Leaking and Legitimacy

Margaret B. Kwoka[*]

Julian Assange, Chelsea Manning, and Edward Snowden have captured the world's attention in recent years by leaking massive quantities of secret government information. In each case, critics have made much of the fact that the leaks were in violation of government secrecy laws, while supporters have drawn parallels with whistleblower leaks, including the most famous and now widely acclaimed leak in United States history, Daniel Ellsberg's leak of the Pentagon Papers.

This Article makes two important contributions to this debate. First, it defines this type of leak — which it labels a "deluge leak" — as a new category. Unlike whistleblower leaks, which expose targeted government policies about which a knowledgeable leaker is concerned (in Ellsberg's case, military involvement in Vietnam), deluge leaks are a broad response to excessive government secrecy insofar as they reveal a vast array of records about which the leaker knows relatively little.

Second, departing from traditional criminal law and First Amendment analyses of these leaks, this Article examines deluge leaks through the lens of the social science literature on legitimacy. That literature establishes that a perceived lack of procedural justice is a key reason that people break the law. Currently, deficient procedural justice characterizes the suite of laws that governs the public's right to access government information, including the Freedom of Information Act, the classification system, and whistleblower protections. This lack of legitimacy is an important motivation for recent deluge leaks, as the leakers' own actions and words demonstrate. The Article concludes by arguing, counter-intuitively, that improving transparency laws would better protect national security secrets.

 Assistant Professor, University of Denver Sturm College of Law. Many thanks to Kim Chanbonpin, Alan Chen, Roberto Corrada, Ian Farrell, César Cuauhtémoc García Hernández, Rashmi Goel, Ernesto Hernández-López, Beto Juárez, Sam Kamin, Nancy Leong, Suzette Malveaux, Justin Pidot, Nantiya Ruan, and the participants in the 2014 Midwestern People of Color Legal Scholarship Annual Meeting for invaluable feedback on earlier drafts, and to Caroline Marfitano for excellent research assistance.

TABLE OF CONTENTS

INTRODUCTION

Leaked information has formed the basis of journalism, public critique, and accountability for centuries.[1] Many view leaks as both inevitable and as largely beneficial in keeping the government honest and informing the public.[2] C.J. Cregg, the press secretary character from the hit political drama *The West Wing*, described this sentiment: "There is no group of people this large in the world that can keep a secret. I find it comforting. It's how I know for sure the government isn't covering up aliens in New Mexico."[3] In fact, there is powerful evidence that leaks form the basis of or contribute to a substantial amount of mainstream news media reporting.[4] On the other hand, the potential harm that may result from leaked information is of dire concern to politicians and the public alike.[5]

Recent unauthorized disclosures of national security information have brought leaking into the forefront of public debate.[6] These events have centered around Julian Assange, the founder of anonymous-leak-facilitating website WikiLeaks,[7] Chelsea Manning, an army intelligence analyst who leaked hundreds of thousands of defense and

---

[1] *See* David E. Pozen, *The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information*, 127 HARV. L. REV. 512, 528 (2013) (documenting the scope of leaking practices).

[2] *See, e.g.*, STEPHEN HESS, THE GOVERNMENT/PRESS CONNECTION: PRESS OFFICERS AND THEIR OFFICES 91 (1984) (quoting political scientist Richard E. Neustadt as saying that "leaks play . . . a vital role in the functioning of our democracy," and historian Bruce Catton as saying that "[o]ur particular form of government wouldn't work without [leaks]").

[3] *The West Wing: Bad Moon Rising*, at 35:00 (NBC television broadcast Apr. 25, 2001).

[4] *See* JACK GOLDSMITH, POWER AND CONSTRAINT: THE ACCOUNTABLE PRESIDENCY AFTER 9/11, at 68-69 (2012) (reporting "hundreds of stories" in the *New York Times* and the *Washington Post* after 9/11 that self-reported disclosures of classified information and many more that appeared to contain classified information without acknowledging as much).

[5] *See* Pozen, *supra* note 1, at 514 (citing evidence that the public is concerned about leaking). For example, President Richard Nixon's secret taping system caught his first reaction to Daniel Ellsberg's release of what is now known as the Pentagon Papers, revealing his statement: "Now, I'd just start right at the top and fire some people. I mean, whoever — whatever department it came out of, I'd fire the top guy." *Richard M. Nixon Presidential Recordings: Nixon Conversation 005-050*, MILLER CTR., http://millercenter.org/presidentialrecordings/rmn-005-050 (last visited Mar. 6, 2014); *see also* GABRIEL SCHOENFELD, NECESSARY SECRETS: NATIONAL SECURITY, THE MEDIA, AND THE RULE OF LAW 22-26 (2010).

[6] Pozen, *supra* note 1, at 514.

[7] DAVID LEIGH & LUKE HARDING, WIKILEAKS: INSIDE JULIAN ASSANGE'S WAR ON SECRECY 43-63 (2011).

diplomatic records,[8] and Edward Snowden, a contractor who leaked thousands of records regarding the National Security Agency's surveillance activities.[9] The actions of Assange, Manning, and Snowden have provoked a complicated response. Many champion these actors as transparency heroes, civil liberties activists, and even martyrs.[10] Others have accused them of being reckless renegades, traitors, and even spies.[11]

While these leaks are often compared to perhaps the most famous leak in American history — Daniel Ellsberg's leak of documents about the history of the United States's involvement in Vietnam, now known as the Pentagon Papers — this Article contends that the recent national security leaks are different in significant ways and thus represent a new type of leak. Ellsberg was a knowledgeable, high-level official who leaked a targeted set of records he believed demonstrated illegal and immoral government behavior. In a sense, the Pentagon Papers leak was a classic whistleblower leak in which an insider publicly announces secret government conduct believed to be illegal or immoral.[12] The recent leaks include this type of whistleblowing, but also go much further. Recent leaks encompass vast quantities of records that the leaker likely knows nothing about, if he or she has even read them. The common thread of leaked records in recent high profile cases is simply that the leaker has access to them.[13] Moreover, these leakers go beyond protesting a single government policy as whistleblowers do; instead, they also describe themselves as

[8] Mark Fenster, *Disclosure's Effects: WikiLeaks and Transparency*, 97 IOWA L. REV. 753, 762 (2012) [hereinafter *Disclosure's Effects*]. Chelsea Manning was formerly known as Bradley Manning. *Kansas: Manning Wins Right to Change Name*, N.Y. TIMES, Apr. 24, 2014, at A18.

[9] GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE 90 (2014).

[10] *See* Mary-Rose Papandrea, *Leaker Traitor Whistleblower Spy: National Security Leaks and the First Amendment*, 94 B.U. L. REV. 449, 482-90 (2014) (documenting the various rhetorical labeling that has attached to recent high profile leakers as a sort of "name game").

[11] For a more detailed account of the reactions to these recent leaks, see *infra* Part II.B.1.

[12] *See* Patrick McCurdy, *From the Pentagon Papers to Cablegate: How the Network Society Has Changed Leaking*, *in* BEYOND WIKILEAKS: IMPLICATIONS FOR THE FUTURE OF COMMUNICATIONS, JOURNALISM AND SOCIETY 123, 126 (Benedetta Brevini et al. eds., 2013).

[13] *See* Roy Peled, *WikiLeaks as a Transparency Hard-Case*, 97 IOWA L. REV. BULL. 64, 69 (2012).

transparency advocates.[14] This Article labels this type of leak the "deluge leak."[15]

Deluge leaks are likely to be on the rise.[16] As government information systems become more centralized and more digitized, more low-level government officials and contractors have access to broad swaths of government information, including national security related records.[17] Technology has also eased the process of leaking. Long gone are Ellsburg's dark nights with photocopy machines; hard copy records have been replaced by easily stored, saved, replicated, and disseminated digital records. Furthermore, global web publishers such as WikiLeaks offer strong anonymity protections, making deluge leaks potentially less costly to leakers.[18] While the impetus to deluge leak may have long existed, the technology only recently made it possible. In short, the deluge leak is just making its debut.

The effects of the recent deluge leaks are difficult to evaluate, even well after they have occurred. These types of leaks, however, generally pose new kinds of potential dangers, even if they have not yet been realized. The increased risk arises from the various ways in which it is inherently harder for leakers and publishers to minimize the harms of deluge leaks while maximizing the public benefit.[19]

Meanwhile, the literature on leaking has largely focused on potential criminal penalties for leakers and publishers of leaked information, as well as the role of the First Amendment's protections for the press.[20]

---

[14] Public Statement, Chelsea E. Manning, Concerns Regarding 2013 Sean MacBride Peace Award (Oct. 7, 2013), *available at* http://www.theguardian.com/world/interactive/2013/oct/09/chelsea-manning-statement-full-document [hereinafter Chelsea Manning Public Statement]; *see also* ANDY GREENBERG, THIS MACHINE KILLS SECRETS: HOW WIKILEAKERS, CYPHERPUNKS, AND HACKTIVISTS AIM TO FREE THE WORLD'S INFORMATION 112 (2012).

[15] For a detailed analysis of the difference between deluge leaks and other types of leaks, see *infra* Part I.C.

[16] For a description of the factors contributing to an increase in deluge leaks, see *infra* Part I.A.

[17] *See* McCurdy, *supra* note 12, at 134.

[18] *See About*, WIKILEAKS (May 7, 2011), https://wikileaks.org/About.html (describing the commitment to anonymity).

[19] For a detailed discussion of the reasons for concern about deluge leaks, see *infra* Part I.B.

[20] *See, e.g.*, Heidi Kitrosser, *Free Speech Aboard the Leaky Ship of State: Calibrating First Amendment Protections for Leakers of Classified Information*, 6 J. NAT'L SECURITY L. & POL'Y 409 (2013) (arguing that government employees who leak classified records should receive some First Amendment protections); Papandrea, *supra* note 10 (arguing that leakers themselves enjoy substantial First Amendment protections, in addition to the press); Nawi Ukabiala, *Wikilaw: Securing the Leaks in the Application of*

Some of the work concerning the criminalization of leaking has focused on the difficulty inherent in defining the prescribed conduct. For instance, one scholar has explained that prescriptive line drawing to maximize protection of national security interests, on the one hand, and government transparency, on the other, has proven historically illusive.[21] In fact, another scholar has compiled substantial evidence that no one — in or outside the government — is truly able to predict with reasonable accuracy whether releasing records will have a particular harmful effect.[22] Nonetheless, such predictions serve as the basis for the laws defining what information must be kept secret.[23] Other recent work has focused on the problems of criminal enforcement. The government, one commentator argued, has an incentive not to vigorously enforce criminal prohibitions on leaking because it benefits more from leaks than it is hurt.[24] A permissive approach to unauthorized leaking allows the government to purposefully and strategically "leak" information with credibility, and serves to reassure the public that important governmental activities will come to light.[25] Even when the government wants to enforce criminal prohibitions against leaking, another scholar has documented various impediments to enforcing criminal penalties against new types of online media that are publishing leaks, such as WikiLeaks.[26] Thus,

First Amendment Jurisprudence to Wikileaks, 7 FED. CTS. L. REV. 209 (2013) (proposing a narrowly construed amendment to the Espionage Act that would impose criminal penalties on publishers of classified information where national security harm can be demonstrated); Candice M. Kines, Note, *Aiding the Enemy or Promoting Democracy? Defining the Rights of Journalists and Whistleblowers to Disclose National Security Information*, 116 W. VA. L. REV. 735 (2013) (arguing that criminal punishment for government leaks should be tied to harms from release, but should exempt good faith whistleblowing, and should reach the press as well as the leaker); Pamela Takefman, Note, *Curbing Overzealous Prosecution of the Espionage Act: Thomas Andrews Drake and the Case for Judicial Intervention at Sentencing*, 35 CARDOZO L. REV. 897 (2013) (arguing that prosecution of government workers under the Espionage Act should be kept in check by judges use of discretion at sentencing).

[21] *See* Pozen, *supra* note 1, at 622 (suggesting that leaks indicate the President is not able to control the executive branch with ex ante laws).

[22] *See generally* Fenster, *Disclosure's Effects*, *supra* note 8 (arguing that the belief that the effects of leaks are predictable relies on a mistaken understanding).

[23] *See generally id.* at 757 ("Information-disclosure law and the theory that supports it rely upon the ability to predict and ascertain disclosure's effects.").

[24] *See* Pozen, *supra* note 1, at 544-86 (arguing that laws are not enforced because leaks create permissive cultures that officials want to exploit).

[25] *See id.* at 517-18.

[26] *See generally* Patricia L. Bellia, *WikiLeaks and the Institutional Framework for National Security Disclosures*, 121 YALE L.J. 1448 (2012) (documenting limits on prosecutions stemming from First Amendment protections, laws concerning extra-

many structural barriers limit the government's willingness and ability to stop leaking. These important contributions highlight the inherent difficulty of creating an ideal legal framework for punishing breaches of secrecy.

Even if we could construct an ideal punishment regime, however, there is good reason to conclude that criminal penalties are unlikely to adequately deter deluge leaks. Technology is evolving such that tracing leaks may become next to impossible as anonymity tools become stronger and more readily available. In addition, criminal enforcement in this area is all but absent and enforcement-based incentives to comply with the law are in any event often ineffective. Furthermore, punishment after a leak has occurred does not prevent any harm that comes from the leak; as the saying goes, one cannot unscramble an egg.[27] Another approach to addressing the dangers of deluge leaks is necessary.

This Article is the first to conceptualize deluge leaks as a distinct phenomenon and to document how they are tied to the failures of government transparency. In so doing, it employs the work of sociologists who have demonstrated that one significant explanatory factor in decisions to obey the law is an individual's view of the legitimacy of the legal authorities.[28] Legitimacy, in turn, is primarily driven by perceptions of the fairness of the procedures used by legal authorities, known as procedural justice.[29] This Article contends that a lack of legitimacy pervades U.S. government transparency laws, and that this legitimacy deficit contributes to the risk of deluge leaks. In fact, our freedom of information, classification, and whistleblower laws are all plagued by procedural shortcomings that contribute to a perception that the laws are administered unfairly. An alternative approach to curbing future deluge leaks thus emerges: reforming our transparency system to achieve public belief in its legitimacy. In so doing, this Article rejects the premise that national security and government transparency are inherently at odds by demonstrating how greater transparency may further our security objectives, too.

To this end, Part I uses a typology of leaks to demonstrate how the recent high-profile leaks are different in kind from past leaks, and defines the category of deluge leaks. Part II argues that deluge leaks are likely to be on the rise, that they pose heightened risks to legitimate needs for secrecy, and that criminal penalties for leakers or

territoriality, and statutory construction considerations).

[27] For a more detailed explanation of the limits on criminalization, see *infra* Part II.C.

[28] *See* TOM R. TYLER, WHY PEOPLE OBEY THE LAW 112 (2006).

[29] *See id.*

publishers of leaked information are unlikely to be an effective deterrent against deluge leaks. Alternative interventions with respect to deluge leaks are thus imperative. Part III documents how the sociological literature on procedural justice and legitimacy can contribute to our understanding of would-be deluge leakers' decisions to break the law by revealing classified information. Part IV argues that in each of the three legal regimes governing disclosure of national security information, legitimacy deficits pervade the procedures used to implement the laws. Most notably, decision-makers lack apparent (or actual) neutrality and stakeholders are denied full participation in the process. Moreover, when processes are opaque, the outcomes are so skewed as to suggest to observers that they are the product of procedural unfairness. Part V utilizes the best available evidence — the recent deluge leakers' actions and public statements — to establish that these leakers responded, at least in part, to the legitimacy deficit. They view their acts as political protests against excessive government secrecy without effective procedural remedies. The Article concludes by suggesting reforms that further both national security and government transparency.

I. THE NEW DELUGE LEAKS

Leaks are as old as secrets. Even though identifying specific information as originating from a leak is often difficult because it is intertwined with material from other sources, studies demonstrate that leaked material does make its way into the press on a regular basis.[30] Not all leaks, however, are created equal. Leaks come in varying sizes and shapes, and the effects of leaks may depend in large part on subtle differences. This Part will identify various types of common leaks and will demonstrate the emergence of a new type of leak — the deluge leak — characterized by lower-level government officials without policy-making authority leaking massive quantities of information on a wide range of subject matter largely out of a belief that government keeps too many secrets.

A. A Typology of Leaks

The word "leak" classically refers to the anonymous unauthorized disclosure of confidential information by a government insider to a

[30] Pozen, *supra* note 1, at 528-29 (collecting data on leaks from a variety of sources, all of which conclude that leaking is very common).

member of the media.[31] Leaks can be distinguished from authorized disclosures designed to further government interests, often referred to as "plants."[32] Merely distinguishing between leaks and plants, however, still lumps together a wide variety of activity under the label "leaking" without accounting for important differences between various kinds of leaking activities. In fact, leaks vary principally by the motivation of the leaker, the identity of the leaker, and the scope of leaked material.

Leaks may be motivated by a variety of concerns. Stephen Hess, a Brookings Institute researcher focusing on governance, has categorized the principle motivations behind leaks: a desire for self-importance, an attempt to curry favor with a reporter, an effort to have some effect on a particular plan or policy, a plot for revenge by embarrassing others, a test of the response of some constituency, or a means of revealing a perceived abuse.[33] This last kind of leak, also known as the whistleblower leak, is the kind of leak most often imagined in the public view.[34]

Leaks can also be categorized by the level of government from which they originate. Past leak originators have ranged from low-level bureaucrats to high-level, senior policymaking officials, and even the President's own closest advisors.[35] In fact, most leaks come from higher-level positions. As a saying commonly heard in discussions of leaking goes, "the ship of the state is the only vessel that leaks from the top."[36] Indeed, Hess, after spending a full year observing press office operations in four government agencies and the White House, observed that leaking is not "often practiced in the lower civil service."[37]

Professor David E. Pozen has created a further division between types of leaks, those he calls "general" versus "specific" leaks. He defines "specific" leaks as conveying "a limited amount of content about a discrete matter," whereas "general" leaks "disclose vast swaths

---

[31] *Id.* at 521.

[32] HESS, *supra* note 2, at 75.

[33] *Id.* at 77.

[34] This common image likely stems from the most famous historical leaker, Daniel Ellsberg, who leaked the Pentagon Papers. For further detail on the incident, see *infra* notes 70–74 and accompanying text.

[35] Pozen, *supra* note 1, at 529-30.

[36] David E. Rosenbaum, *First a Leak, Then a Predictable Pattern*, N.Y. TIMES, Oct. 3, 2003, at A16 (attributing this quote to journalist James Reston).

[37] HESS, *supra* note 2, at 75.

of information more or less indiscriminately."[38] He also notes that general leaks are far more likely to come from lower-level career bureaucrats because senior-level officials "do not tend to see themselves as whistleblowers on a mission to expose abuse or as dissidents on a large scale."[39]

Classifying any particular leak against these three metrics may leave some ambiguity. After all, many people have more than one motivation to act. A leak may originate from a mid-level official with limited policymaking authority, or the scope of the leak may be larger than one issue, but smaller than the universe of records to which the leaker has access. Though these factors operate as more of a continuum in practice, they are nonetheless useful in identifying commonalities between leaks.

B. Recent National Security Leaks

Julian Assange began as a gifted hacker in his native Australia.[40] In 1996, at a relatively young age, he was caught by the Australian police and pleaded guilty to various hacking crimes, but was not sentenced to any jail time because the judge concluded that Assange's actions were not malicious or for personal gain.[41] Only three years later, Assange came up with the idea of a leakers' website, and he registered the domain name wikileaks.org.[42]

Nonetheless, the site remained dormant until Assange launched the project in 2006 with the idea that it would serve as a secure and anonymous publisher of leaked information. In December of that year, Assange facilitated the leak of the first WikiLeaks document, a little noticed "secret decision" by a Somali rebel leader.[43] In 2007, WikiLeaks made more of a splash with the release of a report detailing the corruption of the former President of Kenya,[44] but most of WikiLeaks's early leaking activities made little news.[45] WikiLeaks briefly gained attention when it served as a gag-proof publishing site

[38] Pozen, *supra* note 1, at 533.

[39] *Id.* at 534. Pozen also notes that "[g]eneral leaks are the province of the radically disaffected and the subversive," whereas "[t]op government brass, socialized into and successful in the Washington power culture, are unlikely to be either." *Id.*

[40] LEIGH & HARDING, *supra* note 7, at 33.

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

[42] *Id.* at 46.

[43] *Id.* at 55-56.

[44] *Id.* at 57-58.

[45] *Id.* at 60 ("[Assange] seemed unable to accept that sometimes his leaks might just not be that interesting . . . .").

for source documents when mainstream media were subject to lawsuits.[46] For instance, when Barclay's Bank obtained an order requiring *The Guardian* to take down leaked records revealing a tax-avoidance scandal, WikiLeaks republished the records immediately, rendering the gag order futile.[47]

WikiLeaks's major entry into the public eye began when it served as the vehicle for a series of disclosures now known to have originated with leaker Chelsea Manning, a soldier in the U.S. Army who was then serving as an intelligence analyst.[48] In April 2010, WikiLeaks released a video it entitled "Collateral Murder," which depicted a U.S. Army Apache helicopter attack in Baghdad in which two employees of the Reuters news company were killed on the ground.[49] The video showed that the military's claim that insurgents had been firing on the helicopter was false, and revealed soldiers' disturbingly callous statements, including responding to having wounded children by saying "Well it's [the parents'] fault for bringing their kids into a battle."[50]

The Collateral Murder video was, it turns out, only the beginning. In July 2010, WikiLeaks released thousands of documents about the war in Afghanistan; in October 2010, hundreds of thousands of documents about the Iraq war; from late 2010 to early 2011, hundreds of thousands of diplomatic cables between the U.S. State Department and U.S. embassies around the world; and in April 2011, hundreds of documents about individuals held at Guantanamo Bay.[51] All of these releases have now been attributed to Chelsea Manning, who was convicted in military court for leaking the records and sentenced to thirty-five years' imprisonment.[52]

For a variety of reasons, WikiLeaks's future remains uncertain,[53] but massive and controversial national security leaks have not abated, with

---

[46] *Id.* at 62-63.

[47] *Id.* at 63.

[48] Fenster, *Disclosure's Effects*, *supra* note 8, at 762.

[49] sunshinepress, *Collateral Murder - Wikileaks - Iraq*, (Apr. 3, 2010), https://www.youtube.com/watch?v=5rXPrfnU3G0; GREENBERG, *supra* note 14, at 28-29; Fenster, *Disclosure's Effects*, *supra* 8, at 762.

[50] GREENBERG, *supra* note 14, at 29.

[51] GARY ROSS, WHO WATCHES THE WATCHMEN?: THE CONFLICT BETWEEN NATIONAL SECURITY AND FREEDOM OF THE PRESS, at xxix (2011); Fenster, *Disclosure's Effects*, *supra* note 8, at 762-63.

[52] Charlie Savage & Emmarie Huetteman, *Manning Sentenced to 35 Years for a Pivotal Leak of U.S. Files*, NY. TIMES, Aug. 21, 2013, at A1.

[53] For a long time, major financial institutions blocked donations to WikiLeaks, effectively cutting off its funding, although some have now been lifted. *See MasterCard Breaks Ranks in WikiLeaks Blockade*, WIKILEAKS (July 3, 2013), https://wikileaks.org/

Edward Snowden now filling the spotlight. Snowden held an early-career position with the Central Intelligence Agency ("CIA") stationed in Geneva, Switzerland, and later worked as a contractor for the National Security Agency ("NSA"), first through Dell Computers in Japan and Hawaii, and then Booz Allen Hamilton in Hawaii.[54] In the last position, he worked as an infrastructure analyst, giving him wide-ranging access to classified government documents,[55] volumes of which he eventually leaked to the press.

On June 5, 2013, the press reported that the Foreign Surveillance Intelligence Court authorized the NSA to collect the communication records of millions of U.S. citizens who are Verizon customers.[56] On June 6, stories ran revealing the existence of the PRISM program, which gave the NSA direct access to the servers of many large tech companies like Apple, Google, and Microsoft.[57] Articles documenting leaked national security information continued,[58] and by June 9, Snowden revealed himself as the source of the leaks.[59] Since that time,

MasterCard-breaks-ranks-in.html. In addition, Julian Assange is currently residing in the Ecuadorian embassy in London, where he was granted asylum to avoid extradition to Sweden to face charges of sex offenses. *Julian Assange: Ecuador Will Continue to Grant Asylum*, BBC (June 17, 2013, 7:48 AM), http://www.bbc.com/news/uk-22937293.

[54] MICHAEL GURNOW, THE EDWARD SNOWDEN AFFAIR: EXPOSING THE POLITICS AND MEDIA BEHIND THE NSA SCANDAL 9, 15, 20 (2014).

[55] *Id.* at 21.

[56] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 5, 2013, 6:05 AM EDT), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[57] Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 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; Glenn Greenwald, *NSA Prism Program Taps in to User Data of Apple, Google, and Others*, GUARDIAN (June 6, 2013, 3:23 PM EDT), http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

[58] On June 7, 2013, media reported that President Barack Obama ordered top officials to list potential overseas targets for U.S. cyberattacks, and on June 8, 2013, newspapers revealed an NSA data-mining tool called Boundless Informant that collects metadata from computer networks and harvested almost 3 billion pieces of domestic intelligence in a single month. *See* Glenn Greenwald & Ewen MacAskill, *Boundless Informant: The NSA's Secret Tool to Track Global Surveillance Data*, GUARDIAN (June 8, 2013, 9:00 AM EDT), http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining; Glenn Greenwald & Ewen MacAskill, *Obama Orders US to Draw up Overseas Target List for Cyber-Attacks*, GUARDIAN (June 7, 2013, 3:06 PM EDT), http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas.

[59] Glenn Greenwald, Ewen MacAskill & Laura Poitras, *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, GUARDIAN (June 9, 2013, 9:00

while Snowden has been granted temporary asylum in Russia, news reports based on Snowden's leaked documents have continued to shock the public about the extent of NSA surveillance activities, including those that affect U.S. citizens.[60]

AM EDT), http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

[60] *See, e.g.*, James Ball, *NSA Collects Millions of Text Messages Daily in 'Untargeted Global Sweep*,' GUARDIAN (Jan. 16, 2014, 1:55 PM EST), http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep (reporting that the NSA collects almost 200 million text messages a day around the world); James Ball et al., *Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security*, GUARDIAN (Sept. 6, 2013, 6:24 AM EDT), http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security (revealing that the NSA and British intelligence have broken the codes to read large amount of encrypted internet traffic); Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-mail Address Books Globally*, WASH. POST (Oct. 14, 2013), http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html (reporting that the NSA is collecting hundreds of millions of contact lists from personal email accounts including from U.S. citizens); 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 (reporting that the NSA broke into foreign data centers owned by US companies without their consent); Barton Gellman & Ashkan Soltani, *NSA Surveillance Program Reaches 'Into the Past' to Retrieve, Replay Phone Calls*, WASH. POST (Mar. 18, 2014), http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html (reporting that the NSA has a system to record all of a foreign country's phone calls and store the data for up to thirty days for review); Barton Gellman & Ashkan Soltani, *NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show*, WASH. POST (Dec. 4, 2013), http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html (revealing an NSA program to collect data on the locations of at least hundreds of millions of cellphones around the world); Ewen MacAskill et al., *GCHQ Intercepted Foreign Politicians' Communications at G20 Summits*, GUARDIAN (June 17, 2013, 5:45 AM EDT), http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits (documenting British and NSA cooperation to spy on G20 leaders at the 2009 meetings in the U.K.); Ewen MacAskill & Julian Borger, *New NSA Leaks Show How US is Bugging its European Allies*, GUARDIAN (June 30, 2013, 4:28 PM EDT), http://www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies (documenting NSA's monitoring foreign embassies in the United States including those of some allies); James Risen & Laura Poitras, *N.S.A. Gathers Data on Social Connections of U.S. Citizens*, N.Y. TIMES, Sept. 29, 2013, at A1 (detailing NSA programs to map Americans' personal connections); David Sanger & Mark Mazzetti, *Allegation of U.S. Spying on Merkel Puts Obama at Crossroads*, N.Y. TIMES, Oct. 25, 2013, at A10 (reporting a backlash from the discovery that the NSA was monitoring German Chancellor Angela Merkel's cellphone); Charlie Savage & Laura Poitras, *How a Court Secretly Evolved, Extending U.S. Spies' Reach*, N.Y. TIMES, Mar. 12, 2014, at A1 (publishing secret Foreign Intelligence Surveillance Court

C. Defining the "Deluge Leak"

Under the three metrics identified — the leaker's motivation, the leaker's rank in government, and the scope of the leaked material — the leaks made or facilitated by Manning, Snowden, and Assange via WikiLeaks share the same properties. First, as will be discussed in greater detail, these leakers were motivated by both a desire to unveil specific government conduct they believed was unlawful, as whistleblower leakers are, and also by their belief in the need for greater government transparency generally.[61] The motivation to protest excessive government secrecy more generally is not a driving force behind other leaks, including the Pentagon Papers leak.[62]

Second, these leaks originated with low-ranking officials. Chelsea Manning was a U.S. Army Soldier ranking Private First Class, a relatively junior position within the military.[63] Edward Snowden was likewise a relatively low-level employee, working as a systems administrator for NSA contractor Booz Allen Hamilton.[64] In particular, neither occupied a policymaking position.

Third, the scope of the recent disclosures is unprecedented.[65] Over a very short period of time, Manning, through Assange and WikiLeaks, released the Collateral Murder video, over 77,000 documents about the war in Afghanistan, over 390,000 documents about the Iraq war, over 250,000 diplomatic cables between the U.S. State Department and U.S. embassies around the world, and over 700 documents about individuals held at Guantanamo Bay.[66] Meanwhile, the full extent of Snowden's disclosures remains unclear, but the NSA chief at one point

orders allowing broad NSA wiretapping); Craig Timberg & Ashkan Soltani, *By Cracking Cellphone Code, NSA Has Capacity for Decoding Private Conversations*, WASH. POST (Dec. 13, 2013), http://www.washingtonpost.com/business/technology/by-cracking-cellphone-code-nsa-has-capacity-for-decoding-private-conversations/2013/12/13/e119b598-612f-11e3-bf45-61f69f54fc5f_story.html (revealing that the NSA has cracked the encryption of standard cell phones so it can listen in on private conversations). For a more complete timeline of reporting based on documents leaked by Snowden, see *Timeline of Edward Snowden's Revelations*, AL JAZEERA AM., http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html (last visited Jan. 13, 2015).

61 *See infra* Part V.

62 *See* HESS, *supra* note 2, at 75 (not listing secrecy protest as a common motivation for leaking).

63 *Profile: Private First Class Manning*, BBC, http://www.bbc.com/news/world-us-canada-11874276 (last updated Apr. 23, 2014, 1:50 PM ET).

64 John M Broder & Scott Shane, *For Snowden, a Life of Ambition, Despite the Drifting*, N.Y. TIMES, June 15, 2013, at A20.

65 ROSS, *supra* note 51, at xxix.

66 *Id.*; Fenster, *Disclosure's Effects*, *supra* note 8, at 762.

estimated that he leaked up to 200,000 secret records.[67] In a subsequent hearing before Congress, intelligence officials reported that Snowden accessed roughly 1.7 million files.[68] Because of the massive nature of these leaks perpetrated by individuals with relatively little authority but a profound concern about government secrecy generally, these leaks constitute a new species of leaks: "deluge leaks."[69]

While the recent leaks have been repeatedly compared to the leak of the Pentagon Papers,[70] Daniel Ellsberg's leak is different in important ways. Ellsberg's leak of over 7,000 pages of documents was certainly a massive leak, particularly in a pre-digital era, but those records were "leaked by a person innately involved in [the records'] collection and processing," rather than constituting "incidental files one individual happened to have access to."[71] The recent leaks, by contrast, constitute mass leaks of records including many with which the leakers admit to having had little or no familiarity.[72]

Ellsberg's credentials reinforce the difference in the leakers' situations: Ellsberg had obtained the highest civil service level in the Defense Department early in his career and was a high-ranking analyst at the RAND Corporation at the time he leaked the Pentagon Papers.[73] He has been described as "the consummate insider," one who "worked close to the seat of power on the very dossier he eventually leaked."[74]

---

[67] Mark Hosenball, *NSA Chief Says Snowden Leaked up to 200,000 Secret Documents*, REUTERS (Nov. 14, 2013, 4:04 PM EST), http://www.reuters.com/article/2013/11/14/us-usa-security-nsa-idUSBRE9AD19B20131114.

[68] David E. Sanger & Eric Schmitt, *Snowden Used Low-Cost Tool to Best N.S.A.*, N.Y. TIMES, Feb. 8, 2014, at A1.

[69] The only existing label I have found for this new type of leak is "megaleak," a label of which Julian Assange indicated approval. GREENBERG, *supra* note 14, at 2. This term was not defined as precisely as I define "deluge leaks." *See id.*

[70] For instance, Pozen classifies together as general leaks Ellsberg's leak of the Pentagon Papers, Manning's disclosure the diplomatic cables, and Snowden's mass disclosure of NSA records to the Guardian and the Washington Post. *See* Pozen, *supra* note 1, at 533.

[71] Peled, *supra* note 13, at 69.

[72] For a description of the leaked records and the probable lack of knowledge by the leakers, see *infra* notes 303–16 and accompanying text.

[73] McCurdy, *supra* note 12, at 126; *see also* GREENBERG, *supra* note 14, at 18 ("If Ellsberg's path to becoming the most prolific leaker of his age began with a steep upward trajectory fueled by Ivy League ambition, Bradley Manning set out from far more common circumstances: destitute, middle-American aimlessness.").

[74] McCurdy, *supra* note 12, at 126, 134; *see also* GREENBERG, *supra* note 14, at 21 ("Daniel Ellsberg read as much paperwork on the war in Vietnam as practically any Pentagon analyst.").

This stands in stark contrast to the relatively low ranks held by Manning and Snowden.[75] For reasons that will be elaborated on below, the unique properties of deluge leaks are crucial to understanding both the risks associated with them and the effectiveness of various interventions designed to curb them.

II. DANGERS OF DELUGE LEAKS

Deluge leaks are distinct from past leaks in their scope, the identity of the leaker, and the motivations behind the leak. Their typology, however, is not their only difference. This new type of leak also comes with new types of risks, ones that are likely of concern to a broad cross-section of society. This section will establish those risks, and will further argue that criminalization of leakers and publishers of leaks are likely to be ineffective at preventing deluge leaks.

A. Deluge Leaks Are on the Rise

While there may long have been the impetus to deluge leak, there is, no doubt, a driving force that makes the deluge leak only recently possible: technology. Technology has changed the access to information lower-level government officials and contractors have, thereby enabling them to deluge leak. It has also vastly increased the ease of distributing leaked information.

First, on the question of access, the government has increasingly sought to generate, gather, and share information widely across various government agencies.[76] These efforts have led to enormous databases of information, which vast numbers of people have permission to use.[77] The network Manning accessed, for example, is reportedly accessible to approximately 2.5 million military and civilian

[75] McCurdy, *supra* note 12, at 134 (noting that Manning was a "low-level security analyst, a node in a vast industry").

[76] *See id.* (citing the 9/11 Commission report as a motivating factor, as it concludes that breakdowns in information sharing was a key factor in failing to prevent the 9/11 attacks). Examples of increased sharing of databases within the federal government abound. For instance, under the Secure Communities program, the FBI, which has for decades collected arrestees' fingerprint data from local and state police departments, shares its fingerprint database with Immigration and Customs Enforcement ("ICE") so that ICE may determine if the arrestees may have violated immigration laws. *See Secure Communities*, U.S. IMMIGRATION & CUSTOMS ENFORCEMENT, http://www.ice.gov/secure_communities/ (last visited Jan. 12, 2015).

[77] McCurdy, *supra* note 12, at 134. McCurdy notes that "Consequently, PFC Manning's network access . . . must not be seen as an exception, but as typical of military work in the network society." *Id.* (emphasis omitted).

employees.[78] As for Snowden's information, while there are no precise estimates as to the number of employees who could access the databases from which it came, "details about virtually all of the NSA's surveillance programs were accessible to anyone, employee or contractor, private or general, who had top-secret NSA clearance and access to an NSA computer."[79]

Second, technology has not only changed access to information, but also the means of distribution. The Internet "serves as a force multiplier for leakers," because once information is released, it can be widely distributed instantaneously and, thereafter, difficult to contain.[80] "Mega-disclosures" are, by many accounts, a relatively new practice.[81] A single individual with access to databases can, acting completely alone, make disclosures of vast proportions.[82] One journalist who has studied WikiLeaks extensively declared that it "was the *inevitable* outcome of the changing nature of information and advancements in cryptographic anonymity . . . ."[83] President Barack Obama described Edward Snowden as a "twenty-nine-year-old [who ended up having] free rein to basically dump a mountain of information, much of which is definitely legal, definitely necessary for national security, and [is] properly . . . classified."[84]

The final factor that makes deluge leaks a growing probability is the development of more sophisticated online anonymity tools. WikiLeaks's success, for instance, is largely attributable to its commitment to offering meaningful anonymity to sources. It did so largely by using a system originally developed by the U.S. military known as Tor.[85] Strong anonymity protections can make leaking

[78] *Siprnet: Where the Leaked Cables Came from*, BBC (Nov. 28, 2010, 2:53 PM), http://www.bbc.co.uk/news/world-us-canada-11863618.

[79] James Bamford, *The Most Wanted Man in the World*, WIRED, http://www.wired.com/2014/08/edward-snowden/#ch-1 (last updated Aug. 22, 2014).

[80] Seth F. Kreimer, *The Freedom of Information Act and the Ecology of Transparency*, 10 U. PA. J. CONST. L. 1011, 1043 (2008).

[81] Peled, *supra* note 13, at 75.

[82] For example, nearly a year after Edward Snowden's leaks, investigations by the FBI, the NSA, and the Pentagon have turned up no evidence that Snowden received any help from foreign intelligence agencies, despite suggestions from members of Congress, and the FBI has stood by its conclusion that Snowden acted alone. *See* Sanger & Schmitt, *supra* note 68, at A5.

[83] GREENBERG, *supra* note 14, at 7.

[84] David Remnick, *Going the Distance: On and off the Road with Barack Obama*, NEW YORKER (Jan. 27, 2014), http://www.newyorker.com/magazine/2014/01/27/going-the-distance-2.

[85] GREENBERG, *supra* note 14, at 138 (quoting Assange as saying "Tor's importance to WikiLeaks cannot be understated"). Specifically, the Defense Advanced Research

without consequences a reality. As Assange declared, quoting Oscar Wilde, "Give a man a mask, and he'll tell you the truth."[86]

Deluge leaks are thus of a different nature than the leaking that had occurred before.[87] While not the motivating force behind these leaks, technological innovations in the past two decades have made this new type of leak possible.[88] The question, therefore, is whether these deluge leaks pose different sorts of risks than other types of leaks.

B. Harms from Deluge Leaks

There are many legitimate reasons for the government to keep information secret,[89] and even the most ardent transparency activists would agree that national security interests ought to justify protecting certain records from public view.[90] For instance, few reasonable people would deny the government the ability to keep secret information such as troop movements, the identity of undercover

Project Agency, or DARPA, built Tor. *Id.* at 139. "Tor" is an abbreviation for "The Onion Router," which is an analogy for the method Tor uses to anonymize information by having multiple layers of encryption, each only decipherable by the next "node" in a chain of nodes that handles transmitted data. *Id.* at 141. Anonymity and the use of Tor have been cited as the reasons for the success of BalkanLeaks, a WikiLeaks copycat site directed at the Balkan region. *Id.* at 233.

86 *Id.* at 152.

87 Pozen also notes that he shares an "intuition that there has been significant growth in the raw amount of leaks, or at least in the amount of publicization and republicization of leaks across various media outlets." Pozen, *supra* note 1, at 529.

88 *See* GREENBERG, *supra* note 14, at 46 ("There may not be many Daniel Ellsbergs in the world, ready to push through the twentieth century's stubborn barriers to leaking. But the twenty-first century would be wise to expect more Bradley Mannings.").

89 For example, the Freedom of Information Act ("FOIA") contains nine enumerated exemptions to mandatory disclosure of government records, which protect national security interests, but also other important interests such as trade secrets, personal privacy, law enforcement investigations, and agency deliberations. *See* 5 U.S.C. § 552(b)(1)–(9) (2012).

90 For instance, Rick Blum, the director of the Sunshine in Government Initiative, a coalition of media associations committed to promoting transparency in government, recently wrote an op-ed advocating for, among other things, better communication between government and the press before the publication of leaked national security information so that the press could accurately assess real national security risks — such as disclosure of operational details or intelligence sources and methods — and protect against them. *See* Rick Blum, Op-Ed., *Stop Trying to Stop Leaks. Engage the Press Instead*, ROLL CALL (Sept. 16, 2013, 11:39 AM), http://www.rollcall.com/news/stop_trying_to_stop_leaks_engage_the_press_instead_commentary-227621-1.html.

agents, or the keys to break military codes.[91] Leaks of these types of information would have a serious effect on national security without providing any obvious benefit to the public in its quest to keep the government democratically accountable.

The effect of most leaked information, however, is not nearly so clear as these extreme hypotheticals. Pozen recently argued that the government has deliberately chosen not to punish leakers because while individual leaks may be harmful to government interests, leaks as a whole are more beneficial than detrimental.[92] A permissive attitude toward leaks allows the government to credibly "plant" information in the press, and promotes the public's belief in the legitimacy of the government, compensating for an overbroad classification system.[93] The focus of Pozen's analysis, however, is the much more common, everyday leaks of higher-level government officials, and Pozen acknowledges that some leaks can be truly harmful.[94] Citing Chelsea Manning's disclosures to WikiLeaks as a "rare undeniable leak"[95] of the unauthorized nature, Pozen concedes that even a permissive approach to leakiness "cannot tolerate the proliferation of internal dissenters who seek to impeach the entire secrecy and national security system."[96] Pozen's account of the costs and benefits of leaking thus does not fully account for the deluge leak.

1. Past Harms

Are deluge leaks, then, the leaks that may cause so much harm that they cannot be tolerated? Certainly, government officials have been harsh in their condemnation of past deluge leaks. For example, high-level officials declared that Assange, and his source of Afghanistan war documents (then unknown) "might already have on their hands the

---

[91] *See* Alan M. Dershowitz, *Who Needs to Know?*, N.Y. TIMES, May 30, 2010, at BR13 (reviewing SCHOENFELD, *supra* note 5, at 31-32).

[92] Pozen, *supra* note 1, at 517-18.

[93] *Id.* at 564 ("Leakiness . . . an approach that generates sufficient randomness (or apparent randomness) across government sources as to degrade the ability of outsiders to predict the nature and origin of any given disclosure."); *id.* at 575 ("A leaky government is, over time, a trustworthy government.").

[94] *Id.* at 547 ("Judicial review appears to be an episodically painful, but globally beneficial, institutional design mechanism for Presidents and other high-level officials. The claim here is that leakiness works the same way.").

[95] *Id.* at 572.

[96] *Id.* at 600; *see also id.* at 593 ("For many in the White House, leaks by low-level career employees are seen as 'totally unacceptable from the standpoint of running the government.'").

blood of some young soldier or that of an Afghan family,"[97] that Manning's leak of State Department cables "put at risk our diplomats, intelligence professionals and people around the world who come to the United States for assistance in promoting democracy and open government,"[98] and that the records leaked by Snowden were "putting at risk our national security and some very vital ways that we are able to get intelligence that we need to secure the country."[99]

On the other side of the debate, of course, many have extolled the benefits of deluge leaks. In the case of WikiLeaks, the Iraq and Afghanistan war documents revealed matters of great public importance, including the mistreatment of prisoners,[100] thousands of unreported civilian deaths,[101] and even the likelihood that the United States would fail in reaching its objectives abroad.[102] WikiLeaks disclosures also documented the United States's distain for Tunisian leadership, which has been cited as emboldening opposition within the country and contributing to a popular uprising, kicking off the so-

[97] Greg Jaffe & Joshua Partlow, *Joint Chiefs Chairman Mullen: WikiLeaks Release Endangers Troops, Afghans*, WASH. POST, July 30, 2010, at A4 (quoting the Chairman of the Joint Chiefs of Staff). President Obama also made early comments about WikiLeaks disclosures: "I'm concerned about disclosure of sensitive information from the battlefield that could potentially jeopardize individuals or operations." *Obama on WikiLeaks: 'I'm Concerned*,' ABC NEWS (July 27, 2010), http://abcnews.go.com/Politics/video/obama-wikileaks-im-concerned-11260389.

[98] *Key Reactions to Wikileaks Cables Revelations*, BBC (Nov. 29, 2010, 5:28 PM), http://www.bbc.co.uk/news/world-us-canada-11866220 (quoting a White House statement). U.S. Representative Peter Hoekstra, the senior Republican on the House Intelligence Committee, also stated that "[m]any other countries — allies and foes alike — are likely to ask 'Can the United States be trusted? Can the United States keep a secret?'" *Id.*

[99] Barack Obama, President of the United States, Remarks by the President in a Press Conference (Aug. 9, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference. President Obama also said that Snowden "put people at risk." Remnick, *supra* note 84.

[100] *See* Nick Davies, *Iraq War Logs: Secret Order that Let US Ignore Abuse*, GUARDIAN (Oct. 22, 2010, 4:30 PM), http://www.theguardian.com/world/2010/oct/22/iraq-detainee-abuse-torture-saddam (reporting a military order to coalition troops not to investigate any breach of the laws of war unless it involved members of the coalition, and that the result of this order was widespread abuse of prisoners by Iraqi security forces with the knowledge of the U.S. military).

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

[102] Nick Davies & David Leigh, *Afghanistan War Logs: Massive Leak of Secret Files Exposes Truth of Occupation*, GUARDIAN (July 25, 2010, 5:03 PM), http://www.theguardian.com/world/2010/jul/25/afghanistan-war-logs-military-leaks; Eugene Robinson, *Wikileaks Reveal the Obvious Dangers of Afghanistan*, WASH. POST, Jul. 27, 2010, at A17.

called Arab Spring.[103] In fact, one study in early 2011 found that nearly half of all print issues of the *New York Times* over a five-month period used WikiLeaks documents as sources.[104] Snowden's leaks likewise are credited with revealing key information about the NSA's surveillance of people within the United States and launching an ongoing national debate about the NSA's proper role in private affairs.[105] Concern about these activities was so great that President Obama appointed a panel of advisors to study NSA surveillance, which ultimately recommended strictly curtailing the NSA's ability to engage in warrantless data collection.[106]

In the first attempt to systematically evaluate whether WikiLeaks's disclosures caused harm, Professor Mark Fenster concluded that there is no clear evidence from any public sources that there was significant damage to military operations, national security, or diplomatic efforts.[107] Fenster also noted that even government officials eventually retreated from their initial predictions about the extremely damaging effects.[108] At Manning's recent court-martial trial, the government attempted to mount evidence of the harm that flowed from Manning's leak, but largely failed by all accounts.[109] Similarly, former Secretary of

[103] Sami Ben Hassine, *Tunisia's Youth Finally Has Revolution on Its Mind*, GUARDIAN (Jan. 13, 2011, 5:00 AM EST), http://www.theguardian.com/commentisfree/2011/jan/13/tunisia-youth-revolution.

[104] Caitlin Dickson, *Nearly Half of 2011's New York Times Issues Rely on WikiLeaks*, WIRE (Apr. 25 2011, 4:59 PM ET), http://www.thewire.com/global/2011/04/over-half-2011s-new-york-times-issues-use-wikileaks/37009/.

[105] Editorial, *Edward Snowden, Whistle-Blower*, N.Y. TIMES (Jan. 1, 2014), http://www.nytimes.com/2014/01/02/opinion/edward-snowden-whistle-blower.html. In addition, there is evidence that customers are voting with their feet away from technology companies revealed to be complicit in the NSA PRISM program uncovered by Edward Snowden. *See* Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. TIMES (Mar. 21, 2014), http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html.

[106] David E. Sanger & Charlie Savage, *Obama Is Urged to Sharply Curb N.S.A. Data Mining*, N.Y. TIMES (Dec. 18, 2013), http://www.nytimes.com/2013/12/19/us/politics/report-on-nsa-surveillance-tactics.html.

[107] Fenster, *Disclosure's Effects*, *supra* note 8, at 806.

[108] *Id.* Fenster acknowledges that government agencies have had to adjust certain information protocols. *See id.* There may also be documented effects of the leaks that are simply not public. *Id.* Fenster also evaluates the benefits of the releases, and finds evidence of those benefits equally equivocal. *See id.*

[109] For instance, the general who led a Defense Department task force investigating the leak testified as to the Pentagon's fears that the leak would affect trust among nations, among American citizens, and among soldiers and civilians abroad, but could not cite specific data on chilled communications or trust, nor could he point to an incidence of individual harm. Emmarie Huetteman, *In Sentencing, U.S. Tries to Prove*

Defense Robert Gates, a Republican who served under Republican and Democratic Presidents, told reporters:

> I've heard the impact of these releases [of diplomatic cables] on our foreign policy described as a meltdown, as a game-changer, and so on. I think those descriptions are fairly significantly overwrought. . . . Is this embarrassing? Yes. Is it awkward? Yes. Consequences for U.S. foreign policy? I think fairly modest.[110]

As for Snowden's leaks, while they are much more recent, the evidence of harm is equally equivocal. One report indicated that intelligence agencies saw more harm in their ability to gather intelligence from an unrelated leak of information about a specific terrorist plot than from all of Snowden's leaks combined.[111] In concluding Snowden's leaks had less of an effect, officials reasoned that the surveillance programs revealed were so broad that terrorist organizations did not have a viable method of evading them, and thus did not stop using electronic communications.[112] Still, other officials took the opposite stance, that the Snowden leaks caused terrorists to change communication tactics.[113] Snowden has asserted, nine months after the leaks, that "no one has credibly shown any harm to national security."[114]

Harm from Leaks by Manning, N.Y. TIMES, Aug. 1, 2013, at A12. Another witness, an advisor to the Pentagon's task force on terrorism, did testify the leak could help al-Qaeda recruit and fundraise, but the evidence offered for this effect was thin. Emmarie Huetteman, *Witness in Manning Case Says Leaks Could Help Al Qaeda*, N.Y. TIMES, Aug. 9, 2013, at A9. Four other witnesses testified in secret, as their testimony concerned classified information, and it is hard to know what effects might be known, but subject to secrecy. *See id.*

110 Elisabeth Bumiller, *Gates on Leaks, Wiki and Otherwise*, N.Y. TIMES CAUCUS BLOG (Nov. 30, 2010, 7:30 PM), http://thecaucus.blogs.nytimes.com/2010/11/30/gates-on-leaks-wiki-and-otherwise/ (internal quotation marks omitted).

111 Eric Schmitt & Michael S. Schmidt, *Qaeda Plot Leak Has Undermined U.S. Intelligence*, N.Y. TIMES, Sep. 30, 2013, at A1.

112 *Id.*

113 *Id.* There is some additional recent evidence of changes in al-Qaeda communications tactics. Dina Temple-Raston, *Big Data Firm Says It Can Link Snowden Data to Changed Terrorist Behavior*, NAT'L PUB. RADIO (Aug. 1, 2014, 5:00 AM), http://www.npr.org/blogs/thetwo-way/2014/08/01/336958020/big-data-firm-says-it-can-link-snowden-data-to-changed-terrorist-behavior.

114 Jane Mayer, *Snowden Calls Russian-Spy Story "Absurd" in Exclusive Interview*, NEW YORKER (Jan. 21, 2014), http://www.newyorker.com/online/blogs/newsdesk/2014/01/snowden-calls-russian-spy-story-absurd.html.

While the government has incentives to demonstrate harms from leaks, and thus the lack of evidence of serious harms from the leaks may indeed indicate that none occurred, it is also possible that harms exist that are either kept classified or about which even the government is not aware. In sum, evaluating the actual effects of the deluge leaks that have occurred thus far is a difficult endeavor and the evidence is at best equivocal.

2. Potential Harms

Despite the lack of conclusive evidence of harms related to recent deluge leaks, there are theoretical and practical reasons why deluge leaks pose new concerns that may be particularly troubling. The practical reasons stem from the changing technology that enables deluge leaking. First, although the recent deluge leakers have each attempted to minimize the harm by redaction and selective withholding,[115] the ability of nearly anyone with some tech savvy to become a worldwide publisher certainly raises the possibility that a future publisher may not make such attempts. As Professor Patricia Bellia recently explained, the Supreme Court's heightened First Amendment protection for the press in the Pentagon Papers case was premised, in part, on the idea that "disclosure of national security information depends upon the judgment of the publisher — constrained by the possibility of criminal liability, by the market, or by journalistic ethics — and not solely upon the judgment of the leaker."[116] Non-traditional media in the form of online publishers, though, may not "hew to a set of recognized journalistic norms" in deciding whether to publish national security information.[117] The mere fact of a proliferation of potential publishers without the same kind of professional formation as traditional media raises this possibility,[118] as does, as discussed below, the lack of effective criminal sanctions for those publishers.

[115] For a detailed description of each leaker's efforts at harm minimization, see *infra* Part V.A.

[116] Bellia, *supra* note 26, at 1472.

[117] *Id.* at 1453. Of course, even traditional media may break journalistic norms at times. For instance, a British tabloid, *News of the World*, part of Rupert Murdoch's media conglomerate, was recently discovered to have engaged in illegal wiretapping, among other investigative practices. *See* Katrin Bennhold, *After 7 Months, British Hacking Case Heads to the Jury*, N.Y. TIMES, June. 11, 2014, at A9.

[118] *See* Pozen, *supra* note 1, at 580 ("While reporters and editors at the Times, the Post, and their ilk amass soft power, their commitment to responsible journalism, their interest in avoiding onerous regulation, their desire to remain in the loop for

Second, these leaks may be more dangerous in their sheer scope: whenever hundreds of thousands of records (exponentially larger than even the 7,000 pages of Pentagon Papers) are released, the risk is magnified that some information turns out to have a direct, harmful effect. This is true even when the leakers and/or publishers are taking harm-minimization steps, because mistakes are bound to happen and the risks are greater the larger the set of records. The scope of deluge leaks is augmented because the source documents can be published in their entirety through web publishers. Traditional leaks were constrained by the media's need to use space or airtime only for the most significant events, so not all leaked material would become public. When deluge-leaked records are published in full, however, they may contain information that seemed trivial to the leaker, but turns out to cause harm when expertise in the field is brought to bear.[119]

The final practical reason deluge leaks may pose new dangers is anonymity. Some contend that anonymity comes with a lack of accountability. That is, without the personal risk to the leaker, there is less pressure to get both the contents of the leak and the balance of benefits and harms correct.[120] The anonymity of the leaker may also pose practical difficulties verifying the authenticity of leaked records, thereby increasing the risk of misinformation.

Beyond practical reasons, there is also a theoretical basis for concern with the new deluge leak. Traditional whistleblower leakers disclose information or records concerning a particular government action or program that the leaker thinks reflects improper or illegal activity. These leakers engage in a sort of internal subjective balancing, weighing the public interest in knowing about the misconduct against potential harms that might result. As to these more traditional leaks, Pozen notes that "the backdrop of formal illegality [even if not enforced in practice] remains relevant, because in depressing the

future disclosures, and their repeat interactions with top officials all combine to give those officials leverage and to moderate the reporting. The natural tendency of leaks to cluster in a few major outlets has in turn helped to keep most news coverage within bounds the executive's leadership finds acceptable.").

119 *Id.* at 616.

120 *See, e.g.*, GREENBERG, *supra* note 14, at 218 (quoting Aaron Barr, chief executive of a security firm that has tried to identify leakers, as saying: "In a free and open democracy, [speech] should be attributable. That's one of my problems with anonymity. In most whistleblowing cases, there's a lot of personal risk and sacrifice. Their name's going to be attached to it. There are personal repercussions. There's pressure to get the information right, to get the perspective right. With anonymity, there's none of that").

overall amount of leaking it enhances the significance of the disclosures that occur."[121]

The deluge leaker, on the other hand, does not have the capacity to review the contents of all the records being released and to consider the public interest in disclosure of each one.[122] In fact, the deluge leaker is likely to be disclosing huge amounts of information in which the public has little interest, which shows no real wrongdoing or illegality, and which does not even make it into the public discourse. Nonetheless, this information may still have some harm associated with its disclosure, even if not the worst types of acute harm. Thus, even if the deluge leaker is successful in redacting or withholding the most sensitive information, he may be creating significant, if less critical, harms with no associated upsides to the public's interest in holding the government accountable.

This key difference is illustrated by the public discourse regarding two recent leaking examples. The first example is a specific leak made by Thomas Tamm who was the primary source behind the *New York Times* Pulitzer Prize winning story in 2005 revealing the Bush-era warrantless wiretapping program that eavesdropped on U.S. citizens.[123] As Tamm explained his motivations, it is clear that he weighed the public interest in the information he leaked: "I thought this [secret program] was something the other branches of the government — and the public — ought to know about. So they could decide: do they want this massive spying program to be taking place?"[124] The public debate about this leak, likewise, has focused on the benefits to the public versus the harms that may have arisen. For example, a leading critic of national security leaks has argued that this leak exposed a particularly successful program in a way that revealed intelligence sources and methods, and that the leak would logically deter al-Qaeda operatives from using certain methods of communication that would be susceptible to surveillance under the program.[125] On the other hand, a former whistleblower contended that

---

[121] Pozen, *supra* note 1, at 578.

[122] *See id.* at 617 (contending that low-level employees have the least understanding of the policy concerns or significance of the information they may encounter).

[123] 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; *see* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), http://www.nytimes.com/2005/12/16/politics/16program.html.

[124] Isikoff, *supra* note 123.

[125] SCHOENFELD, *supra* note 5, at 31-32.

the revealed program was unconstitutional, and, thus, that Tamm was justified in revealing its existence to the public.[126] Whatever the truth of the matter is, it is clear that both the potential public interest and the potential harm was considered by the leaker, and the debate is accordingly along those lines.

With deluge leaks, this kind of calculation is never made as to most of the records, nor could it be. Take, for example, WikiLeaks's publication of over 250,000 diplomatic cables between the U.S. State Department and U.S. embassies around the world. Although WikiLeaks frames this leak in the same way Tamm described his own, as an act of whistleblowing,[127] not all, or even close to all, of the cables released demonstrate objectionable government behavior, much less illegal behavior. Rather, the leak includes plenty of material that, while the public might find interesting or entertaining, no one would seriously argue implicates the public's interest in government oversight. For instance, one diplomatic cable recounted how the mayor of Paris had lit the Eiffel Tower in Turkey's national colors in honor of a visit from Turkey's Prime Minister.[128] Because former Prime Minister Nicolas Sarkozy was adamantly against Turkey's entry into the European Union, however, aides were afraid it would displease him and thus rerouted his plane to avoid him seeing the lit Eiffel Tower.[129] There is little, if any, value to the public from knowing how afraid Sarkozy's aides were of upsetting him, and yet there is also harm — albeit likely a small one — to the United States's relations with Prime Minister Sarkozy that one might naturally think would result. Whether or not this kind of material should be public, a traditional

---

126 *See, e.g.*, Jesselyn Radack, *Whistleblowers Expose Illegal Activity, Not Government Secrets*, *in* WHISTLEBLOWERS 87, 87-89 (Noah Bertlatsky, ed., 2012) (arguing that Schoenfeld's reasoning would lead to a contradiction where whistleblowers violated their oath of secrecy by revealing information, but the government did not violate its oath to uphold the Constitution when it acted).

127 On its own website, it declares: "The cables show the extent of US spying on its allies and the UN; turning a blind eye to corruption and human rights abuse in 'client states'; backroom deals with supposedly neutral countries; lobbying for US corporations; and the measures US diplomats take to advance those who have access to them." *Secret US Embassy Cables*, WIKILEAKS, https://wikileaks.org/cablegate.html (last visited Jan. 13, 2015).

128 Katrin Bennhold, *Cables Praise French Friend with "Mercurial" Side*, N.Y. TIMES (Nov. 30, 2010), http://www.nytimes.com/2010/12/01/world/europe/01wikileaks-france.html [hereinafter *Cables Praise*]; *see also US Embassy Cables: Nicolas Sarkozy Strikes Fear into His Advisors*, GUARDIAN (Nov. 30, 2010, 4:30 PM), http://www.theguardian.com/world/us-embassy-cables-documents/238115 [hereinafter *US Embassy Cables*].

129 *See* Bennhold, *Cables Praise*, *supra* note 128; *US Embassy Cables*, *supra* note 128.

leaker would hardly consider disclosing it sufficiently worthwhile to the public to put him or herself at risk. In the context of a deluge leak, however, the sheer volume of records makes calculations about the public benefit of each individual document impossible. Thus, deluge leakers may be able to avert the most serious harms through, say, redaction, but are still prone to causing less serious and more diffuse harms simply because the deluge leaker makes no individualized determination that each leaked record is important to the public.[130] Certainly, the government itself sees the threat of deluge leaks as distinct.[131]

Pozen has remarked that although leaks to date have proven to confer more benefit than harm to government interests, and thus have been treated with relative permissiveness, "[i]t is an open question whether leaking will continue to provide similar benefits for executive policymakers and the establishment press in the years ahead" given the new media publishers uptick in leak-related activity.[132] The practical and theoretical reasons why deluge leakers pose heightened risks, as described in this section, suggest that deluge leaking will become more costly over time.

C. Limits of Criminalization

Acts of leaking classified information have long been criminalized. The Espionage Act of 1917, the primary statutory vehicle for addressing leaks of national security information, criminalizes various activities connected to obtaining and releasing information related to

---

[130] To be clear, I do not contend that government release of records through our formal mechanisms, such as FOIA, should be preconditioned on a showing of public interest. To the contrary, FOIA appropriately presumes all government records to be available, subject to enumerated exemptions. *See infra* Part IV.A (discussing FOIA in detail). I argue only that when considering informal disclosure through leaks, the leakers themselves have different considerations in a targeted leak versus a deluge leak, and that those different considerations are likely to lead to more diffuse and varied types of harms that pose different concerns.

[131] *See* Pozen, *supra* note 1, at 630-31 (noting that the Obama administration's uptick in leak prosecution may respond to the perception that leaks are producing greater genuine security threats perhaps as a result of low level employees greater ability to engage in deluge leaking, and that the changing leak landscape may mean that while "plants may need to be watered with leaks . . . they are unlikely to thrive in a downpour"). Tom Tyler has observed that "[l]egal authorities often find that they must tolerate occasional noncompliance with laws that are generally followed, and at some times they are faced with noncompliance so widespread that it threatens their ability to govern effectively." TYLER, *supra* note 28, at 64. The deluge leaker poses the type of widespread noncompliance that poses such a potential threat.

[132] Pozen, *supra* note 1, at 581.

the "national defense."[133] Those who disclose classified information to non-authorized recipients can be, and in fact have been, prosecuted.[134] Deluge leakers are no exception. Manning, for instance, was court-martialed, and charged with twenty-two crimes, seven of which were violations of the Espionage Act and of those she was convicted of six.[135] Snowden was likewise charged with three criminal offenses, two of which were for violations of the Espionage Act.[136] Certainly, then, the leakers themselves can be criminally punished for their actions.

Despite the clear legal authority for prosecuting leakers, shockingly few prosecutions occur. In fact, there have only been between one and two-dozen criminal prosecutions of individuals who have leaked national security-related information.[137] Even the recent seeming uptick in prosecutions during the Obama Administration (eight) represents a miniscule proportion of leaks that resulted in criminal

[133] 18 U.S.C. § 793 (2012). For a detailed account of the various specific provisions of the Espionage Act, see Stephen I. Vladeck, *Inchoate Liability and the Espionage Act: The Statutory Framework and the Freedom of the Press*, 1 HARV. L. POL'Y REV. 219, 221-26 (2007).

[134] Pozen, *supra* note 1, at 525 (detailing the consensus that virtually all unauthorized disclosures of classified information would be prosecutable offenses).

[135] Ernesto Londono, Rebecca Rolfe & Julie Tate, *Verdict in Bradley Manning Case*, WASH. POST (July 30, 2013), http://www.washingtonpost.com/wp-srv/special/national/manning-verdict/. Technically all of Manning's charges fell under the Uniform Code of Military Justice ("UCMJ") because she was a soldier, but the UCMJ incorporates the criminal code in certain respects, including the Espionage Act. Press Release, U.S. Div. — Ctr., Soldier Faces Criminal Charges (July 6, 2010), *available at* http://www.cbsnews.com/htdocs/pdf/ManningPreferralofCharges.pdf. In addition to the one count under the Espionage Act, the only other charge of which Manning was acquitted was the most serious charge of aiding the enemy. Londono, Rolfe & Tate, *supra*. The other charges of which she was convicted included stealing government property and violations of the Computer Fraud and Abuse Act, as well as violations of military regulations. *Id.*

[136] *See* Criminal Complaint, United States v. Snowden, No. 1:13 CR 265 (CMH) (E.D. Va. June 14, 2013), *available at* https://s3.amazonaws.com/s3.documentcloud.org/documents/716888/u-s-vs-edward-j-snowden-criminal-complaint.pdf. The third charge was for theft of government property. *Id.* Because Snowden has gained temporary asylum in Russia, he has not yet stood trial for these charges. *See* Steven Lee Myers & Andrew E. Kramer, *Defiant Russia Grants Snowden Year's Asylum*, N.Y. TIMES, Aug. 2, 2013, at A1.

[137] David McCraw & Stephen Gikow, *The End to an Unspoken Bargain? National Security and Leaks in a Post-Pentagon Papers World*, 48 HARV. C.R.-C.L. L. REV. 473, 492 (2013) (citing three prosecutions under the Espionage Act prior to the Obama Administration, six more during the Obama administration, and a handful of other Obama Administration investigations that did not result in charges); Pozen, *supra* note 1, at 534 (adding to that list two more recent indictments, including Snowden's, and citing another roughly dozen cases in history that arguably should be on the list).

consequences.[138] The relative rarity of prosecutions of leakers also seems to fly in the face of government officials' statements about the serious harms to national security that result from leaks.

Several leading theories have emerged as to why so few leakers have been prosecuted. The classic theory is that enforcement efforts in this area are notoriously difficult because leakers are nearly impossible to identify.[139] Pozen has called this theory into considerable question by documenting a lack of evidence that leak investigations are truly too difficult. Pozen has offered an alternative explanation that executive branch officials prefer not to enforce anti-leaking laws because the government receives significant benefits from its permissive approach to leaks.[140] Another theory explaining the under-enforcement is that the government has essentially struck a bargain with the press in which the press and leakers would not be punished. In exchange, the press would be responsive to the government's national security concerns in deciding what to publish.[141] Under both theories, leakers go free because the government wants them to.

Whatever the reason, there is widespread consensus that relying on criminal prosecution to deter leakers has, to date, proved an ineffective deterrent, especially as the government has consistently under-enforced the laws on the books.[142] Nonetheless, many of the proposals to address the problems of leaks center on toughening anti-leak laws. In Congress, anti-leak legislation has been introduced innumerable times, usually failing to pass because of concerns about press freedom and whistleblower protections.[143] One prominent attempt in 2012 would have required all intelligence employees to report all contacts with media, limited the authority to provide off-the-record information to certain high-ranking officials, and set up a leak-reporting procedure within intelligence agencies.[144] In March 2014, the head of the NSA suggested that yet another anti-leak legislation proposal was coming soon.[145] Scholars have likewise "felled forests in

---

[138] Pozen, *supra* note 1, at 536.

[139] ROSS, *supra* note 51, at 20-22.

[140] Pozen, *supra* note 1, at 544-45.

[141] McCraw & Gikow, *supra* note 137, at 479.

[142] ROSS, *supra* note 51, at 19, 28.

[143] Cora Currier, *Washington's War on Leaks, Explained*, PROPUBLICA (Aug. 2, 2012, 10:52 AM), http://www.propublica.org/article/washingtons-war-on-leaks-continues-cracking-down-on-press.

[144] *Id.*

[145] *Anti-leaks Legislation Coming Within Weeks, Says NSA Chief*, RT (Mar. 5, 2014, 4:26 AM) http://rt.com/usa/leaks-legislation-coming-nsa-alexander-879/.

the past several decades attempting to suggest how such comprehensive legislative reform could — and should — be pursued."[146] Despite the volume of proposed reforms, the evidence suggests that the extant laws cover the essential objectionable leaking conduct, but that enforcement is consistently lacking. Simply refining the conduct that would be deemed criminal would fail to address this fundamental concern.

Moreover, there are additional significant barriers to criminal enforcement with respect to third-party publishers of leaked records. The language of the Espionage Act appears on its face to reach the actions of members of the media who publish classified information leaked to them, but not a single member of the press has ever been prosecuted for publishing leaked material.[147] The government did famously attempt to enjoin the *New York Times* and the *Washington Post* from publishing the Pentagon Papers, but the Supreme Court refused to issue a prior restraint on the publication by reasoning that the press enjoyed First Amendment protections.[148] While post-publication prosecution remains a theoretical possibility, no such prosecutions have been brought, and in any event, they would likely be subject to a very stringent standard in light of First Amendment constraints.[149] For these very reasons, the Department of Justice has not brought charges — under the Espionage Act or any other criminal statute — against Julian Assange or WikiLeaks.[150] Justice Department officials described prosecuting Assange as posing a "*New York Times* problem," by which they meant that if Assange were prosecuted, the *New York Times* or other mainstream news media could also be prosecuted every time they published any classified material.[151]

---

[146] Stephen I. Vladeck, *Commentary in* ROSS, *supra* note 51, at xiii [hereinafter *Commentary*].

[147] Geoffrey Stone, *Government Secrecy vs. Freedom of the Press*, 1 HARV. L. & POL'Y REV. 185, 197 (2007).

[148] N.Y. Times Co. v. United States, 403 U.S. 713, 714 (1971) (per curiam).

[149] Stone, *supra* note 147, at 202 ("I conclude that the test articulated in *Pentagon Papers* is essentially the standard the Court would have applied in a criminal prosecution of the *Times* for publishing the Pentagon Papers. And even if that was not obvious in 1971, it is certainly clear today.").

[150] Sari Horwitz, *Julian Assange Unlikely to Face U.S. Charges over Publishing Classified Documents*, WASH. POST (Nov. 25, 2013), http://www.washingtonpost.com/world/national-security/julian-assange-unlikely-to-face-us-charges-over-publishing-classified-documents/2013/11/25/dd27decc-55f1-11e3-8304-caf30787c0a9_story.html (reporting that the Justice Department had "all but concluded it will not bring charges against WikiLeaks founder Julian Assange").

[151] *Id.*

Perhaps because the Pentagon Papers case leaves open the question of whether the press can, consistent with the First Amendment, be criminally prosecuted for publishing national security information, numerous scholars have explored the scope of First Amendment protections in this area.[152] Some proposed reforms have focused on criminally punishing the press. Professor Geoffrey Stone, for example, addressed the circumstances in which the government should be able to criminally punish public employees for leaking, the press for publishing leaked material, and journalists for receiving leaked material.[153] Hudson Institute researcher Gabriel Schoenfeld proposed a regime of increased prosecutions of the press, with prosecutorial discretion balancing the public's interest in a free press versus the public's interest in national security.[154] Among these commentators, however, there is widespread agreement that the First Amendment at a minimum constrains the ability to prosecute the press.

In addition to First Amendment concerns, Professor Patricia Bellia has argued that there are unique doctrinal hurdles to holding a publisher such as WikiLeaks liable that do not apply to a traditional publisher such as the *New York Times*.[155] First, it is not clear whether existing criminal penalties do or could reach the extraterritorial activities of a non-U.S. based Internet publisher.[156] Second, even if the law did reach those activities, it is not clear that a judgment rendered against such a publisher would be enforceable.[157] These pose substantial constitutional and statutory hurdles to effective criminal enforcement.

Finally, as other countries have stronger protections for journalists, those locations will become safe havens for publishers of leaked information and extradition from those countries may not be possible.[158] For example, Sweden, where WikiLeaks moved its servers to in 2007,[159] offers the oldest protection for freedom of the press

[152] For examples, see sources cited *supra* note 20.

[153] GEOFFREY R. STONE, TOP SECRET: WHEN OUR GOVERNMENT KEEPS US IN THE DARK 3-4 (2007). He also addressed the circumstances under which the government should be able to compel a journalist to reveal a source. *Id.*

[154] SCHOENFELD, *supra* note 5, at 268.

[155] Bellia, *supra* note 26, at 1506-11.

[156] *Id.* at 1479.

[157] *Id.* at 1482.

[158] Molly Thebes, Note, *The Prospect of Extraditing Julian Assange*, 37 N.C. J. INT'L L. & COM. REG. 889, 913 (2012) (analyzing the bases for extradition and concluding that extradition to the United States from either Sweden or Iceland, the two countries to which Assange has the strongest ties, may not be possible).

[159] *See* Malin Rising, *Sweden's Pirate Party Offers WikiLeaks Safe Haven Online*,

embodied in its constitution, which allows broad access to public records, the right to communicate information to the media, and the media's right to protect anonymous sources.[160] Iceland has also recently moved onto the global stage as an "international transparency haven."[161] In 2010, the Icelandic Parliament passed the Icelandic Modern Media Initiative, a resolution that directs the government to begin reforms to strengthen various protections for free speech and journalism by borrowing from the most journalist-friendly laws around the world and making Iceland a place where media would be immune from various types of liability that exist elsewhere.[162]

The volume of scholarly debate on legal reforms alone demonstrates the difficultly of the issues. When viewed through the lens of criminalization, the multiple public interests implicated by deluge leaks compete with one another: the freedom of the press and the secrets concerning our national security cannot both be perfectly protected at once, and the perfect balance of criminalization versus permissiveness may not be ascertainable. Constitutional and practical constraints make the most aggressive criminal penalties unlikely to succeed, thereby establishing a need to look elsewhere for solutions. Moreover, social science literature demonstrates that imposing criminal penalties as a method for deterring undesirable behavior is widely regarded as a relatively inefficient and ineffective way to achieve social order.[163] The amount of enforcement needed to

HUFFINGTON POST (Aug. 19, 2010, 10:51 AM), http://www.huffingtonpost.com/2010/08/18/wikileaks-seeks-online-sa_n_686815.html.

160 *See The Swedish System of Government*, SWEDISH INST., http://sweden.se/society/the-swedish-system-of-government/ (last updated Nov. 13, 2014). The freedom of press protections were first introduced in Sweden in 1766. *Id.*

161 *See IMMI Resolution*, INT'L MODERN MEDIA INST., https://en.immi.is/immi-resolution/ (last visited Jan. 7, 2015).

162 Afua Hirsch, *Iceland Aims to Become a Legal Safe Haven for Journalists*, GUARDIAN (July 12, 2010, 1:59 AM), http://www.theguardian.com/media/2010/jul/12/iceland-legal-haven-journalists-immi. In fact, Julian Assange collaborated on drafting the IMMI. Arne Hintz, *Dimensions of Modern Freedom of Expression: WikiLeaks, Policy Hacking, and Digital Freedoms*, *in* BEYOND WIKILEAKS, *supra* note 12, at 146, 157-58. Hintz explains that the IMMI was designed to "prevent the suppression of content by both public and private actors." *Id.* at 157.

163 *See* TYLER, *supra* note 28, at 110 ("[R]ecent studies have found that creating a moral climate of support for a law will alter compliance more effectively than will changing estimates of the certainty or severity of punishment."); Josh Bowers & Paul H. Robinson, *Perceptions of Fairness and Justice: The Shared Aims and Occasional Conflicts of Legitimacy and Moral Credibility*, 47 WAKE FOREST L. REV. 211, 273 (2012) ("[M]anipulating liability and punishment rules within [the criminal justice] system will work only in . . . atypical cases . . . ."); Daniel S. Nagin, *Criminal Deterrence Research at the Outset of the Twenty-First Century*, 23 CRIME & JUST. 1, 1-42 (1998).

sufficiently deter behavior through threat alone is incredibly resource-intensive, and even more so in the context of anti-leak laws that officials contend are particularly difficult to enforce. Lastly, there is a certain futility to targeting people who release information, since the information is already publicly available for anyone to do with it as they wish. Indeed, as one commentator noted, "[t]ools to address ex post the secondary transmission of leaked information are, by definition, less effective."[164] In sum, criminalization has not worked in this area, proposals for reform necessarily engage in impossible line drawing in an attempt to balance press freedoms and national security, and any increase in enforcement would likely be very costly with little deterrence benefit. Other avenues must be explored.

III. PROCEDURAL JUSTICE AND LEGITIMACY

In seeking methods to curb deluge leaks other than criminalization, understanding the impetus behind these leaks is critical. Other scholars have asserted that excessive secrecy drives leaking. One scholar contended that "[n]ontransparent policies will ultimately result in cyber protests through hacks, leaks, and the assembly of organizations such as WikiLeaks, with the goal of bringing frustrations to the attention of the general public."[165] Another noted,

> We live in an age of "unlawful secrets" — information that is either wrongly classified, or classified information about unlawful governmental programs. . . . I doubt I am exaggerating in suggesting that the government's credibility — or lack thereof — had as much to do with the upsurge in unauthorized disclosures in the latter years of the Bush administration as the collective media itself.[166]

Yet another suggested that "if members of Congress were more willing to evaluate and consider releasing classified information, future Mannings and Snowdens might be willing to leak to them rather than engaging in indiscriminate public releases."[167]

Most notably, Pozen's in-depth treatment of leaking practices generally concluded that leaking "may be better understood as an adaptive response to key external liabilities — such as the mistrust

---

[164] Bellia, *supra* note 26, at 1508.

[165] Renee Keen, *Untangling the Web: Exploring Internet Regulation Schemes in Western Democracies*, 13 SAN DIEGO INT'L L.J. 351, 375 (2011).

[166] Vladeck, *Commentary*, *supra* note 146, at xiv.

[167] Josh Chafetz, Response, *Whose Secrets?*, 127 HARV. L. REV. FORUM 86, 91 (2013).

generated by presidential secret keeping and media manipulation — and internal pathologies — such as overclassification and fragmentation across a sprawling bureaucracy — of the modern administrative state."[168] His work compellingly demonstrated that the government's decision not to aggressively prosecute leakers is deliberate because the government receives a net benefit from leaking insofar as it gives them the necessary "leeway and legitimacy" to govern.[169] Under Pozen's theory, however, legitimacy is only one of the many benefits the government accrues from leaking,[170] and the focus of his study is the much more historically common form of leaking: small scale, single topic, high-level official leaking.[171]

Despite scholars' general suggestions that the existing government transparency system leads to leaking, no one has articulated a theoretical basis for this hypothesis or documented evidence of the link. This Part describes the social justice literature on procedural justice and legitimacy, and argues that it can be used to understand the driving forces behind deluge leaks.

A. Perceptions of Fairness in Law

In his seminal work, *Why People Obey The Law*, Professor Tom Tyler reported the findings of a study in which he interviewed over 1,500 people to determine why people complied with various types of laws, including littering, speeding, drunk driving, and theft.[172] Having taken

168 Pozen, *supra* note 1, at 517-18.

169 *Id.* at 518. Pozen explains how leaks may create a public trust in the legitimacy of the government: "If members of the public believe leaking is pervasive, then they should expect to learn about most of the nefarious or unlawful things the executive branch might be doing, along with any associated internal disagreements, whether or not the President wants them to." *Id.* at 574.

170 He identifies the various interests as "preserving ambiguity as to the origins of unattributed disclosures and therefore the communicative flexibility of top officials; signaling trustworthiness; facilitating richer internal information flows; pacifying constituencies for transparency in Congress, the media, and civil society; and mitigating the classification system's political and deliberative costs." *Id.* at 518; *see id.* at 562 ("Planting is not an incidental practice of a few craven officials. It is programmatic, a mode of governance."); *id.* at 564 ("Leakiness preserves the President's plausible deniability as to his role in the disclosure, if not in the underlying policy as well.").

171 *See id.* at 551 (arguing that enforcing anti-leak laws should be easier because "leaks are predominantly the province of top government officials with good media contacts"); *id.* at 567 (stating that there is a "spectrum [that] runs from the quintessential plant . . . to the quintessential leak . . . . Most unattributed disclosures to the press reside somewhere well between these poles").

172 TYLER, *supra* note 28, at 41.

into account a range of factors in determining legal compliance, Tyler concluded that individuals' belief in the legitimacy of the legal system significantly influenced their decisions to comply with the law.[173] Legitimacy, he notes, is characterized by the "belief that some decision made or rule created by [an] authorit[y] is valid in the sense that it is entitled to be obeyed by virtue of who made the decision or how it was made."[174] Tyler's work also demonstrated that socialization — attitudes and beliefs about legal authorities formed during childhood — does not fully explain individuals' perception of the legitimacy of the legal system.[175] Instead, Tyler showed that views of legitimacy are significantly affected by individuals' experiences with the law over their lifetimes and, in particular, whether they feel they have been treated fairly in those experiences.[176] Importantly, the driving experiential factor in determining legitimacy was found to be what is now known as procedural justice; that is, the perception that the process used was fair, rather than simply whether the outcome was favorable.[177]

Tyler's study examined compliance with the law at a high level of generality by documenting interactions of any kind with police or courts and subsequent law-breaking of the most common types of laws encountered every day, such as littering and traffic laws.[178] Moreover, his study focused on the effect of personal, rather than vicarious interactions with law enforcement.

Other scholars, however, have demonstrated that compliance with certain sets of laws is linked to views of the legitimacy of those particular laws, and have also accounted for the effect of vicarious, rather than personal, experience in forming beliefs on legitimacy.[179] One such study examined the factors that influence migrants to the

---

[173] *Id.* at 61 ("[T]he finding that legitimacy influences compliance is robust across a variety of changes in methodology.").

[174] Tom R. Tyler, *Psychological Perspectives on Legitimacy and Legitimation*, 57 ANN. REV. PSYCHOL. 375, 377 (2006).

[175] TYLER, *supra* note 28, at 67.

[176] *Id.* at 63.

[177] *Id.* at 106. Certainly, there is a debate in the literature about how conclusively the procedural justice component of legitimacy has been proven to affect compliance rates. Bowers & Robinson, *supra* note 163, at 255.

[178] TYLER, *supra* note 28 at 19, 43.

[179] Janice Nadler, *Flouting the Law*, 83 TEX. L. REV. 1399, 1408-09 (2005). Even distant vicarious experiences, such as images of the legal system and enforcement in the media, can form the basis for legitimacy beliefs. *See* Bowers & Robinson, *supra* note 163, at 221-22 (citing the examples of Rodney King, Arthur McDuffie, and Abner Louima).

United States from Mexico to violate U.S. immigration laws.[180] In that study, the participants who viewed the U.S. immigration law system as procedurally unjust were much more likely to enter the United States in violation of those laws.[181] By contrast, participants' views on the acceptability of law breaking generally had a smaller effect on their likelihood to enter the United States without authorization than their views on the fairness of immigration laws specifically.[182] Moreover, participants were asked about their perception of the law's fairness without regard to whether that perception was formed by personal or vicarious experience.[183]

Similarly, another study documented the relationship between perceived procedural unfairness in the administration of the U.S. tax laws and the intention to break tax laws in the future.[184] Participants in this study reported their views on the procedural justice of tax laws based on both their own experiences with the IRS and the experiences of people the participants knew.[185] As with the perceived fairness of immigration laws, this study also suggests that the perceived legitimacy of a particular set of laws — whether formed by personal or vicarious experience — is related to the intent to comply with that same set of laws.[186]

Importantly, the literature has also identified certain aspects of procedure that most influence individuals' views of the legitimacy of law enforcement. Among the most important factors are neutrality of the decision-maker, ability to participate in the process, and the decision-maker's apparent efforts to be equitable.[187] Moreover, when

---

[180] Emily Ryo, *Deciding to Cross: Norms and Economics of Unauthorized Migration*, 78 AM. SOC. REV., 574, 574-603 (2013).

[181] *Id.* at 592 (reporting that an individual's agreement that the U.S. immigration law system is not legitimate increases the odds of intending to migrate without authorization by a factor of 2.735).

[182] *Id.* at 589, 592 (reporting agreement that it is sometimes okay to break the law as increasing the likelihood of deciding to enter the United States without authorization by a factor of 1.941).

[183] The relevant survey questions asked for levels of agreement with the following statements: "U.S. immigration service treats Mexicans fairly," and "U.S. immigration service treats lighter-skinned immigrants better." *Id.* at 583.

[184] Karyl A. Kinsey, *Deterrence and Alienation Effects of IRS Enforcement: An Analysis of Survey Data*, *in* WHY PEOPLE PAY TAXES: TAX COMPLIANCE AND ENFORCEMENT 259, 276 (Joel Slemrod ed., 1992).

[185] *Id.* at 264.

[186] *Id.* at 276; *see also* Nadler, *supra* note 179, at 1410 (noting this as a limitation for Nadler's purpose, but also that the study demonstrates correlation, and not causation).

[187] TYLER, *supra* note 28, at 137-38; *see also* Bowers & Robinson, *supra* note 163, at

governmental procedures are opaque or inaccessible, individuals' views of the general outcomes of cases may also serve as a proxy for their views of the fairness of the process.[188] An examination of the procedural fairness of any set of laws should thus be focused on these factors.

B. Relevance to Deluge Leaks

As for the decision of government employees or contractors to engage in deluge leaking, the relevant legitimacy inquiry can be focused on a specific set of laws that is of core concern: laws regulating the disclosure of government information. Certainly, this set of laws includes the criminal statutes that punish leaking, as described above, but also the classification laws, which designate the records that must be kept secret;[189] the Freedom of Information Act ("FOIA"), which designates those records that must be made public;[190] and the whistleblower protection laws, which designate procedures for

215-16 ("[P]rocedures are legitimate when they are neutral, accurate, consistent, trustworthy, and fair — when they provide opportunities for error correction and for interested parties to be heard."); Debra L. Shapiro & Jeanne M. Brett, *Comparing Three Processes Underlying Judgments of Procedural Justice: A Field Study of Mediation and Arbitration*, 65 J. OF PERSONALITY & SOC. PSYCHOL. 1167, 1167-77 (1993) (emphasizing participation in the process as an important factor in various ways). The factors are sometimes articulated differently when discussing the actions of police versus the actions of adjudicators, but the principles are very similar, and in the case of secrecy laws, the police do not play a big role. *See, e.g.*, Bowers & Robinson, *supra* note 163, at 252 ("The bulk of studies drawing this link between perceptions of legitimacy and deference have examined the question through the lens of police practices."); *id.* at 221 ("[P]eople are likelier to perceive police decision making as fair when officers make decisions according to readily discernible and generally applicable rules, standards, and guidelines. Likewise, people are likelier to perceive police treatment as fair when officers behave in manners that are trustworthy, equitable, dignified, and respectful.").

[188] Joseph P. Daly & Thomas M. Tripp, *Is Outcome Fairness Used to Make Procedural Fairness Judgments When Procedural Information is Inaccessible?*, 9 SOC. JUST. RES. 327, 328-31 (1996). Tyler himself acknowledges this potential link. Over the long run, Tyler posits, if the outcomes are viewed as consistently unjust, the procedures used to get there, no matter how many bells and whistles, will not be viewed as fair. *See* TYLER, *supra* note 28, at 30. This is akin to the law's recognition that due process rights reflect not only procedural rights, but substantive ones as well: some laws may produce such substantively unfair results that no amount of process can redeem the outcome. *See id.* Indeed, whether process and substantive outcome are distinct is still an open question. Bowers & Robinson, *supra* note 163, at 220. Nonetheless, Tyler posits, legitimacy can act as a "cushion of support" that allows legal authorities to exercise discretion effectively. TYLER, *supra* note 28, at 30.

[189] Classification is governed primarily by executive order. For a detailed discussion, see *infra* Part IV.B.

[190] 5 U.S.C. § 552 (2012); *see also infra* Part IV.A (discussing FOIA).

reporting illegal government conduct.[191] This set of laws addresses different facets of the same question: the circumstances under which government information must be kept secret versus when it may be disclosed. It is this set of laws that should be analyzed for perceptions of legitimacy on the part of those with access to secret government information.

Government employees and contractors are likely to form their perception of the legitimacy of laws regulating the disclosure of government information from a mixture of personal and vicarious experience. While certainly not all government employees or contractors will have personal experience with FOIA, classification, or whistleblower laws, vast numbers will have at least encountered the first two sets of laws. As to classification, as of October 1, 2012, there were an estimated 4,917,751 individuals who held security clearances that allowed them access to classified information.[192] That is, literally millions of people have jobs where they interact with the classification system. Many (though certainly not all) of those individuals are likely to have access to the large quantities of information necessary to deluge leak.

As to FOIA, while precise numbers of government employees directly involved with processing FOIA requests are not available, it is clear that significant numbers of staff have at least some personal involvement. For instance, the Department of Transportation reported that in FY 2011 92.65 staff-years were spent administering FOIA, but only 37 staff-years were attributed to full-time FOIA employees.[193] The remaining 55.65 staff-years were attributed to part-time FOIA staff and also program office staff, who searched for and reviewed responsive records.[194] That is, FOIA responsibilities are spread widely, and the

191 *See infra* Part IV.C (discussing whistleblower laws).

192 OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, 2012 REPORT ON SECURITY CLEARANCE DETERMINATIONS 3 (2013), *available at* https://www.fas.org/sgp/othergov/intel/clear-2012.pdf. Of these, 3,507,782 held a security clearance for confidential/secret information, and 1,409,969 for top secret information. *Id.* The majority were government employees, but contractors made up over a million of those holding security clearances, and held 483,263 of the "top secret" clearances. *Id.* "Secret," "confidential," and "top secret" are all designations within the classification scheme. *See* Exec. Order No. 13,526, § 1.2, 3 C.F.R. 298, 298-99 (2009), *available at* http://www.gpo.gov/fdsys/pkg/CFR-2010-title3-vol1/pdf/CFR-2010-title3-vol1-eo13526.pdf.

193 *FOIA-Related Open Government Information, Description of the Department's Staffing, Organizational Structure, and Process for Analyzing and Responding to FOIA Requests*, U.S. DEP'T OF TRANSP., http://www.dot.gov/individuals/foia/foia-related-open-government-information (last updated Jan. 20, 2015).

194 *Id.*

search for and review of responsive records often involves the individuals working on the agency's substantive agenda.

Certainly, some people with access to confidential government information (potential deluge leakers) will not have had personal experiences with classification or FOIA laws. Furthermore, it is likely that very few such individuals would have personal experience with whistleblower laws. For those, vicarious experiences through the media or colleagues will serve as their sources of information on the legitimacy of this set of laws. In fact, exposure to vicarious information about how these laws operate is highly likely given the wide coverage of government secrecy that appears in major news outlets as well as the close personal and professional contact federal employees have with one another, especially in the Washington, D.C. region.

Before proceeding to document the reasons why the perceived legitimacy of transparency laws is likely to be low, it is worth noting that a distinct phenomenon called moral credibility promotes compliance with the law independent of legitimacy.[195] A law attains moral credibility when it "assigns liability and punishment in ways that the community perceives as consistent with its shared intuitions of justice . . . ."[196] Unlike unjust outcomes of particular cases that implicate a problem of enforcement, substantively unjust laws are laws that are perceived to proscribe the wrong conduct or require unfair results.[197] Examples include the public's perception of the underlying fairness of three strikes laws, high penalties for drug offenses, felony murder laws, and others.[198]

While moral credibility's effect on compliance is recognized to be substantial, and sometimes asserted to be stronger than the effect of legitimacy,[199] the impact of procedural justice on compliance is likely at its apex in the context of compliance with secrecy laws because these laws are regulatory. Regulatory crimes, also loosely the same as

---

[195] *See* Bowers & Robinson, *supra* note 163, at 218, 259-60.

[196] *See id.* at 218.

[197] Nadler examines both unjust outcomes and unjust legislation together, describing both of them as substantive, rather than procedural, unfairness. *See* Nadler, *supra* note 179, at 1408, 1432. While this categorization is useful for Nadler's study, the two are distinct for the purposes of a procedural justice analysis because the outcomes of individual cases have been demonstrated to influence views of the procedural fairness where procedural information is unavailable. *See* discussion *supra* note 188 and accompanying text.

[198] *See* Bowers & Robinson, *supra* note 163, at 241.

[199] *See id.* at 278 (contending that even Tyler, whose work has championed procedural justice, seems to concede that moral credibility has a much greater effect in shaping compliance than does legitimacy).

crimes referred to as malum prohibitum crimes, are acts that are wrong only because the law says they are wrong.[200] By contrast, traditional crimes such as murder are considered malum in se because they are acts that are inherently morally wrong.[201] For regulatory crimes, there is typically much less consensus that the proscribed conduct itself is morally wrong, thus legitimacy is the only avenue left for the government to increase compliance.[202] The end result is that "procedural fairness is more important to the enforcement of regulatory crime, while moral credibility is more important to the enforcement of conventional crime."[203]

While it is imperative that the legitimacy scholarship not be utilized in a way that asserts causal effects without rigorous empirical study, it can still be useful in suggesting motivations for law breaking, understanding the limitations of the conclusions one might draw.[204] In the next Part, this Article does not purport to conclusively establish a causal link between legitimacy and law breaking in the case of deluge leaking. It does, however, provide strong suggestive evidence of a connection between the two, as well as setting forth a theoretical framework that could serve as the basis for future empirical research. Moreover, it forms the basis for policy considerations often absent from the current debate about national security leaks, and which, to an extent, challenge the assumption that security and transparency are at odds with one another.

IV. LEGITIMACY DEFICITS

A close analysis of our secrecy laws, including FOIA, classification standards, and whistleblower protection laws, uncovers systematic failures of administration that strongly suggest perceptions of procedural injustice and potential lack of legitimacy. This section will demonstrate that the procedures used in administering laws regulating

200 *See* Darryl K. Brown, *Criminal Law Theory and Criminal Justice Practice*, 49 AM. CRIM. L. REV. 73, 79 (2012); Ryo, *supra* note 180, at 594.

201 *See* Brown, supra note 200, at 79; Ryo, *supra* note 180, at 594.

202 *See* Bowers & Robinson, *supra* note 163, at 278 ("[L]egitimacy may be the sole effective source of any power [to prevent violations] because traditional carrots and sticks are particularly insufficient for deterring commonplace borderline crime.").

203 *Id.* at 279.

204 *See id.* at 228 ("[A]cademics should resist the temptation to rely too casually on the legitimacy project as a fulcrum to leverage idiosyncratic preferences and conceptions of what constitutes professional policing. Academics may appropriately offer policy prescriptions based on suggestive data, but they ought to acknowledge that the data is less than clear.").

government secrecy fail to effectuate some of the core elements necessary for potential deluge leakers to see the legal framework as procedurally just, suggesting that secrecy laws may suffer from a perception of illegitimacy.

A. The Freedom of Information Act

FOIA, first enacted in 1966, is the lynchpin of our legal framework governing what information remains secret and what must be disclosed.[205] It regulates the public's right to access nearly all records within the executive branch, and was designed to serve as the primary guardian of citizens' right to "know what their government is up to," a tool necessary to holding democratically elected officials accountable.[206] Unfortunately, FOIA has been riddled with problems, largely procedural, that have shaken the public confidence in its efficacy. These problems closely track the factors that have been identified as contributing to individuals' views concerning whether a process is fair: the lack of apparent neutrality of the decision-maker, the inability of stakeholders to participate in the process, and, where the process is opaque, troubling outcomes that signal procedural unfairness. These problems plague both FOIA litigation and administrative processing.

FOIA gives every person the right to inspect government records upon request, subject to only nine enumerated exemptions.[207] If a person requests information and is denied, she or he has a right to bring a lawsuit in court to challenge the denial of access.[208] The litigation then typically centers on whether the records fall within one of the enumerated exemptions to disclosure, which protect interests such as privacy, trade secrets, agency deliberations, and national security.[209] Importantly, the government bears the burden of proving

---

[205] The Freedom of Information Act, Pub. L. No. 89-554, 80 Stat. 383 (1966) (codified as amended at 5 U.S.C. § 552 (2012)).

[206] EPA v. Mink, 410 U.S. 73, 105 (1973) (Douglas, J., dissenting) (quoting Henry Steele Commager, *The Defeat of America*, THE NEW YORK REVIEW OF BOOKS, Oct. 5, 1972, at 7); *see also* 5 U.S.C. § 552 (2012); Mark Fenster, *Seeing the State: Transparency as Metaphor*, 62 ADMIN. L. REV. 617, 624 (2010) (documenting the pervasive political rhetoric that holds transparency up as a necessary component of democracy).

[207] 5 U.S.C. § 552(a), (b).

[208] *Id.* § 552(a)(4)(B).

[209] *Id.* § 552(b)(1)–(9). The full list of exemptions covers records that (1) are properly classified under an executive order, (2) are related solely to internal personnel rules, (3) are exempt from disclosure by another statute, (4) contain trade secret or confidential commercial information, (5) would be privileged in civil litigation against

that one of the exemptions applies and the court is required to review the agency's decision to withhold records de novo.[210]

While the statutory framework seems strongly protective of the public's rights, judges in FOIA cases have engaged in practices that may appear to the public to be biased in favor of the government. In particular, judges have altered the standard of review, openly applying a strong form of deference to the government's position in litigation, particularly under certain exemptions.[211] This practice occurs despite Congress's clear intent that the de novo review standard protect against undue government secrecy.[212] Having one standard articulated in the law and another used in practice has the potential to undermine litigants' confidence that judges are treating their case fairly, thereby implicating a central procedural justice concern: the neutrality of the decision-maker.[213]

National security is one area in which this deference is pervasive, and the ramifications for litigants are perhaps the clearest. The language of the original 1966 Act exempted records "specifically required by Executive order to be kept secret in the interest of the national defense or foreign policy."[214] In 1973, the Supreme Court in *EPA v. Mink* held that de novo review of an agency's decision to withhold records under this provision would only reach whether the withheld records were in fact classified, but not whether the classification was proper under the relevant executive order.[215] This decision had the effect of providing complete judicial deference to the government's decision to classify records. Congress immediately viewed this decision as contrary to its intent in providing for de novo review, and amended FOIA in 1974 (even overriding President Gerald Ford's veto) to change the language of the exemption to cover records "specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and . . . [which] are in fact properly classified pursuant to such

the agency, (6) would cause an unwarranted invasion of personal privacy, (7) are law enforcement records the release of which would cause certain harms, (8) pertain to certain banking matters, and (9) concern the location of wells. *Id.*

210 *Id.* § 552(a)(4)(B).

211 *See* Margaret B. Kwoka, *Deferring to Secrecy*, 54 B.C. L. REV. 185, 211-20 (2013) [hereinafter *Deferring to Secrecy*].

212 *Id.* at 198.

213 *See supra* notes 187–88 and accompanying text.

214 EPA v. Mink, 410 U.S. 73, 81 (1973), *superseded by statute*, Act of Nov. 21, 1974, Pub. L. 93-502, 88 Stat. 1561, *as recognized in* CIA v. Sims, 471 U.S. 159 (1985).

215 *Id.*

Executive order."[216] It further added a provision authorizing courts to review records in camera.[217] These provisions made clear that courts were to review de novo not only the fact of classification, but also the propriety of classification under the criteria in the executive order.

Nonetheless, courts today are near unanimous in their declaration that they "accord substantial deference to the [agency's] determination that information must be withheld" because it is classified.[218] In fact, the deference is nearly complete: one study found no successful challenge to a national security withholding under FOIA over a ten-year period in the 1990s.[219] A Department of Justice ("DOJ") report could not identify a single example of a successful challenge to the national security exemption claim that withstood appeal.[220] The Justice Department has even admitted that under FOIA, "courts generally have heavily deferred to agency expertise in national security cases."[221] Judges can easily appear biased to litigants and to the public when they give strong, even conclusive, deference to the government despite Congress's clear mandate for stringent review.[222] Even if the courts have benign subjective reasons for their actions,[223] the impact on the public is one of perception,[224] and that perception is likely to undermine a belief in the procedural fairness of decisions under FOIA and, ultimately, the legitimacy of FOIA itself.[225]

---

216 5 U.S.C. § 552(b)(1) (2012).

217 *Id.* § 552(a)(4)(B).

218 Maynard v. CIA, 986 F.2d 547, 555-56 (1st Cir. 1993); *see also* Kwoka, *Deferring to Secrecy*, *supra* note 211, at 214-15.

219 *See* Paul R. Verkuil, *An Outcomes Analysis of Scope of Review Standards*, 44 WM. & MARY L. REV. 679, 714-15 (2002).

220 *See* U.S. DEP'T OF JUSTICE, FREEDOM OF INFORMATION ACT GUIDE 211, 211 fn. 56, 212 (2007).

221 U.S. DEP'T OF JUSTICE, GUIDE TO THE FREEDOM OF INFORMATION ACT 147 (2009), *available at* http://www.justice.gov/oip/foia_guide09/exemption1.pdf.

222 *Cf.* Meredith Fuchs, *Judging Secrets: The Role Courts Should Play in Preventing Unnecessary Secrecy*, 58 ADMIN. L. REV. 131, 176 ("All too often, courts easily accept the argument that the executive needs unquestioning adherence to its judgments and that the court is not competent to assess those judgments in the realm of national security.").

223 *See* Margaret B. Kwoka, *Deference, Chenery, and FOIA*, 73 MD. L. REV. 1060, 1071 (2014).

224 Moreover, national security is not the only context in which this occurs: courts have openly deferred to the government's position on central questions under other exemptions as well, most notably deferring to the government's representation the records are created for law enforcement purposes under exemption 7 and to the government's representations about its own decision-making process under exemption 5. *See* Kwoka, *Deferring to Secrecy*, *supra* note 211, at 216-22.

225 *See supra* notes 187–88 and accompanying text.

Perhaps even more troubling is a set of procedures courts use to decide all FOIA cases — no matter the exemption claimed — that deviate from typical litigation procedures. These procedures have the effect of giving the government advantages by cutting off the procedural rights of plaintiffs that are normally available.[226] This collection of practices, in effect, curtails FOIA plaintiffs' opportunities to participate and be heard in FOIA litigation, directly affecting another central factor — participation — that contributed to low views of legitimacy in procedural justice studies.[227]

The first procedural deviation in FOIA litigation concerns discovery. Discovery opportunities typically afforded to litigants in other cases are routinely denied to plaintiffs in FOIA cases.[228] Just as in other civil cases, FOIA cases often turn on factual disputes, about which parties would benefit from discovery.[229] The need for discovery is particularly true for the plaintiff in a FOIA case, because the agency almost always has all the relevant evidence. Outside the FOIA context, litigants use discovery to gather the evidence necessary to prove or defend the case. In FOIA cases, however, courts refuse to allow discovery as a matter of routine.[230] Instead, courts have developed a FOIA-specific procedure known as the Vaughn Index, which is a specialized affidavit required of the government in most FOIA cases listing each withheld record, the claimed exemption, and the basis for the claim.[231] In practice, Vaughn Indices are rarely of much help to the requester because they contain very little detail and are not subject to any subsequent testing for veracity, for instance by deposing the declarant.[232]

The justification offered for departing from the trans-substantive nature of civil litigation's procedural rules in FOIA cases has been that traditional discovery is simply unworkable because there is an

[226] For a full accounting of this so-called unspoken deference and its origins, see Kwoka, *Deferring to Secrecy*, *supra* note 211, at 221-35.

[227] *See supra* notes 187–88 and accompanying text.

[228] Discovery is presumptively available under the Federal Rules of Civil Procedure. *See* FED. R. CIV. P. 26–37.

[229] *See* Margaret B. Kwoka, *The Freedom of Information Act Trial*, 61 AM. U. L. REV. 217, 234-43 (2011) [hereinafter Kwoka, *The Freedom of Information Act Trial*] (detailing the types of factual disputes that commonly arise in FOIA cases). These disputes often center not on the contents of the requested records, but on external issues such as how the records were used, whether they were shared outside the agency, or whether their release would cause a particular kind of harm. *See id.*

[230] *See* Wheeler v. CIA, 271 F. Supp. 2d 132, 139 (D.D.C. 2003) ("Discovery is generally unavailable in FOIA actions.").

[231] *See* Vaughn v. Rosen, 484 F.2d 820, 824 (D.C. Cir. 1973).

[232] *See* Kwoka, *Deferring to Secrecy*, *supra* note 211, at 223.

inherent information imbalance in FOIA litigation that is not present in other cases.[233] As I have argued elsewhere, that justification is unwarranted.[234] Not only does this judicial practice adversely affect litigation outcomes for FOIA requesters, it also cuts off the ability of the litigants to participate in their own case by gathering the evidence they need to mount their arguments. This is precisely the kind of denial of participation that leaves individuals feeling the process has been unfair: they are, in effect, litigating with one hand tied behind their back.

Another procedural departure in FOIA cases is courts' misuse of the summary judgment standard to dispose of nearly all FOIA cases, regardless of whether there are material factual disputes.[235] This practice is not only contrary to the Rule 56 summary judgment standard used in other cases,[236] but it also has the effect of systematically hurting requesters by cutting off their ability to be heard.[237] In effect, it denies requesters the ability to orally argue before a judge, including to answer questions or concerns the judge may have, to cross-examine witnesses, and to expose weaknesses in the government's case.[238] Trials are held up as the gold standard of dispute resolution, and they are categorically unavailable for FOIA cases. The practice of deciding all cases on summary judgment also may create a perception that FOIA procedures are fundamentally unfair by failing to give FOIA plaintiffs the same opportunities to be heard as are available to other litigants.[239]

While average members of the public may not be aware of the procedural injustices of FOIA litigation that might contribute to a legitimacy deficit, potential deluge leakers in all probability have experiences — personal or vicarious — that would inform their perception. Potential deluge leakers are insiders, because they are

---

233 *See Vaughn*, 484 F.2d at 824.

234 *See* Kwoka, *Deferring to Secrecy*, *supra* note 211, at 222-28.

235 *See* Kwoka, *The Freedom of Information Act Trial*, *supra* note 229, at 244-61.

236 *See* FED. R. CIV. P. 56.

237 Kwoka, *The Freedom of Information Act Trial*, *supra* note 229, at 264-67, 273-76 (using interviews with lawyers who have litigated FOIA trials and empirical evidence to demonstrate that plaintiffs may fare better at trial than at the summary judgment stage).

238 *See id.* In addition, my previous work demonstrated that when the government loses a summary judgment motion, courts grant it a second chance at summary judgment, rather than ordering the case to trial or ruling for the plaintiff. This, too, has the effect of cutting off plaintiffs' procedural rights. *See* Kwoka, *Deferring to Secrecy*, *supra* note 211, at 231-35.

239 *See supra* notes 187–88 and accompanying text (noting the importance of being heard as a factor determining the perception of procedural justice).

government employees or contractors with access to government secrets. They are more likely to know about or be involved in helping to respond to FOIA litigation brought against the agency they work for by the nature of their positions.

Finally, even those potential deluge leakers without knowledge about FOIA litigation procedures may at least generally know that agencies overwhelmingly prevail. While most agency actions challenged in court are affirmed about 60% to 70% of the time, in FOIA cases the agency's withholding of requested information is affirmed a full 90% of the time.[240] Thus, the agency win rate in FOIA cases is significantly higher even though agencies are supposedly subject to a tougher standard of review than the deferential treatment they enjoy in other types of litigation. This agency win rate produces a palpable sense that the deck is stacked in favor of the agency. Thus, for those without experience with FOIA litigation procedures, they are likely to use these very lopsided outcomes as a proxy for measuring the fairness of FOIA litigation and conclude that the FOIA litigation process is unjust, thereby decreasing FOIA's legitimacy.[241]

Litigation under FOIA is not the only contact point with FOIA laws. Administrative processing of FOIA requests, and the resulting administrative decisions to release or withhold requested records, form another source of information about the legitimacy of FOIA. Here, too, however, there are ample bases for the public and government employees alike to question FOIA's procedural fairness. For one, agencies undermine the legitimacy of FOIA as a transparency tool by consistently violating the statutory deadlines for responding to FOIA requests. Under FOIA, agencies must respond to requests within twenty business days,[242] but in practice, agencies often surpass that deadline even for simple requests and far exceed it for complex inquiries, with the worst of the agencies clocking in at an average of 917 days.[243] In 2007, Congress declared that "[c]hief among the

[240] *See* Verkuil, *supra* note 219, at 713 (reporting the 90% affirmance rate in FOIA cases); David Zaring, *Reasonable Agencies*, 96 VA. L. REV. 135, 169 (2010) (reporting affirmance rates in agency cases as typically falling between 60% and 70%).

[241] *See supra* notes 187–88 and accompanying text (explaining that where processes are opaque, individuals often use outcomes as a proxy for determining if the process was fair).

[242] 5 U.S.C. § 552(a)(6)(A)(i) (2012).

[243] U.S. DEP'T OF JUSTICE, OFFICE OF INFO. POLICY, SUMMARY OF ANNUAL FOIA REPORTS FOR FISCAL-YEAR 2012, at 10-11, *available at* http://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/fy2012-annual-report-summary.pdf. In fiscal year 2012, the DOJ reported an average processing time of 22.66 days for simple requests across the government, and also reported that 22 agencies' averages exceeded 30 days.

problems with FOIA are the major delays encountered by FOIA requestors,"[244] and in 2014 the Associated Press reported that most agencies took longer to answer FOIA requests than the previous year.[245] An obvious failure of the government to follow a basic procedural requirement of FOIA is likely to have an impact on the statute's perceived legitimacy.

In addition, evidence suggests that requesters are frustrated in their dealings with agency FOIA staff. Congress took up this issue in the most recent significant amendments to FOIA, enacted in 2007, by requiring each agency to have a FOIA Public Liaison responsible for improving agency communication with requesters.[246] Anecdotal evidence suggests that communication with FOIA staff continues to try requesters' patience. For instance, one organization reported that an agency responded to its request for a single document with an acknowledgement letter that classified the request as "complex," a tracking designation that affects where the request will fall in the queue.[247] When the organization pointed out that the request was hardly complex, as it sought a single identifiable document, the FOIA officer represented that the letter was simply the agency's standard response to all requests.[248] In sum, the requesters' dealings with FOIA staff do not encourage requesters to feel as if they have been heard and treated respectfully, concerns that have been demonstrated to affect individuals' perception of the legitimacy of laws.[249]

Finally, in agency processing, reliance on exemptions to withhold information is on the rise: 2013 saw a record number of denials of information, and more than double the number of withholdings based on national security as compared to 2009.[250] Thus, individuals looking at FOIA outcomes at the administrative level also have reason to believe that FOIA processing is leading to more and more secrecy, and may lack the perception of legitimacy as a result.

Id. at 10. For complex requests, the government-wide average was 82.35 days. *Id.*

[244] *See* S. REP. NO. 110-59, at 3 (2007).

[245] Ted Bridis & Jack Gillum, *US Cites Security More to Censor, Deny Records*, ASSOCIATED PRESS (Mar. 16, 2014, 2:55 PM EDT), http://bigstory.ap.org/article/us-cites-security-more-censor-deny-records.

[246] OPEN Government Act of 2007, S. 2488, 110th Cong. § 10 (2007).

[247] *A Call with the Department of Defense*, OPENTHEGOVERNMENT.ORG (Oct. 17, 2012), http://managingfoia.wordpress.com/2012/10/17/a-call-with-the-department-of-defense/.

[248] *Id.*

[249] *See supra* notes 187–88 and accompanying text.

[250] Bridis & Gillum, *supra* note 245.

B. Classification

Much like FOIA, the federal government's classification system regulates what information it discloses and what remains secret. The standards for classifying information are governed by executive order and have remained relatively constant between administrations.[251] Information can be classified at one of three different levels — top secret, secret, or confidential — based on the severity of harm to national security that would result from release, and all such records must pertain to a topic listed in the executive order, which includes subject matter such as military operations, foreign government information, intelligence activities, and nuclear materials.[252] Classification is further limited insofar as officials must be able to identify and describe the harm that would result from release, and they may not classify records to conceal wrongdoing or prevent embarrassment.[253]

While these substantive standards for classification seem relatively constrained, like with FOIA, there are significant procedural deficiencies in the classification system that may undermine confidence in the system and potential deluge leakers' view of its legitimacy. First, because of a two-tiered system for designating classified information, the total number of individuals with authority

[251] To be sure, President Obama's executive order on classification, issued in 2009, limited classification in a few respects. Exec. Order No. 13,526, 3 C.F.R. 298 (2009), *available at* http://www.gpo.gov/fdsys/pkg/CFR-2010-title3-vol1/pdf/CFR-2010-title3-vol1-eo13526.pdf. For instance, President Obama required that records not be classified if there was significant doubt about the need for secrecy. *Id.* § 1.1(b), 3 C.F.R. at 298.

[252] *See id.* § 1.2(a), 3 C.F.R. at 298-99; *id.* § 1.4, 3 C.F.R. at 300. The full list of categories includes:

> (a) military plans, weapons systems, or operations;
> (b) foreign government information;
> (c) intelligence activities (including covert action), intelligence sources or methods, or cryptology;
> (d) foreign relations or foreign activities of the United States, including confidential sources;
> (e) scientific, technological, or economic matters relating to the national security;
> (f) United States Government programs for safeguarding nuclear materials or facilities;
> (g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or
> (h) the development, production, or use of weapons of mass destruction.

Id.

[253] *See id.* § 1.7, 3 C.F.R. at 302-03.

to classify records is incredibly high. The first tier of the system consists of "original classifiers," a relatively small group of very senior officials authorized in the first instance to designate information at any level of classification.[254] The problem lies in the second tier, the practice of "derivative classification" through which anyone with authorization to access classified materials — now totaling almost five million individuals[255] — can designate as classified new records that incorporate, paraphrase, or restate information that was originally classified.[256] While original classification decisions have been decreasing in number in the last decade (the last reported annual total standing at 73,477 original classification designations), the far-reaching derivative classification authority has led to an exponential increase in such designations, last reported as 95,180,243 in one year.[257] Alone, this incredibly high rate of classification decisions may justifiably contribute to a perception that the process of classification is unfairly skewed toward secrecy and thus illegitimate.[258]

Procedural problems also, however, abound, about which potential deluge leakers — themselves by definition with access to classified records and therefore familiar with the classification system — would be aware. Reports have noted that lower-level government officials tend to err on the side of classification for a variety of reasons, including a culture of secrecy in government agencies, a desire to hide government misconduct or incompetence, a perceived need to make policy quickly and without the hindrance of public debate, and a risk-averse fear of negative consequences for mistakenly releasing sensitive information.[259] In contrast to the sometimes serious consequences for wrongly releasing information to the public, there are no meaningful consequences for wrongly keeping information secret: internal checks are next to nonexistent; Congress cannot oversee day to day matters; and the public is unable to use FOIA as a meaningful check on

---

[254] NAT'L ARCHIVES & RECORDS ADMIN., INFO. SEC. OVERSIGHT OFFICE, ANNUAL REPORT TO THE PRESIDENT 2 (2012) [hereinafter ISOO REPORT], *available at* http://www.archives.gov/isoo/reports/2012-annual-report.pdf. In fiscal year 2012, there were only 2,326 original classifiers. *Id.*

[255] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *supra* note 192, at 3.

[256] ISOO REPORT, *supra* note 254, at 7.

[257] *Id.* at 5, 8.

[258] *See supra* notes 187–88 and accompanying text.

[259] ELIZABETH GOITEIN & DAVID M. SHAPIRO, BRENNAN CTR. FOR JUSTICE, REDUCING OVERCLASSIFICATION THROUGH ACCOUNTABILITY 21 (2011), *available at* http://www.brennancenter.org/sites/default/files/legacy/Justice/LNS/Brennan_Overclassification_Final.pdf; *see also* Bellia, *supra* note 26, at 1520; Papandrea, *supra* note 10, at 474 (citing a "culture of caution").

national security secrecy, as discussed above.[260] Moreover, overclassification becomes a self-fulfilling prophecy: classifying so much information means that many more government employees need access to classified information to do their jobs, thereby expanding the pool of people with access, and thus the pool of people who have derivative classification authority, and then in turn the number of new documents that will be designated as classified.[261] All of these factors could contribute to a perception by would-be deluge leakers that the decision-makers — the classifiers themselves — are not acting in an unbiased fashion because they are heavily incentivized toward unnecessary secrecy, thereby calling into question a central element of procedural justice.[262]

Not only are incredibly vast swaths of government information classified, but those designations, once made, are difficult to remove even when the threat to national security has ended. Again, procedural issues constitute the central problems. Formally, every classification designation must be assigned a sunset provision, a time at which the information will be "automatically" declassified. The first difficulty comes with the time frames themselves: though the original classifier must specify a declassification date of ten years or less unless certain findings are made requiring a longer time period,[263] in the last reported year, 52% of classification designations were for more than ten years.[264] The ultimate difficulty, though, is that "automatic" declassification at the date specified is actually not automatic, because agencies still undertake individual review and only the originally classifying agency can declassify a document, thereby leading to lengthy consultations between agencies.[265] The other avenues to

[260] Fuchs, *supra* note 222, at 148-51.

[261] *See* GOITEIN & SHAPIRO, *supra* note 259, at 9 (citing overclassification as the reason that so many people now have security clearances to access classified information).

[262] *See supra* notes 187–88 and accompanying text.

[263] Exec. Order No. 13,526, § 1.5(b), 3 C.F.R. 298, 300-01 (2009), *available at* http://www.gpo.gov/fdsys/pkg/CFR-2010-title3-vol1/pdf/CFR-2010-title3-vol1-eo13526.pdf (specifying that the sunset date must be 10 years or less "unless the original classification authority otherwise determines that the sensitivity of the information requires that it be marked for declassification for up to 25 years from the date of the original decision"). President Obama's executive order for the first time specifies that in no case can a designation be indefinite. *Id.* § 1.5(d), 3 C.F.R. at 301.

[264] *See* ISOO REPORT, *supra* note 254, at 6.

[265] GOITEIN & SHAPIRO, *supra* note 259, at 17; *see also* Herbert Briick, *Simplifying the Declassification Review Process for Historical Records*, NAT'L ARCHIVES TRANSFORMING CLASSIFICATION BLOG (Mar. 29, 2011), http://blogs.archives.gov/transformingclassification/?p=110.

declassification fail to make a meaningful impact on the problem of overclassification either because, in the case of requests by members of the public for declassification review of certain documents, the process is infrequently used,[266] or because, in the case of FOIA requests, they are infrequently successful.[267]

Thus, while the executive order standards seem to set boundaries on the practice of classification,[268] the procedures for implementing those standards result in vast numbers of classified records, and very little effective declassification once the need for secrecy is over, representing a "persistent gap between written regulation and actual practice."[269] The problem of overclassification has been recognized across the political spectrum, and has been acknowledged in countless studies including those coming from within the government.[270] Senior government officials have estimated that between 50% and 90% of classified material should not be so designated.[271] Striking examples of classification decisions that obviously do not implicate national security concerns have been widely reported.[272] As such, it is fair to

[266] This process, known as Mandatory Declassification Review ("MDR"), is relatively successful when used, but is used relatively infrequently as compared to the number of classified records. In FY 2012, only 7,589 MDR requests were made concerning a total of 372,354 pages of records. ISOO REPORT, *supra* note 254, at 15. Of those, 58.4% were declassified in their entirety, and an additional 23.3% were declassified in part. *Id.*; *see also* Papandrea, *supra* note 10, at 472 (noting that the appeals body for mandatory declassification review, the Interagency Security Classification Appeals Panel, lacks sufficient staff to handle the demands of MDR requests).

[267] Challenges to national security withholdings are essentially never successful in litigation. *See* discussion *supra* note 218–21 and accompanying text; *see also* GOITEIN & SHAPIRO, supra note 259, at 18-19 ("FOIA challenges have proven to be far less effective than MDR, however, in obtaining the declassification and release of classified information.").

[268] To be sure, reforms on the substantive standards for classification have also been proposed. *See, e.g.*, Papandrea, *supra* note 10, at 477 (noting the classification standard would be improved by requiring a weighing of the public interest in knowing the information). Nonetheless, as described in this section, procedural concerns remain at the forefront.

[269] GOITEIN & SHAPIRO, *supra* note 259, at 2.

[270] *See id.* at 1-2 (documenting a history of government studies and high-level officials from both Democratic and Republic administrations to admit to the problem of overclassification).

[271] *Espionage Act and the Legal and Constitutional Issues Raised by WikiLeaks: Hearing Before the H. Comm. on the Judiciary*, 111th Cong. 17 (2010) (statement of Tom Blanton, Dir., Nat'l Sec. Archive) [hereinafter *Espionage Act Hearing*].

[272] *See* GOITEIN & SHAPIRO, *supra* note 259, at 4-6 (collecting examples). In a particularly ironic example, a volume of the Pentagon Papers, all of which were classified, was revealed to contain nothing but already public statements of Presidents

say that the perception of an overclassification problem is so widespread that, even if would-be deluge leakers did not understand the details of the classification process, they would have a basis for concluding that the process is broken because of the results it produces.[273]

While no one has to date invoked a procedural justice framework for understanding the link, many have articulated a connection between overclassification and national security leaks, including recent deluge leaks. Professor Bellia notes that overclassification contributes to the sheer volume of information that may be subject to a leak.[274] A recent report by the Brennan Center is even more explicit: "Unnecessary secrecy . . . threatens national security by undermining respect for the classification system and thereby promoting leaking by government officials."[275] Justice Potter Stewart succinctly made the case in the Pentagon Papers case:

> For when everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self-protection or self-promotion. . . . [T]he hallmark of a truly effective internal security system would be the maximum possible disclosure, recognizing that secrecy can best be preserved only when credibility is truly maintained.[276]

More than just assertions or speculations, the procedural justice literature provides a tested theoretical basis on which the problem of overclassification can be linked to leaking. First, the procedures by which information is classified, which lend themselves to overclassification, and the procedural difficulties in declassification may form the basis for people familiar with classification to discount the legitimacy of the classification authority.[277] Would-be deluge leakers are among the most likely to have intimate knowledge of the classification process, as they have security clearances. Second, even

John F. Kennedy and Lyndon B. Johnson. *See* Bellia, *supra* note 26, at 1519-20.

[273] *See supra* notes 187–88 and accompanying text.

[274] Bellia, *supra* note 26, at 1519.

[275] GOITEIN & SHAPIRO, *supra* note 259, at 8; *see also Espionage Act Hearing*, *supra* note 271, at 3 (statement of Tom Blanton, Dir., Nat'l Sec. Archive) ("The only remedies that will genuinely curb leaks are ones that force the government to disgorge most of the information it holds rather than hold more information more tightly.").

[276] N.Y. Times Co. v. United States, 403 U.S. 713, 729 (1971) (Stewart, J., concurring).

[277] *See supra* note 187 and accompanying text.

those who do not know the process well may use the visible outcomes of the classification process — including the widespread consensus that overclassification is rampant — to conclude that those procedures are not fair.[278] As is the case with FOIA, the standards on the books are subject to less critique than the process of implementing them and rendering individual secrecy decisions, a process that may well seem unjust and illegitimate.

C. Whistleblower Protections

The final central component of government secrecy laws is the set of protections extended to whistleblowers. In this area, Congress has attempted to ensure that government employees can come forward to report incidents of misconduct. But again, the procedures are so lacking that the whistleblower laws have come under intense criticism as failing to effectuate that goal. The failings of these processes, as with the other secrecy laws, implicate important procedural justice concerns.

The centerpiece of whistleblower protections for federal employees is the Federal Whistleblower Protection Act ("WPA"), but that Act does not cover employees of the Federal Bureau of Investigation, the Central Intelligence Agency, the Defense Intelligence Agency, and the National Security Agency, among other national security related government workers,[279] and it does not protect disclosures of classified national security information.[280] Instead, the Intelligence Community Whistleblower Protection Act ("ICWPA") applies to national security whistleblowers, and it authorizes employees to report matters of "urgent concern," defined as a "serious or flagrant" violation of the law or executive order, a false statement to Congress, or reprisal against a person who reported a matter of urgent concern.[281]

As with FOIA and classification, the process that the ICWPA requires national security whistleblowers to follow lends itself to procedural critique. First, employees must disclose the information to the agency's Inspector General, who then must determine if the complaint or information is credible, and in turn must notify the head of the agency of the complaint as well as the determination on

[278] *See supra* note 188 and accompanying text.

[279] 5 U.S.C. § 2302(a)(2)(C)(ii) (2012).

[280] *Id.* § 2302(b)(8)(A).

[281] 50 U.S.C. § 403q(d)(5)(G)(i) (2012). This protection is certainly much narrower substantively than the coverage of the Federal Whistleblower Protection Act, which reaches reports of any violation of the law, instance of mismanagement of waste, or threat to public health or safety. *See* 5 U.S.C. § 2302(b)(8)(A)–(B).

credibility.[282] Only if the Inspector General does not find the complaint or information credible can the employee make a report to congressional intelligence committees, and only then after notifying the Inspector General and receiving instructions on how to contact Congress.[283] Critically, the decision of the Inspector General is expressly unreviewable,[284] and disclosure to the intelligence committees may not produce any actual oversight. There is nowhere else for the whistleblower to turn beyond this narrow path.[285]

Perhaps the biggest procedural failure of the ICWPA is that it authorizes this reporting procedure, but, unlike the WPA, does not prohibit retaliation against an employee who uses the procedure, nor does it provide any remedy for such an aggrieved employee.[286] Accordingly, it has been snubbed as a "misnamed" statute[287] since it "arguably fails to provide any real protection to national security whistleblowers."[288] Furthermore, creating a right to report without an adequate process for vindicating the right is a recipe for failure, and the numbers of reporting incidents confirms that fact. According to the Project on Government Oversight, an independent watchdog group, there are no known successful whistleblowing instances from FBI employees, and fewer than ten CIA employees over a seven-year period used the system to report concerns of which only one ended in an inspector general recommendation for corrective action.[289]

---

[282] 50 U.S.C. § 403q(b).

[283] *Id.* § 403q(d)(1)–(2).

[284] *See id.* § 403q(d)(3).

[285] Inspectors General themselves have come under attack as insufficiently effective. *See* Ed O'Keefe, *Difficulty Contacting Inspectors Lets Waste and Abuse Go Unchecked, Report Says*, WASH. POST, Mar. 23, 2009, at A13 ("Federal inspectors general too often ignore or discount the complaints of whistleblowers, and concerned citizens attempting to report government waste or mismanagement may face difficulty making even basic contact with the offices via telephone or the Internet.").

[286] Papandrea, *supra* note 10, at 493.

[287] Robert J. McCarthy, *Blowing in the Wind: Answers for Federal Whistleblowers*, 3 WM. & MARY POL'Y REV. 184, 196 n.79 (2012).

[288] Papandrea, *supra* note 10, at 493. Even under the comparatively robust WPA, the designated reporting entity, the Office of Special Counsel, closes the vast majority of reports without any investigation, and about half of federal employees who blew the whistle reported negative consequences, including threats and acts of reprisal. McCarthy, *supra* note 287, at 192-93. Those who report to OSC are "overwhelmingly dissatisfied" with the response. *Id.* at 194. For these reasons, only about 10% of employees who observe reportable activities actually report. *Id.* at 191.

[289] Danielle Brian, Exec. Dir., Project on Gov't Oversight, Testimony Before the Senate Homeland Security and Governmental Affairs Committee on S. 372: The Whistleblower Protection Enhancement Act of 2009 (June 11, 2009), *available at* http://www.pogo.org/our-work/testimony/2009/wi-wp-20090611.html.

Anecdotal experience of recent national security whistleblowers confirms the procedural difficulties of working within the system, and the wide reporting of these stories may form the basis for others' beliefs in the illegitimacy of whistleblower protection laws. Indeed, would-be whistleblowers became leakers as their efforts to blow the proverbial whistle through official channels failed. For instance, Thomas Drake, a former senior executive at the NSA, became concerned about Trailblazer, a post-9/11 program designed to fund private contractors to build new surveillance tools, which Drake believed was riddled with waste and corruption.[290] Drake first tried to take his complaints to a member of the House Intelligence Committee who oversaw the agency's budget, but his attempt to work within the system produced no results.[291] He then went to the press, and, without leaking any classified documents, simply told a reporter at *The Baltimore Sun* about the waste he had witnessed.[292] Despite the care he took, he was prosecuted and pled guilty under the Espionage Act for the act of illegally taking classified papers from his office to his home.[293]

In another striking example, Robert MacLean, a former Federal Air Marshal, was alarmed when he learned that the Department of Homeland Security ("DHS") was canceling a plan to deploy air marshals on certain overnight flights despite an ongoing hijacking threat.[294] MacLean first went to his supervisor, who cited a budget shortfall but did not take any action, and then he went to the Inspector General's office, where he was advised to "walk away" rather than risk his career.[295] He then decided he had to protect public safety by going to the press.[296] His leak prompted outrage from Congress, and led to DHS changing its position and reinstating air marshal coverage.[297] MacLean, however, was fired from his position and fought his case all the way to the Supreme Court before finally winning protected whistleblower status.[298] These stories have been widely

[290] *See* GREENBERG, *supra* note 14, at 221.

[291] *Id.* at 222. Drake did not go through clearance process with the IG before going to Congress, as required by the ICWPA. Jane Mayer, *The Secret Sharer: Is Thomas Drake an Enemy of the State?*, NEW YORKER (May 23, 2011), http://www.newyorker.com/magazine/2011/05/23/the-secret-sharer [hereinafter *The Secret Sharer*].

[292] GREENBERG, *supra* note 14, at 222; Mayer, *The Secret Sharer*, *supra* note 291.

[293] GREENBERG, *supra* note 14, at 223-24.

[294] Brief in Opposition to Certiorari at 9, Dep't of Homeland Sec. v. MacLean, 134 S. Ct. 2290 (2014) (No. 13-894), 2014 WL 1275196.

[295] *Id.* at 9-10.

[296] *Id.* at 10.

[297] *Id.*

[298] *See* Dep't of Homeland Sec. v. MacLean, 135 S. Ct. 913, 918, 924 (2015). The

reported in the press, along with many others. The perception of whistleblower laws as failing to offer meaningful processes for blowing the whistle or to secure protections for those who do may undermine employees' belief in the legitimacy of these laws.

While there certainly have been legitimate critiques and proposed reforms concerning the substantive standards for our government secrecy laws, it is striking that in each of the main legal areas, procedural problems dominate the discussion. Analyzing the procedural defects in these three areas together makes clear that the processes collectively fail, in the context of secrecy laws, to adequately assure some of the key protections that inform the public's view about fairness: unbiased decision-makers, the ability to participate in the process, and courteous treatment. Moreover, the outcomes of these processes are so skewed that even those not familiar with the procedural problems may use those outcomes as a proxy to form a conclusion that the processes are not fair. In sum, the perception of procedural justice in this area may be unfavorable, potentially significantly undermining the legitimacy of secrecy laws themselves.

V. DELUGE LEAKS AS SELF-HELP

The many deep flaws in our secrecy laws — mainly resulting from procedural failures — combined with sociological research demonstrating that procedural justice influences individuals' compliance with the law suggests that government employees and contractors who violate anti-leaking laws may be influenced by their perception that formal mechanisms for governmental accountability lack legitimacy. This section hones that analysis to a particular type of government employee, contractor, and leak facilitator: the deluge leaker. Two types of evidence demonstrate that the recent deluge leaks have been uniquely motivated by this perception: the inferences that can be drawn from the documented actions of recent deluge leakers and the stated motivations of those leakers.[299] Both types of evidence indicate that the lack of legitimacy in transparency laws contributed to decisions to deluge leak.

Court ruled that whistleblower laws protect an employee who discloses information that is not classified or protected by statute, but rather is only made secret under an agency regulation. *See id.* at 921.

[299] By definition, there are not many people in the category of deluge leakers. Accordingly, even if access to them were unfettered such that survey or interview data could be had, it would be difficult to gather enough meaningful data to study deluge leakers' reasons for breaking anti-leaking laws empirically.

A. Actions of Deluge Leakers

Actions, as the saying goes, speak louder than words. There are several types of actions that evidence the choices made by deluge leakers and their publishers. These choices, in turn, permit inferences about these actors' motivations. First, the scope of the material these actors decided to disclose reveals important information about their motivations. Second, the type of material they decided to withhold from public view also indicates what objectives they had. And third, the choices of other actors within their network who, while they had the opportunity, decided not to engage in deluge leaking are also telling. The bulk of all of this evidence suggests that recent deluge leakers may be influenced by the lack of legitimacy in formal secrecy laws, rather than merely whistleblower protests against certain government actions or a desire to engage in destructive activity.

The scope of deluge leaks itself is the single strongest piece of evidence that deluge leakers are motivated by their perception that secrecy laws lack legitimacy. The actions of deluge leakers are distinct from traditional whistleblower leakers. Certainly, some subset of the leaked records in recent deluge leaks were tied to government actions the leakers believed were illegal or improper, but the scope of the leaks went far beyond records that fit that description. The fact that leaked material includes voluminous records not implicated in any particular objectionable governmental action shows that the purpose of the leak is more than mere whistleblowing (even if that is one of the motivations), but also an action of protest against government secrecy or demonstration of the need for greater transparency.

WikiLeaks's activities prior to Manning's leaks demonstrate its broader purpose in protesting excessive secrecy, rather than just exposing wrongdoing. For instance, Julian Assange at one point sought to publicize a leaked copy of a U.K. counter-insurgency manual.[300] At another point, he tried to interest the media in a set of emails, numbering in the thousands, between President Hugo Chávez of Venezuela and a speechwriter.[301] Reporters who have worked closely with Assange describe WikiLeaks's early activities as "posting long lists of raw and random documents . . . ."[302] As such, WikiLeaks was not designed only to expose illegal or immoral conduct; it was designed to expose secrets.

---

300 LEIGH & HARDING, *supra* note 7, at 60.

301 *Id.*

302 *See id.* at 61.

Manning's leaks, facilitated by WikiLeaks, demonstrate the same properties. While certain of her leaks were clearly meant to expose a particular instance of governmental wrongdoing, such as the so-called Collateral Murder video,[303] many thousands of records were released without regard to whether they showed wrongdoing. For instance, in the first mass release, Manning, through WikiLeaks, disclosed 92,201 hour-by-hour field reports from the war in Afghanistan, and shortly thereafter, over 391,000 such records from the war in Iraq.[304] Some of those individual records showed that the official accounts of certain military incidents were not accurate, and the real events disclosed much more questionable military conduct.[305] But the records Manning leaked to WikiLeaks, and that WikiLeaks gave to journalists, were not limited to those that demonstrated government misconduct or misreporting of facts; rather, the records were the complete set of war logs. Most records were unremarkable. Inevitably, for the vast majority of the records, Manning and Assange could not even have known the extent to which the contents would prove to blow the whistle on any misconduct. The time and expertise journalists brought to bear just to decipher the meaning of the records they were given further demonstrate Manning and Assange's ignorance about the documents.[306]

Even to the extent it is tempting to say the war logs collectively showed that the government misled the public about key facts of war, despite individual records not demonstrating wrongdoing, no such claim to an overall whistleblowing purpose could be made as to Manning and Assange's leak of diplomatic cables. This set of more than 250,000 cables between the State Department and U.S. embassies around the world, if printed, "would have made up a library containing more than 2,000 sizeable books."[307] That is, Manning and Assange handed over everything to which they had access, not just those records that might serve a whistleblowing purpose. Bill Keller of the *New York Times* described the effect of the cables overall:

---

303 For a description of the leak, see *supra* notes 49–50 and accompanying text.

304 LEIGH & HARDING, *supra* note 7, at 105.

305 For instance, an incident that had been publicly reported as a military airstrike in Afghanistan by Coalition forces in which seven children died was found out to have been a ground based GPS guided rocket attack executed by a somewhat-secret U.S. military task force for the purpose of executing an al-Qaeda leader who turned out to have escaped. *Id.* at 116-17.

306 *See id.* at 117 (showing that there were over 92,000 records for journalists to decipher).

307 *Id.* at 140.

> The value of these documents — and I believe they have immense value — is not that they expose some deep, unsuspected perfidy in high places or that they upended your whole view of the world. For those who pay close attention to foreign policy, these documents provide texture, nuance and drama. They deepen and correct your understanding of how things unfold; they raise or lower your estimation of world leaders. For those who do not follow these subjects as loosely, the stories are an opportunity to learn more.[308]

If Manning and Assange were only concerned with exposing misconduct or wrongdoing, these are not the actions they would have taken. Rather, these are the actions of individuals who believe the current legal mechanisms for releasing information the public are broken and produce insufficient public oversight. As an antidote, they took their own corrective actions.

Snowden's leaks are somewhat more complicated to analyze if only because we know so much less about them. The full set of records about governmental activity he took while working at Booz Allen Hamilton and turned over to reporters has not come to light; rather, a series of stories based on those records and very selected portions of them have been released.[309] The scope of the document release, however, has been described by Glenn Greenwald, one of the three reporters to whom Snowden made his initial disclosures, as "stunning in both size and scope," and that it contained "tens of thousands of NSA documents [which] had been produced by virtually every unit and subdivision within the sprawling agency" as well as some from foreign intelligence agencies.[310] Snowden himself estimated that the number of documents attributable to the British intelligence agency alone numbered 50,000 or 60,000.[311] NSA officials have estimated Snowden may have released records that number in the millions.[312]

Snowden certainly knew quite a bit about some of the material he was leaking.[313] The reporters he worked with credit him as having been organized and helping them to decipher the complex records,

---

[308] Bill Keller, *Dealing with Assange and the WikiLeaks Secrets*, N.Y. TIMES, Jan. 30, 2011, at MM32.

[309] For a list of significant stories that have come from Snowden's leak, see *supra* notes 56–60 and accompanying text.

[310] GREENWALD, *supra* note 9, at 90.

[311] LUKE HARDING, THE SNOWDEN FILES: THE INSIDE STORY OF THE WORLD'S MOST WANTED MAN 144 (2014).

[312] *See* Sanger & Schmitt, *supra* note 68, at A1.

[313] *See* GREENWALD, *supra* note 9, at 43.

especially shorthand and technical material.[314] Nonetheless, he was only working in his post at Booz Allen Hamilton, where he gained the most access to leaked materials, for less than three months when he effectuated the leak.[315] It is unimaginable that he was able to review even most of the records individually to determine their importance, choosing instead to leak huge swaths of records.

The result, like with Manning's and WikiLeaks's disclosures, was that some records were of great public importance, calling attention to questionable government behavior and thereby promoting greater oversight, while many, many others simply had little value. As Greenwald described, "dramatic revelations were mixed in with large amounts of banal or highly technical material."[316] Snowden's leaks were thus not limited to records that expose wrongdoing.

The recent deluge leakers have also engaged in some telling non-disclosures, which can shed light on their motivations. For instance, WikiLeaks withheld about fifteen thousand files from the Afghan war logs that media partners believed were too sensitive and might risk civilian informants.[317] With respect to the Iraq war documents, they were so numerous that Assange decided to redact names from the files with an automated program.[318] WikiLeaks, when it released the State Department cables, initially did so by partnering with various mainstream media outlets, mostly print newspapers, whose journalists combed through the records to redact names of people who might be harmed by the release.[319] Assange also reached out to the State Department and asked for input concerning individuals who may be "at significant risk of harm" if certain records were released, but the government refused to consult with Assange, stating, in essence, that the damage was already done by releasing the material to media outlets.[320]

---

314 *See id.* at 91.

315 Press Release, Booz Allen Hamilton, Inc., Booz Allen Statement on Reports of Leaked Information (June 11, 2013), *available at* http://www.boozallen.com/media-center/press-releases/2013/06/statement-reports-leaked-information-060913.

316 GREENWALD, *supra* note 9, at 91.

317 GREENBERG, *supra* note 14, at 295.

318 *Id.*

319 LEIGH & HARDING, *supra* note 7, at 184 (describing the redacting process for the initial stories based on the cables).

320 *See* Letter from Harold Hongju Koh, Legal Adviser, U.S. Dep't of State, to Jennifer Robinson, Attorney for Mr. Julian Assange, WikiLeaks (Nov. 27, 2010), *available at* http://media.washingtonpost.com/wp-srv/politics/documents/Dept_of_State_Assange_letter.pdf.

Certainly, there was ample room to criticize WikiLeaks's attempts at harm minimization. It has been noted that WikiLeaks's use of multiple media partners might have made it more difficult for any one outlet to self-sensor based on assessed harms.[321] Moreover, journalists from *The Guardian* who worked with Assange said he was initially opposed to any redaction, but was able to be convinced.[322] Ironically, it was the involvement of some of the journalist partners that led to the release of unredacted cables. At least one journalist himself released to others unredacted versions of the portion of the cables to which he had access.[323] The ultimate harm from the diplomatic cables, however, came from two elementary mistakes. David Leigh and Luke Harding, reporters with *The Guardian*, published a book about their work with WikiLeaks in which they printed Assange's personal password for the file containing the full set of unredacted cables.[324] This might not have mattered much, except that WikiLeaks had previously released an archive of already published material from the cables, which accidentally included an encrypted file with the unredacted versions, the key to which was Assange's password.[325] Eventually, this led to the cables being published in full, unredacted form on a third party site, and then, only once it was already accidentally public, WikiLeaks published a copy on its own site.[326]

Snowden's efforts at harm minimization were even more careful and ultimately more successful. Snowden partnered with independent journalist Glenn Greenwald, independent documentary filmmaker Laura Poitras, and *The Guardian*'s Ewan McAskill to publish articles revealing the leaked material.[327] In so doing, Snowden's express purpose was to ensure that journalists would publish only what would further the public's interest in overseeing the NSA without releasing details that would harm individuals or national security interests.[328] While some raw documents have been published alongside articles reporting on their contents, they have been comparatively rare, and no mass publication of raw NSA records ever resulted from Snowden's leak.[329]

---

321 Bellia, *supra* note 26, at 1499.

322 LEIGH & HARDING, *supra* note 7, at 111-12.

323 GREENBERG, *supra* note 14, at 262.

324 LEIGH & HARDING, *supra* note 7, at 135 (the password is the subheading of Chapter 11).

325 GREENBERG, *supra* note 14, at 305-06.

326 *Id.* at 307.

327 HARDING, *supra* note 311, at 80-82.

328 *See* GREENWALD, *supra* note 9, at 53; HARDING, *supra* note 311, at 42.

329 *See* GREENWALD, *supra* note 9, at 53 (showing the steps Snowden took to

However imperfect they sometimes were, these efforts at harm minimization demonstrate that the recent deluge leakers are not simply attempting to take down systems of governance, nor do they believe in complete unmitigated transparency. Rather, they believe our current regime fails to effectuate the public's need to know what the government is doing, and that leaks are the only recourse to give the public access to information it should have.

Also instructive is a look at those involved in the hacker movements in which Assange originated who did not seek to facilitate deluge leaks. For instance, Tim May co-founded the so-called cypherpunks, a group of technology activists committed to the creation of strong cryptography that could permit true Internet anonymity.[330] This group included Assange and others eventually involved in WikiLeaks, but was broader in nature. May was the originator of a prototype called BlackNet, a sort of precursor to WikiLeaks born of a thought experiment about the possibility of anonymous secret-spilling.[331] May demonstrated that the technology could work, but then, when he received a communication promising evidence that the CIA was trying to expose corruption in a central African country by spying on its ambassadors in Washington, D.C., he never acted to expose the secret.[332] As he describes the incident, BlackNet was created to show it was possible, but that he didn't have the "kinds of political interests" that would lead him to the actions of a transparency activist.[333] May is simply an example of a deeply libertarian person interested in technology as a source of personal freedom, but not a means to political ends.[334]

Moreover, within the hacker movement, some conduct was deemed to go "too far," demonstrating that the movement's aims were not to destroy the political system. Jim Bell proposed a tool called "Assassination Politics" in which cryptography could provide the anonymity necessary for funding through numerous small donors the professional assassination services to target anyone in the world, but most especially government employees.[335] As Bell explained his theory, "Chances are good that nobody above the level of county

publish documents journalistically).

330 *See* GREENBERG, *supra* note 14, at 81-82.

331 *Id.* at 90-91.

332 *Id.* at 91.

333 *Id.*

334 *See id.*

335 *Id.* at 119-20.

commissioner would even risk staying in office."[336] This idea of government destruction, however, proved far too much for the cypherpunks, who attacked the idea as immoral, and even led one prominent member to question cryptography altogether.[337]

Taken together, the scope of deluge leaks, the efforts at harm minimization taken by each deluge leaker, and the fellow travelers in the cypherpunk movement who declined opportunities to engage in leak promotion or publication combine to form powerful evidence that deluge leakers are motivated by a concern over broken secrecy laws. This motivation is distinct from leakers in days past, including Daniel Ellsberg, who engaged in classic whistleblowing to protest particular governmental activity, and is also distinct from anti-government activists interested in destroying the government altogether. Although concern over the legitimacy of secrecy laws may have existed before now, the technology to deluge leak did not, and deluge leaks may evidence the first time leakers have had the ability to take actions that directly react to the legitimacy of government secrecy laws.

B. Stated Goals of Deluge Leakers

The second available type of evidence of recent deluge leakers' motivations are their own words. Each of the recent deluge leaks has been accompanied by various types of statements, including at various times public representations contemporaneously with the leaks, statements to the press after the leaks, and statements in judicial proceedings.

To begin, WikiLeaks as an institution has put forth its stated purpose. A comprehensive study of the movement that led to the creation of WikiLeaks described it as a movement of people "who aim to obliterate the world's institutional secrecy."[338] Its own website explains that "[p]ublishing improves transparency, and this transparency creates a better society for all people."[339]

Assange, of course, is the single person most publicly affiliated with WikiLeaks, and his use of technology for political ends is longstanding. As a sixteen-year-old hacker, he promoted an ethical code: "Don't damage computer systems you break into (including crashing them); don't change the information in those systems (except

336 *Id.* at 120.

337 *See id.* at 121-22, 128.

338 *Id.* at 8.

339 *About*, *supra* note 18.

for altering logs to cover your tracks); and share information."[340] When he was eventually caught and prosecuted, the judge showed leniency as a result of Assange's idealistic aspirations of "a world without limits on information."[341] Later in life, when he became involved with the cypherpunks, he declared the Internet a "censorship free zone."[342] Others often describe him not as an anti-war activist or even an anti-government activist, but rather as "an information freedom advocate."[343]

Assange eventually wrote his own "Crypto-Anarchist Manifesto," posted to his then-blog entitled "Conspiracy as Governance," where he identified leaks as the solution to accountable governance.[344]

> The more secretive or unjust an organization is, the more leaks induce fear and paranoia in its leadership and planning coterie. This must result in minimization of efficient international communications mechanism (an increase in cognitive "secrecy tax") and consequent system-wide cognitive decline resulting in decreased ability to hold onto power as the environment demands adaption.[345]

He concluded, "[h]ence in a world where leaking is easy, secretive or unjust systems are nonlinearly hit relative to open, just systems."[346]

Assange's early statements about his beliefs and purpose demonstrate that his actions are not solely about whistleblowing, but about fighting for better government accountability systems. While some may read his words as simply demonstrating a desire to dismantle government power, a closer read shows that he believes a truly transparent and accountable government would not be threatened by leaks; it is only the governments without adequate processes for accountability that will be threatened. Accordingly, his leak philosophy is a protest of excessive government secrecy and a lack of adequate means for oversight.

Others affiliated with WikiLeaks demonstrate the same views. The only American publicly affiliated with WikiLeaks, Jacob Appelbaum, gave a keynote speech representing WikiLeaks in place of Julian Assange at the Hackers on Planet Earth Conference, in New York City

340 GREENBERG, *supra* note 14, at 106-07.
341 *Id.* at 112.
342 *Id.* at 114.
343 *Id.* at 113.
344 *Id.* at 128-29.
345 *Id.* at 128-29.
346 *Id.* at 129.

in 2010. There, he talked about his views on the injustice of the wars in Afghanistan and Iraq, but spent most of his time much more generally speaking about the importance of leaks as an accountability tool, and urging the audience of hackers to become leakers themselves.[347]

Even defectors from WikiLeaks share these sentiments. Eventually, on WikiLeaks's way down, having been starved for funds and having criminal investigations commenced against Julian Assange, Assange's two collaborators, Daniel Domscheit-Berg and an anonymous individual known as the Architect, left the organization.[348] With them, they took an archive of thousands of unpublished submissions.[349] Their stated reasons, though, still demonstrate their political ends: they cited as justification for their actions that they did not trust Assange to properly protect the leaked material and the sources.[350] Despite their demonstrated interest in transparency, they continue to believe that some sensitive information ought to remain secret.

Chelsea Manning, for her part, spoke to her motivations in a prepared statement she read as part of her court-martial proceedings.[351] As to the "Collateral Murder" video, she described being disturbed when she first discovered the video because of the comments made by military personnel involved in combat, which she viewed as dehumanizing.[352] She then researched the video and discovered that it showed an incident in which two Reuters' employees were killed.[353] She further learned that Reuters had submitted a FOIA request for the video, but that the government had replied that it could not give a time frame for responding and that the video may no longer exist.[354] A year later, a news account reported that Reuters never received a response as required under FOIA.[355] As Manning put

[347] *See id.* at 168; *see also* Ben Hassine, *supra* note 103 (discussing how in Tunisia Wikileaks could be an opportunity to rebel against President Ben Ali's regime).

[348] GREENBERG, *supra* note 14, at 296-97.

[349] *Id.* at 300.

[350] *Id.* at 297.

[351] Bradley Manning, Private First Class, U.S. Army, Statement in Support of Providence Inquiry for Formal Plea of Guilty in *United States v. Pfc. Manning* (Feb. 28, 2013), *available at* http://www.alexaobrien.com/secondsight/wikileaks/bradley_manning/pfc_bradley_e_manning_providence_hearing_statement.html.

[352] *Id.*

[353] *Id.*

[354] *Id.*

[355] *Id.*

it, "The fact [that the government agencies] would not voluntarily release the video troubled me further."[356]

Manning released a public letter several months later, in which she explicitly denied self-identifying as a "'pacifist,' 'anti-war,' or (especially) a 'conscientious objector.'"[357] Instead, she defined herself as a "transparency advocate," explaining that she "feel[s] that the public cannot decide what actions and policies are or are not justified *if they don't even know the most rudimentary details about them and their effects*."[358] Manning was troubled by some particular government activities which she believed were immoral and/or illegal, thus fitting a whistleblower leaker profile, but her intentions were much bigger than that. She believed leaking was the only way left to inform the public about matters of public concern because of the inefficacy of transparency laws.

Snowden, for his part, released a twelve-minute video just a week after reporting began concerning the NSA material he leaked.[359] He described his motivations as his belief that "this is something that's not [the government's] place to decide, the public needs to decide whether these programs and policies are right or wrong."[360] As he said in another instance, transparency was his primary goal: "The consent of the governed is not consent if it is not informed,"[361] and he felt there was no meaningful oversight of the NSA.[362] Consistent with his

356 *Id.*

357 Public Statement, Chelsea E. Manning, *supra* note 14, at 2.

358 *Id.* (emphasis added).

359 *NSA Whistleblower Edward Snowden: 'I Don't Want to Live in a Society that Does These Sort of Things' — Video*, GUARDIAN (June 9, 2013), http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video.

360 *Id.* at 5:00; *see also* HARDING, *supra* note 311, at 238 (quoting Snowden as saying: "I took what I knew to the public, so what affects all of us can be discussed by all of us in the light of day, and I asked the world for justice"). Others have characterized Snowden's actions as a form of civil disobedience. *See* William E. Scheuerman, *Whistleblowing as Civil Disobedience: The Case of Edward Snowden*, 40 PHIL. & SOC. CRITICISM 609, 610 (2014) ("Snowden has thought long and hard about the fundamental question of when and how citizens of a liberal democratic state are morally and politically obliged to violate the law."); *see also Last Week Tonight: Government Surveillance* at 21:32 (HBO Television Broadcast Apr. 5, 2015), *available at* https://www.youtube.com/watch?v=XEVlyP4_11M (documenting where Snowden explained, "I did this to give the American people a chance to decide for themselves the kind of government they want to have").

361 HARDING, *supra* note 311, at 53.

362 *See id.* at 7.

goals of openness, Snowden also felt his actions were in defense of a free Internet.[363]

Moreover, he describes himself as a patriot, not as someone trying to harm U.S. national security or individual members of the security community:

> Anybody in the positions of access . . . could [] suck out secrets, pass them on the open market to Russia . . . . I had access to [] the full rosters of . . . the entire intelligence community . . . the locations of every station we have, what their missions are, and so forth. If I had just wanted to harm the U.S., [I] could [have] shut down the surveillance system in an afternoon.[364]

In fact, long prior to his leaks, Snowden had railed against leaks of classified information that produce real security risks.[365]

Another aspect of Snowden's public statements strikingly implicates the legitimacy of secrecy laws, and in particular whistleblower laws. Snowden watched and was influenced by the experience of Thomas Drake, who attempted to use the whistleblower procedures without avail, eventually taking his information to the press and suffering criminal prosecution as a result.[366] Snowden believed any reporting up the chain would be futile because "[t]he system doesn't work. You have to report the wrongdoing to those most responsible for it."[367] Snowden had also had his own experience of reporting comparatively minor security problems when working at the CIA earlier in his career, for which he was eventually reprimanded, something that may

---

[363] GREENWALD, *supra* note 9, at 47; HARDING, *supra* note 311, at 110.

[364] *NSA Whistleblower Edward Snowden*, *supra* note 359, at 9:51.

[365] *See id.* at 33-34 (citing Snowden's statements in an online chat, including, "that shit is classified for a reason").

[366] *Id.* at 52. For more details about Thomas Drake, see *supra* notes 290-93 and accompanying text.

[367] HARDING, *supra* note 311, at 52. While Snowden's perception of the legitimacy of the whistleblower laws is more important for present purposes, whether Snowden could even have taken advantage of whistleblower protection laws as a contractor is itself unclear. *See* Glenn Kessler, *Edward Snowden's Claim that He Had 'No Proper Channels' for Protection as a Whistleblower*, WASH. POST (Mar. 12, 2014), http://www.washingtonpost.com/blogs/fact-checker/wp/2014/03/12/edward-snowdens-claim-that-as-a-contractor-he-had-no-proper-channels-for-protection-as-a-whistleblower/; *see also* Remnick, *supra* note 84 (quoting Obama as having said that "the benefit of the debate [Snowden] generated was not worth the damage done, because there was another way of doing it").

have affected his view of the efficacy of raising problems to superiors.[368]

In sum, these leakers are not simply trying to take down governments or corporations or promote some sort of anarchist ideal. Rather, they are motivated by the fact that the systems that keep governments accountable, in their view, are not working. For this reason, "there is nothing inherently odd about the observation that those who flout the rules on disclosing classified information would nonetheless abide by certain other norms on leaking."[369] That is, each one has an ethical code; they are not attempting to simply maximize the harm they can inflict on individuals or institutions. Their stated motivations demonstrate their concern with a lack of legitimacy in formal transparency and oversight mechanisms, and thus link their actions to the failure of procedural justice in our secrecy laws.

CONCLUSION: IMPROVING TRANSPARENCY AND SECURITY

Deluge leaks pose new kinds of dangers that are worth addressing. The current dialogue, however, has focused on increasing criminal penalties for those involved in such leaks, whether by leaking itself or by publication, and thereby deterring others from engaging in this behavior. Typically, such proposals pit national security interests against the public's interest in oversight, implying, if not stating, that more oversight would directly harm security interests. Not only would an increased criminalization approach be expensive, however, it would also be unlikely to succeed.

A better approach is to look at the root of deluge leaking. The excessive secrecy pervasive in the national security realm subject only to procedural rights that do not effectively vindicate the public's right to access government information forms the basis on which government employees and contractors may conclude the secrecy laws lack legitimacy.[370] Under a theory of procedural justice, secrecy laws viewed as illegitimate are significantly more likely to be broken, thereby creating an environment ripe for leaks.[371] Recent deluge

368 HARDING, *supra* note 311, at 37. He has been described as having lost faith in congressional oversight of intelligence as well. *See id.*

369 Pozen, *supra* note 1, at 602.

370 *See supra* Part IV. Even the most ardent of contemporary anti-leak intellectuals, Gabriel Schoenfeld, has acknowledged that "our national security system is saddled with pervasive mis- and overclassification that remains entrenched despite universal recognition of its existence and numerous attempts at reform." SCHOENFELD, *supra* note 5, at 268.

371 *See supra* Part III.

leakers have displayed actions and statements that indicate they were, in fact, influenced by their view that secrecy laws are broken and that the legal procedural mechanisms for public oversight are unjust.[372]

By looking at the problem through this lens, we can reframe government transparency and national security as being in less tension with one another than usually believed. Improving our government transparency laws and procedures, to the extent it could improve the legitimacy of the government in the view of the many civil servants and contractors working with classified information, could both improve public oversight and accountability as well as prevent deluge leaks. Both aims are worthwhile.

A procedural justice approach to curbing deluge leaking would also reduce the role that leaks play out of necessity. As one scholar noted about leaks generally, "[I]n some instances leaks disclose information that should never have been classified; these leaks can play an important role in correcting the rampant and, to date, unsolved overclassification problem."[373] Using illegal leaks to serve an important public purpose of government oversight, however, is a highly questionable strategy, if only because leaks will be both over- and under-inclusive in the information they release. Instead, our secrecy laws should be tailored so as to deny leaks a vital unfulfilled role in our democracy.

Pozen suggests that "there are two stable equilibria in the U.S. market for transparency: broad formal classification with broad informal disclosure, or narrow formal classification with narrow informal disclosure."[374] A shift to the second type of equilibrium — one in which procedural access to government information was greatly improved, thereby reducing the amount of government secrecy overall — is the kind of shift that would curb the need or incentive to rely on unauthorized disclosures, i.e., leaks. Increasingly costly deluge leaks may prompt Congress to crack down on leaking, but should also prompt Congress to address the problems of overly broad official secrecy.[375]

Perhaps, in fact, as we disclose more information to the public through formal means, we will achieve a state where the amount of leaking is tolerable, which will naturally bring us to a better

---

372 *See supra* Part V.

373 Papandrea, *supra* note 10, at 478.

374 Pozen, *supra* note 1, at 581. Pozen also argues that if we had less secrecy, people might treat the secrecy we do have with more respect. *Id.* at 581-82.

375 *See id.* at 581 (arguing Congress has no incentive to address excessive secrecy since leaks provide the counterbalance).

equilibrium balance between national security and government transparency.[376] This equilibrium may be more achievable than the sort of ex ante proscriptions of categories of information that should or should not be public.[377] In this way, a procedural justice approach to government secrecy will address deluge leaking specifically, but also may contribute to more just secrecy laws. More robust transparency laws can in fact result in more effective national security secrets.

[376] Other scholars have noted the near impossibility of making a determination about the right balance between transparency and security in the abstract. *See, e.g.*, *id.* at 605 & n.418.

[377] *See id.*