public disclosures that arose from a common set of operative facts that led to the disclosure of the charged documents as relevant to the defense. Courts would then have to assess the relative weight of the disclosures that would be covered by the defense and those that would not. The critical point is that courts cannot exclude such disclosures from the record as irrelevant simply because they were not included in the charged documents. This is particularly important in bulk disclosure cases of the type made more feasible by digitized information, where the use of a reliable intermediary for mitigation is critical, and where admixture of information disclosing violations of law or systemic failure with information that does not include such disclosures will be the rule, rather than the exception. In Snowden's case, the preponderance of the disclosures were within the defense, and the defense should not be susceptible to prosecutorial circumvention by charging only the subset of documents that would not be eligible for the defense by themselves.

V. Conclusion

The past decade has seen a dramatic increase in criminal prosecutions to deter national security leakers and whistleblowers. The technical ease of leaking large dumps of data offers an explanation for the form that two of the major leak cases took, but the driver of increased leaks appears to be individual conscience resisting perceived abuse of power under the post-9/11 state of emergency. As was true of the burst of national security whistleblowers in the 1970s, the response of the national security establishment to the state of emergency has led to conflicts between system behavior and the individual conscience of insiders. This tension destabilized the status quo that prevailed since the mid-1970s, where leaks were generally not prosecuted, or, in an extremely rare prosecution, punished at levels well below legal maxima. The new disruption has led to a significant heightening

of risk of criminal prosecution, with its attendant risks of suppressing genuinely valuable exposure and public accountability.

The national security establishment is not an abstract system of values. It is a set of organizations and institutions subject to the standard limitations that typify all organizations and collective sense-making processes. While the special risks associated with breaching the secrecy of national security agencies are well recognized, it is important to understand that precisely the critical role that these bureaucracies play also makes oversight, accountability, and error correction indispensable. The post-Watergate delegated oversight model proved adequate for a long period, but buckled under the post-9/11 state of emergency mindset. Whether it is in the macro decision to launch the Iraq War on false premises, the narrower but morally abhorrent decision to adopt torture, or the excesses of pervasive surveillance, the national security establishment has made systematic and significant operational and normative errors, and has successfully coopted or subverted its institutionalized oversight system to avoid accountability and error correction. The study of the national security establishment as a system should also undermine our confidence in current efforts to reform the bulk surveillance problem that has been the subject of our case analysis here. Heavy reliance on minimization rules and a somewhat improved FISC process ignores the systematic imbalance between the executive elements of the national security establishment and the FISC, the technical complexity of the bulk surveillance that makes judicial oversight vastly more difficult than in the normal case of warrants and subpoenas, and the pressure and systemic error dynamics that would, of necessity, pervade minimization procedures and their judicial oversight.

In the face of repeated system failure, individual conscience and the refusal of individuals to play along—coupled with public pressure that comes from disclosure—require that we recreate the space for safe unauthorized disclosures of matters of grave public concern. A first step will be introduction of a public accountability defense in criminal law to protect sources who inform the public of significant violations of human and civil rights, major matters of war and peace, and other instances of substantial error, incompetence, and malfeasance. A review of the major cases arising from disclosures of national security secrets in the past fifty years suggests that adopting such a defense would be a less radical step than appears on its face.

A public accountability criminal defense would be a first step only. As Jesselyn Radack's case illustrates, the Executive can use administrative sanctions to deter whistleblowers without recourse to criminal prosecution, and as Drake's case illustrates, it can use aggressive prosecution to impose punishment by process even if the defense ultimately prevails. To combat these, it will be important to complement the criminal defense with a private cause of action for abusive process, shaped along similar contours to those outlined here for the criminal defense. Moreover, given the critical role that

whistleblowers play, the private cause of action should be coupled with a modification of the qualified immunity of prosecutors and investigators. In particular, as objective facts unfold that tend to support the availability of the defense, such as judicial or legislative corrective action, these should be incorporated into a determination of whether continuation of an investigation or prosecution reasonably open continues to be so, or has become abusive.

Disclosure is no panacea. The politics of national security tend to lead majorities to be overly lenient even when disclosures show national security illegality or failure.[203] Accountability in the sense of people responsible for the illegality or systemic failure being prosecuted or losing their jobs, as appropriate, a reliable level of public discourse that would actually lead the public to pay attention to systemic failure, and a political system that translates such public opinion into action are all critical for our open, democratic society to utilize its greatest power to continuously learn about our failures and improve on them. But information about illegality and systemic failure is a critical element in the longer-term struggle to resist the inevitable risks associated with having a large, complex, and powerful national security system. A powerful legislative push against the increasingly aggressive prosecutions of the past decade, such a public accountability defense would restore something close to the pre-9/11 equilibrium in practice and, importantly, would do so by institutionalizing a basic skepticism about the extent to which the national security establishment can be trusted to avoid the humdrum failures that all large, complex organizations suffer. Recognizing our limitations is the beginning, even if only the beginning, of addressing them.

[203] *See id.* at 34 (Recommendations 23–25).