St. John's Law Review

Volume 85
Number 4 *Volume 85, Fall 2011, Number 4*

Article 1

April 2014

Adjudicating Classified Information

Alex Rossmiller

ARTICLES

ADJUDICATING CLASSIFIED INFORMATION

ALEX ROSSMILLER[†]

TABLE OF CONTENTS

[†] J.D., 2010, New York University School of Law; B.A., 2004, Middlebury College. Fellow, National Security Network. I am especially grateful to Beth George for her invaluable help and patience. Thanks also to Professor Sam Rascoff for his input and guidance, and to Tess Bridgeman for her encouragement. Finally, special gratitude to Sarah Zearfoss, who is always right.

INTRODUCTION

There is tremendous debate over how the judicial system should handle information and materials the government would prefer to keep secret. Courts, scholars, and policymakers struggle with the relevant procedures and incentives, many of which are complex or contradictory; secret information is handled in a variety of different ways, depending on precise circumstances. The post-9/11 era has amplified the issues regarding protected information and the judicial system; as the United States government shifted its attention to national security in a number of unprecedented ways, one effect has been an explosion of secrecy claims in court, as well as a tremendous proliferation of litigation involving security issues.

Disputed topics include what kind of protected information should be admissible, what standards and review processes should govern those decisions, and who should be responsible for the various aspects of these steps.[1] Courts have expressed frustration with legal structures and government decisions regarding protected information;[2] academic commentary has pronounced security-related processes broken and suggested various possible solutions in both civil and criminal contexts;[3] and both houses of Congress recently have considered legislation aimed at substantially altering how courts would approach and manage classified material.[4]

These questions are essential, of course, and some amount of reform—or standardization and clarity, at the very least—would greatly improve the situation for courts and litigants alike. While such reform would be beneficial, however, rather than resolving judicial uncertainty, any structural process—including the extant one—prompts a number of vital and unresolved

---

[1] *See* Robert M. Chesney, *State Secrets and the Limits of National Security Litigation*, 75 GEO. WASH. L. REV. 1249, 1302–06 (2007); Amanda Frost, Essay, *The State Secrets Privilege and Separation of Powers*, 75 FORDHAM L. REV. 1931 (2007); Carrie Newton Lyons, *The State Secrets Privilege: Expanding Its Scope Through Government Misuse*, 11 LEWIS & CLARK L. REV. 99 (2007).

[2] *See, e.g.*, Mohamed v. Jeppesen Dataplan, Inc., 614 F.3d 1070, 1094 (9th Cir. 2010) (en banc) (Hawkins, J., dissenting) ("It is far better to require the government to make its claims of state secrets with regard to specific items of evidence or groups of such items as their use is sought in the lawsuit."), *cert. denied*, 131 S. Ct. 2442 (2011); Boumediene v. Bush, 579 F. Supp. 2d 191, 197 (D.C. Cir. 2008) ("[W]hile the Government has provided some information about the source's credibility and reliability, it has not provided . . . enough information to adequately evaluate the credibility and reliability of this source's information."); Parhat v. Gates, 532 F.3d 834, 848 (D.C. Cir. 2008) ("Lewis Carroll notwithstanding, the fact that the government has 'said it thrice' does not make an allegation true.").

[3] *See, e.g.*, Jonathan M. Fredman, *Intelligence Agencies, Law Enforcement, and the Prosecution Team*, 16 YALE L. & POL'Y REV. 331, 348, 370–71 (1998) (discussing problems with discovery processes when intelligence and law enforcement activities overlap); Meredith Fuchs, *Judging Secrets: The Role Courts Should Play in Preventing Unnecessary Secrecy*, 58 ADMIN. L. REV. 131, 168–76 (2006) (arguing that courts can and should review government assertions of secrecy); David E. Pozen, Note, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628, 632 (2005) (advocating increased judicial scrutiny of government protection of classified materials).

[4] State Secrets Protection Act, S. 2533, 110th Cong. (2008), was first proposed in the Senate during the 110th Congress, on January 22, 2008; similar legislation was introduced in the House, H.R. 5607, 110th Cong. (2008), on March 13, 2008. The bill was reintroduced in the 111th Congress in both houses, as S. 417, 111th Cong. (2009) and H.R. 984, 111th Cong. (2009), on February 11, 2009. None of these bills received floor votes.

questions. Perhaps most importantly, if and when classified materials are introduced into the legal system, courts need to know how they should treat the information *itself*.

Knowing how to view, evaluate, and understand intelligence products is neither intuitive nor widely understood in the legal community. There is therefore a pressing need for a blueprint, the beginnings of which this Article will attempt to provide. This Article examines the current landscape of courts and their treatment of protected material, critically addressing the shortcomings and inconsistencies of judicial attempts to grapple with government secrets. It proposes a more rigorous and consistent juridical approach to these issues, and it argues that the existing treatment of classified material is substantially lacking but readily improvable.

Part I of this Article briefly examines the existing legal and conceptual frameworks that purport to manage protected information in the judicial system. It compares and contrasts the civil and criminal approaches, and it notes challenges to the existing processes and proposed changes from policymakers and scholars. Part I also discusses the questions and problems raised by potential changes—and even by the status quo. Part II explores secret information: its creation by individuals and agencies; its synthesis into "finished" intelligence; its various uses; and the challenges it poses for the legal process.

Part III offers three proposals for how courts should treat secret information to avoid or counteract the problems discussed and to maximize the interests of justice in criminal, civil, and nontraditional contexts. It argues that critical judicial responsibilities include: (1) reviewing information designated as secret, (2) applying appropriate skepticism to secret information and government claims, and (3) examining source material. Part III then reviews selected decisions in which courts have made judgments about protected information, and it discusses and evaluates these approaches.

I. FRAMEWORKS FOR PROTECTED INFORMATION: CURRENT STRUCTURES AND CHALLENGES

To adequately address how courts should treat protected information, it is necessary to first briefly consider the existing legal and conceptual structures that shape the roles of classified and other secret information in the judicial system. Additionally,

it is useful to note and analyze challenges to the current processes, as well as pending legislation and cases that could produce transformation.

A. Legal and Conceptual Frameworks for Classified Information

1. Protected Information in Criminal Law

"Protected" information generally is addressed in markedly different ways, depending on the legal context. In criminal law, use of secret information is governed by the Classified Information Procedures Act ("CIPA"), which provides guidelines for the government and defendants alike to balance the government's interest in secrecy against the various rights of the accused and the public in the justice system.[5]

Passed by Congress in 1980, CIPA codified a pragmatic approach to the rights and incentives involved in using classified information in criminal cases. The principal goal of the statute was to protect the government against "graymail," where a defendant threatens to reveal classified information at trial to deter prosecution.[6] Additionally, CIPA helps regulate government use of classified information, requiring that such materials be made available to defendants and their attorneys as well as mandating cooperation with the court to fulfill a number of requirements.[7]

CIPA attempts to address three common scenarios: the government's need to use classified evidence to prosecute; a defendant's need to introduce classified information—of which she is already aware—for exculpation; and the respective obligations of both sides in discovery.[8] A defendant does not want to be surprised by classified information (and indeed may

---

[5] Classified Information Procedures Act, 18 U.S.C. app. 3 §§ 1–16 (2006).

[6] United States v. Poindexter, 725 F. Supp. 13, 34 (D.C. Cir. 1989) ("CIPA serves [the security of the nation] . . . by helping to ensure that those with significant access to such information will not escape the sanctions of the law applicable to others by use of the graymail route.") (citing S. Rep. No. 96–823, at 3 (1980), *reprinted in* 1980 U.S.C.C.A.N. 4294, 4296); *Bill Summary & Status, 96th Congress (1979–1980), S. 1482, CRS Summary*, THOMAS (LIBRARY OF CONGRESS), http://thomas.loc.gov/cgi-bin/bdquery/z?d096:SN01482:@@@D&summ2=4& (last visited Mar. 24, 2012) ("Classified Information Procedures Act—Sets forth pretrial, trial, and appellate procedures for criminal cases involving classified information ('graymail' cases.)").

[7] 18 U.S.C. app. 3 §§ 5–6.

[8] *See id.* §§ 4–6.

have the right not to be under the 6th Amendment);[9] neither does the government, because such disclosure could damage national security. CIPA addresses this mutual interest in advance notice of intended utilization of protected materials by placing disputes over their use firmly in the pre-trial phase, allowing the government to make its cost-benefit analysis early in the process.[10] Whether it is the government or a defendant intending to introduce classified material, the government in both instances must decide whether the benefits of prosecution outweigh the potential costs of exposing the protected information.[11]

In the context of discovery, CIPA allows courts to authorize the government to redact classified information from documents provided to the defendant, substitute an unclassified summary, or substitute a statement admitting relevant facts that the classified information would tend to prove.[12] The government may pursue these options *ex parte* and *in camera*.[13] The statute also requires advance disclosure by the defendant of any intent to disclose classified information at trial, whether such materials are already in her possession or are received through discovery.[14] If a court determines that certain evidence must be included, the government's refusal to do so, or unwillingness or inability to provide an appropriate substitution, can lead to sanctions up to and including dismissal of the indictment.[15] CIPA does not purport to change evidentiary standards,[16] nor does it allow courts to question the validity or level of the classification,[17] but those limitations are subordinate to the important and useful

---

[9] *See* Greene v. McElroy, 360 U.S. 474, 496 (1959) ("[T]he evidence used to prove the Government's case must be disclosed to the individual so that he has an opportunity to show that it is untrue.").

[10] *See* 18 U.S.C. app. 3 § 6(a)–(b).

[11] *See id.* § 4.

[12] *See id.* § 6(b)–(c).

[13] *See id.* § 6(c)(2).

[14] *See id.* § 5(a).

[15] *See id.* § 6(e)(2).

[16] *See id.* § 4 (noting that classified elements of materials discoverable under the Federal Rules of Criminal Procedure may be redacted). *But see* United States v. Smith, 780 F.2d 1102, 1105 (4th Cir. 1985) (finding that "[CIPA's] application results in a more strict rule of admissibility" than is normally the case under the usual relevance standard).

[17] *See Smith*, 750 F.2d at 1217 ("[T]he government . . . may determine what information is classified A defendant cannot challenge this classification. A court cannot question it.").

provisions for targeted redaction and/or unclassified substitution.[18] As a matter of evidentiary process, CIPA is reasonably effective, setting the government's desire to prosecute against its inclination toward secrecy in matters of national security.

The statute does not, however, provide any guidance to courts regarding the information itself. There is no instruction about how to evaluate the classified materials, how to determine whether unclassified summaries are adequate or accurate, or, perhaps most importantly, how the fact-finder should assess the contents, analysis, or conclusions of the protected information.

2. Protected Information in Civil Law

Classified material is managed quite differently in civil cases, where the State Secrets Privilege ("SSP") is the relevant governing principle. The SSP is an evidentiary rule based on English common law and established in modern American jurisprudence by the Supreme Court decision in *United States v. Reynolds*.[19] When the government believes that court proceedings might disclose sensitive information that could endanger national security, it may submit a formal claim of privilege asking the court to prevent the admission or use of the disputed materials.[20]

The use of the SSP is both more haphazard and more expansive than CIPA procedures. Rather than prosecutors and defendants identifying classified materials and working with judges to find ways to use the information, or limiting the prosecution accordingly if the government is unable or unwilling to do so, the SSP is invoked by a "formal claim of privilege, lodged by the head of the department which has control over the matter."[21] In *Reynolds*, for example, the SSP was invoked by the Secretary of the Air Force.[22] In addition to the huge number of individuals who are "the head of the department" and who could therefore assert the privilege, the SSP is further expanded by the

---

[18] 18 U.S.C. app. 3 § 6(c).

[19] United States v. Reynolds, 345 U.S. 1, 7–8, 11 (1953). *See generally* EDWARD C. LIU, CONG. RESEARCH SERV., R40603, THE STATE SECRETS PRIVILEGE AND OTHER LIMITS ON LITIGATION INVOLVING CLASSIFIED INFORMATION (2009).

[20] *See Reynolds*, 345 U.S. at 7–8; LIU, *supra* note 19, at 2.

[21] *Reynolds*, 345 U.S. at 7–8.

[22] *See id.* at 4.

apparent lack of restriction to classified information.[23] Neither the Supreme Court nor any lower court has provided a clear definition of state secrets. Instead, courts rely on the nebulous, senescent *Reynolds* opinion.[24] Furthermore, while *Reynolds* established SSP applicability for military matters, subsequent decisions have expanded the coverage considerably.[25] The government has claimed the privilege, for example, in relation to programs that have been publicly identified[26]—not to mention the invocations later revealed to be duplicitous, including in *Reynolds* itself.[27]

Unlike with CIPA, where the United States has a strong interest in working toward the admissibility of classified information in some form—whether as part of its own case or to avoid dismissal if the defendant possesses and wants to use such materials—the incentives with the SSP are overwhelmingly in favor of government recalcitrance. If the government is a party at all—which it need not be to assert the privilege[28]—it is as a defendant, and there is virtually no incentive to disclose; indeed, when the information will be used against the government, there is substantial motivation to keep the secrets (or so-called "secrets") out of court.

---

[23] *See id.* at 10 (speaking not of "classified" information being privileged, but, rather, that which "in the interest of national security[ ] should not be divulged").

[24] *See id.* at 10 ("It may be possible to satisfy the court, from all the circumstances of the case, that there is a reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged. When this is the case, the occasion for the privilege is appropriate . . . ."); *see also* Adam Liptak, *In Knotty State Secrets Case, Justices Ponder Telling Litigants To 'Go Away,'* N.Y. TIMES, Jan. 19, 2011, at A15 ("It has been almost 60 years since the Supreme Court last had a hard look at the state secrets privilege . . . . The privilege was at the center of an argument at the court on Tuesday. But the justices did not seem inclined to use the opportunity to give the lower courts guidance about its contours.").

[25] *See* Ellsberg v. Mitchell, 709 F.2d 51, 57 (D.C. Cir. 1983) ("Possibly because the state secrets doctrine pertains generally to *national security* concerns, the privilege has been viewed as both expansive and malleable.").

[26] *See* Mohamed v. Jeppesen Dataplan, Inc., 614 F.3d 1070, 1074 (9th Cir. 2010) (en banc) (discussing plaintiff's claim that the circumstances surrounding one plaintiff's rendition had "been publicly acknowledged by the Swedish government"), *cert. denied*, 131 S. Ct. 2442 (2011); El-Masri v. United States, 479 F.3d 296, 301 (4th Cir. 2007) (acknowledging plaintiff's claim that "CIA rendition operations . . . had been widely discussed in public forums").

[27] *See infra* Part III.B.4.

[28] *See, e.g.*, *Jeppesen*, 614 F.3d at 1076 (where the United States intervened to assert the privilege).

This combination of the incentive to conceal with the lack of judicial guidance or oversight has resulted in mounting condemnation of SSP practices. The criticisms are both quantitative and qualitative. SSP assertions have grown substantially in number in recent years, and the frequency of the government's use of the privilege is accelerating. Between 1953 and 1977, there were very few instances of SSP invocation, with most accounts reporting single digit usage. Between 1977 and 2001, there were around fifty reported such instances.[29] The Bush administration, in just eight years, reportedly asserted the privilege "at least 39" or "dozens of" times.[30] Because not all uses of the SSP are reported, it is difficult to determine with certainty the frequency of its invocation, but if the reported cases are any guide, the increase in recent years is substantial.[31]

---

[29] *See* TED GUP, NATION OF SECRETS: THE THREAT TO DEMOCRACY AND THE AMERICAN WAY OF LIFE 109 (2007) ("In the 19 years between 1954 and 1973, the U.S. government invoked the state secrets privilege only four times. In the five years since 9/11, it has been invoked at least 23 times . . . ."); Frost, *supra* note 1, at 1938 ("[S]tarting in 1977, the executive raised the privilege with greater frequency. Between 1953 and 1976, there were only eleven reported cases addressing the privilege; between 1977 and 2001 there were fifty-nine reported cases."); Fuchs, *supra* note 3, at 134–35 ("In the 23-year span between the Supreme Court case that authorized use of the state secrets privilege in 1953 and 1976, the government litigated cases involving the privilege four times. In the 24 years between 1977 and 2001, courts were called to rule on the government's invocation of the privilege 51 times.").

[30] *See* Nicholas Goldberg, Editorial, *Backgrounder; 'State Secrets' Go on Trial*, L.A. TIMES, Feb. 15, 2009, at A33 ("There's a strong case to be made that the Bush administration overused and misused the state secrets privilege. After 9/11, Bush Justice Department officials invoked the privilege dozens of times—far more times a year than any of their predecessors."); Dana Priest, *Secrecy Privilege Invoked in Fighting Ex-Detainee's Lawsuit*, WASH. POST, May 13, 2006, at A03 ("The state secrets privilege was invoked about 55 times from 1954 to 2001, according to the Reporters Committee for Freedom of the Press, and in the first four years after the Sept. 11, 2001, attacks, it was invoked 23 times."); David Kravets, *New Attorney General Orders Review of Bush-Era State Secrets*, WIRED (Feb. 9, 2009, 3:34 PM), http://www.wired.com/threatlevel/2009/02/ag-holder-deman ("The Bush administration invoked the privilege at least 39 times, whereas all U.S. presidents have invoked it roughly 55 times combined . . . [including just] six times between 1953 and 1976 . . . ."); Marc A. Sorel, *Rethink the State Secrets Privilege*, BALT. SUN (May 7, 2010), http://articles.baltimoresun.com/2010-05-07/news/bs-ed-state-secrets-20100507_1_privilege-wiretapping-government ("Since Sept. 11, the U.S. government has asserted the privilege in more than 100 cases.").

[31] *See* Laura K. Donohue, *The Shadow of State Secrets*, 159 U. PA. L. REV. 77, 81 (2010) ("[C]urrent scholarship . . . [omits] the many cases in which the court sidesteps the question altogether or dispenses of the state secrets questions at an early stage in the litigation . . . [or in] unreported and unpublished opinions . . . as well as sealed memoranda and opinions."); William G. Weaver & Robert M. Pallitto,

However, during that time there has been no corresponding increase in clarity or consistency of the use or interpretation of the SSP. The guidance for lower courts continues to be rooted in the *Reynolds* decision, which established a two-step process to use when the privilege is asserted.[32] First, the head of the department with control over the matter must formally invoke the privilege.[33] Second, and more substantively, the court "must determine whether the circumstances are appropriate for the claim of privilege, and yet do so without forcing a disclosure of the very thing the privilege is designed to protect."[34]

The *Reynolds* opinion, even while acknowledging the "real difficulty" of such a task, hedged on exactly how courts could or should accomplish this goal.[35] The Court said that "[i]t may be possible to satisfy the court, from all the circumstances of the case" that the privilege should apply—but, the Court indicated, such a determination might not involve actually reviewing the materials at issue.[36] The Court further elaborated: "[T]he court should not jeopardize the security which the privilege is meant to protect by insisting upon an examination of the evidence, even by the judge alone, in chambers."[37] The *Reynolds* decision also noted that while control over evidence "cannot be abdicated to the caprice of executive officers," the court would "not go so far as to say that the court may automatically require a complete disclosure to the judge" for the claim to be accepted.[38]

In addition to being used with increasing frequency, the SSP also has been used more expansively in recent years. The SSP was initially formulated as a privilege to prevent the admission of specific pieces of evidence, whereby the government could assert the SSP during discovery.[39] This would allow courts to determine the necessity of the materials to the litigation, the

---

State Secrets and Executive Power, 120 POL. SCI. Q. 85, 101 (2005) ("Because reported cases only represent a fraction of the total cases in which the privilege is invoked or implicated, it is unclear precisely how dramatically the use of the privilege has grown. But the increase in reported cases is indicative of greater willingness to assert the privilege than in the past.").

[32] *See* United States v. Reynolds, 345 U.S. 1, 7–8 (1953).

[33] *Id.*

[34] *Id.* at 8.

[35] *Id.*

[36] *Id.* at 10.

[37] *Id.*

[38] *Id.* at 9–10.

[39] *See* Chesney, *supra* note 1, at 1281.

possibility of using available alternative information, and the circumstances of the case as they applied to the legitimacy of the invocation.[40] Naturally, sometimes the successful use of the privilege would result in dismissal during the discovery phase, if the evidence excluded were central to the plaintiff's case.[41] Recently, however, the executive branch repeatedly has used the SSP to prevent lawsuits from even reaching the discovery phase by invoking the privilege even before answering plaintiffs' complaints.[42] Accordingly, the privilege becomes essentially a pre-discovery motion to dismiss, even if the plaintiff might otherwise be able to amass enough evidence to move past the pleadings stage.[43]

The jurisprudence resulting from this precedential morass has been widely—and increasingly—criticized.[44]

3. Protected Information in Nontraditional Legal Settings

Since the attacks of September 11, the United States has dramatically augmented its efforts against global terrorism, including via engagement in two major wars, in Afghanistan and Iraq, as well as through expanded law enforcement and intelligence operations throughout the world. The legal framework for counter-terrorism rests somewhere between

---

[40] *See Reynolds*, 345 U.S. at 7–8; LIU, *supra* note 19, at 2–3.

[41] *See, e.g.*, Molerio v. FBI, 749 F.2d 815 (D.C. Cir. 1984) (dismissing an action against the FBI for alleged discriminatory termination after the court accepted the FBI's proffered *in camera* explanation and determined that the reason for the termination was deemed protected by the SSP); Halkin v. Helms, 690 F.2d 977, 990–97 (D.C. Cir. 1982) (dismissing an action against the National Security Agency upon finding that evidence of communications interception was privileged).

[42] *See* Al-Aulaqi v. Obama, 727 F. Supp. 2d 1, 8 (D.C. Cir. 2010); Mohamed v. Jeppesen Dataplan, Inc., 614 F.3d 1070, 1076 (9th Cir. 2010) (en banc), *cert. denied*, 131 S. Ct. 2442 (2011); El-Masri v. United States, 479 F.3d 296, 299–300 (4th Cir. 2007).

[43] *See Al-Aulaqi*, 727 F. Supp. 2d at 8–9; Lyons, *supra* note 1, at 117 ("The state secrets privilege was not crafted in *Reynolds* to be a complete bar on the adjudication of complaints by the courts; the government, however, is applying the privilege in such a way that complaints are being completely dismissed, denying any forum to plaintiffs for redress.").

[44] *See, e.g.*, Weaver & Pallitto, *supra* note 31, at 87–88 ("The incentives to abuse the privilege are obvious . . . . As presently formulated, the privilege is ill-equipped to balance between [the] two goals" of protecting "legitimate interests . . . while trying to eliminate abuse of power . . . ."); *supra* note 1 and accompanying text.

ambiguity and nonexistence, and the government, academics, and litigants have all scrambled to find their respective footing in an evolving area of the law.

Some aspects of that developing genre are orthogonal to this discussion, such as the reach of the Constitution to foreign individuals and countries, or separation of powers questions at the highest levels of government. Other elements, such as the admissibility of classified information in lawsuits brought by plaintiffs alleging that they have been spied upon or subject to abuse while in detention, or in the prosecution of alleged terrorists in federal court, are related but generally encompassed by traditional civil or criminal frameworks. These latter examples are governed by CIPA and the SSP, and although government actions in recent years have presented new and challenging issues, those structural approaches are relatively familiar.[45]

In some instances, however, neither CIPA nor the SSP govern the review or use of protected materials.[46] In particular, cases in recent years regarding detainees at military facilities outside the United States have dominated legal debates and headlines.[47] Such proceedings have presented new and unusual jurisprudential issues, including how courts should use and view protected information. Accordingly, some of these cases are excellent examples of how judges have struggled to address classified information in its many forms.[48] Because of the structure of detainee trials and appeals, and the bifurcated legal routes available—habeas corpus petitions as well as appeals on the merits of military tribunal decisions—district and circuit courts alike have encountered issues of intelligence and classified information in various contexts. These cases, and their implications, will be further addressed in Parts III and IV; in this initial exploration, it is simply important to note that courts are

---

[45] *See, e.g.*, *El-Masri*, 479 F.3d at 300 (plaintiff claimed that he was illegally detained and abused); Ellsberg v. Mitchell, 709 F.2d 51, 52–53 (D.C. Cir. 1983) (plaintiffs claimed that they were illegally subject to electronic surveillance).

[46] *See infra* notes 168–169 and accompanying text.

[47] *See, e.g.*, Editorial, *Another Rebuke on Guantanamo*, N.Y. TIMES, June 25, 2008, at A22 (discussing the detention of Huzaifa Parhat at the United States Navy Base in Guantanamo, Cuba); Peter Finn & Del Quentin Wilber, *On Appeals, Detainees Have Never Won*, WASH. POST, July 6, 2011, at A01 (discussing the status of Guantanamo Bay detainees' court battles).

[48] *See* discussion *infra* Part III.B.

confronted with protected material in some circumstances wherein there is even less precedent and guidance than in traditional criminal and civil processes.

4. Current Criticisms, Challenges, and Proposed Reforms

In the context of criminal law, the competing government incentives of prosecution versus concealment of information help create a rough equilibrium of interests. This balance, combined with the statutory codification of principles and processes in CIPA, gives criminal law a structural framework that is less vulnerable to confusion or abuse than other areas of jurisprudence. Accordingly, criticisms of the judicial system's dealings with protected information are often concentrated on civil and nontraditional processes. Those criticisms are extensive and varied, as are the proposed remedies; they are briefly addressed here to provide context for the more specific discussion of protected materials themselves—and to establish the dearth of guidance regarding those materials' contents.

Two leading scholars of the SSP have called it "judicially mishandled to the detriment of our constitutional system."[49] Its problems derive mainly from the combination of two elements: inadequate verification of government privilege claims by courts and the lack of sufficient government incentives to reveal protected information in civil proceedings. While the latter factor results from entrenched structural influences, the former can be addressed by courts under existing judicial powers and responsibilities.

Regarding verification of government privilege claims, courts have largely failed to act as a check against executive overreach in asserting the SSP. Despite the *Reynolds* court's exhortation that "[j]udicial control over the evidence in a case cannot be abdicated to the caprice of executive officers,"[50] judges virtually always allow the exercise of the privilege; while precise reported numbers vary, out of dozens of SSP assertions by the government, few if any have been denied.[51] In most instances,

---

[49] Weaver & Pallitto, *supra* note 31, at 86.

[50] United States v. Reynolds, 345 U.S. 1, 9–10 (1953).

[51] Weaver & Pallitto, *supra* note 31, at 87, 102 ("The privilege seems to be ultra-constitutional, for the courts have not forced the government to disclose agency-held classified information in any case in which the privilege has been asserted . . . . In only four cases did courts ultimately reject the government's assertion of the

courts grant the privilege without even looking at the evidence that is allegedly a state secret. With the caveat that quantification of the SSP is elusive,[52] a comprehensive study on its use found that courts failed to review, even *in camera*, the information in question in more than two-thirds of the instances of privilege invocation.[53] Observers have rightly criticized this extreme judicial deference to executive branch assertions of the privilege; the problem is severe and is likely to continue.

In response, scholars and policymakers have proposed a number of solutions. In Congress, a bill under consideration[54] would mandate judicial review of each specific item of evidence against which the government has asserted the SSP, in order to determine the legitimacy of the invocation.[55] If the privilege is granted, a judge would then have to decide whether a non-privileged substitute could be created, much like under CIPA.[56] Courts would ostensibly be aided in this process by other features of the bill, including, among other things, allowance of *in camera* review, assistance of a special master, and *ex parte* hearings.[57] Academics have also suggested a variety of possibilities, most focused on judicial oversight,[58] but also via administrative remedies.[59]

---

privilege. But even this number is misleading, for in two of those cases, the privilege was obviously misused to protect unclassified information in the Department of Commerce[;]" in a third, the rejection was procedural and ultimately reversed; in a fourth, a complete trial was held in secret.).

[52] *See supra* note 31.

[53] Weaver & Pallitto, *supra* note 31, at 101 ("In less than one-third of reported cases in which the privilege has been invoked have the courts required *in camera* inspection of documents, and they have only required such inspection five times out of the twenty-three reported cases since the presidency of George H.W. Bush.").

[54] *See supra* note 4. The proposed Senate bill, S. 417, is used for purposes of this analysis; it does not differ substantively from the 2008 Senate bill or their companion House versions.

[55] State Secrets Protection Act, S. 417, 110th Cong., § 4054(d)–(e) (2009).

[56] *Id.* § 4054(e)–(f).

[57] *Id.* § 4052.

[58] *See, e.g.*, sources cited *supra* notes 1 & 3.

[59] An intriguing and persuasive case for an administrative approach to the challenges and difficulties presented by the SSP is made by Beth George, who argues that administrative law-based reforms will deter government abuse of the state secrets privilege more effectively than judicial review alone. Beth George, Note, *An Administrative Law Approach to Reforming the State Secrets Privilege*, 84 N.Y.U. L. REV. 1691 (2009).

There also has been tremendous criticism of the nontraditional legal systems established to process terrorism suspects, particularly regarding detainees held in military or intelligence facilities in Guantanamo Bay, Cuba; Bagram, Afghanistan; and so-called "black sites" throughout the world.[60] This opprobrium has not, however, principally addressed how courts or tribunals have dealt with classified information, perhaps because there have been much larger problems with these processes; the use of protected information is a relatively minor issue compared to, for example, the constitutionality of entire structures. It is in nontraditional legal settings, however, where courts paradoxically have the most freedom regarding protected information, as there are virtually no statutory or common law restrictions. As a result, some courts dealing with detainee issues have provided rare examples of deft and insightful management of classified information. Some of these instances are discussed in depth in Part IV.

B. *The Increasing Importance of Judicial Treatment of Protected Information*

Nearly all discussion of judicial processes involving protected information involves issues of admissibility. Virtually none of the relevant commentary or proposed legislation confronts the critical matter of judicial treatment of the protected information itself, independent of whether or not to allow it into a particular case or proceeding.[61] In today's juridical environment, addressing how courts should analyze and understand protected materials is more important than ever, for three primary reasons.

---

[60] Leila Nadya Sadat, *A Presumption of Guilt: The Unlawful Enemy Combatant and the U.S. War on Terror*, 37 DENV. J. INT'L L. & POL'Y 539, 541 (2009).

[61] Many of the existing and proposed methods for determining admissibility, substitution, etc. include judicial examination of the underlying information. This accentuates the importance of judges understanding how to understand and analyze that information for the purpose of making procedural determinations, as will be discussed thoroughly in Part III.

1. Post-9/11 Effects on Types of Cases

Most obviously, the United States' efforts against terrorism, as well as our involvement in two major wars, have generated an explosion of legal attention to—and court engagement with—questions of national security, many of which involve classified or otherwise protected information.

American policy regarding detention of individuals suspected of terrorism seems to receive the most scholarly and media contemplation. It is not hard to discern why detainees have captured so much attention: first, the constitutional relevance to criminal procedure is firmly rooted in American legal tradition, with courts accustomed to addressing habeas corpus petitions in particular[62]; second, detainees are able to meet standing and jurisdiction requirements in ways unavailable to prospective litigants who have been, for example, unknowingly spied on or hit by a Predator drone missile strike.[63]

Less obvious but of similar importance are the changes in governmental strategy and structure. The disintegration of the "FISA wall," for example, has caused law enforcement and intelligence entities to reconnect in unprecedented ways, mixing roles and responsibilities and creating novel problems for the use of protected material in criminal processes.[64] The Foreign Intelligence Surveillance Act ("FISA"), enacted by

---

[62] Habeas rights are constitutionally guaranteed, and while an examination of the history of habeas corpus in the United States is beyond the scope of this Article, it suffices to say that courts are very well acquainted with challenges to the legitimacy of detention. While the legal particulars of detainee appeals based on the Suspension Clause differ from, for example, an inmate appealing his death sentence in New York State, the processes and structures for habeas claims have been firmly established. Individuals held pursuant to the "global war on terror" therefore have a relatively straightforward path to dispute the legitimacy of their imprisonment, and judges have an established framework for handling these challenges. While the paths of these habeas cases have at times been prolonged and circuitous, courts have not shied away from grappling with the issues in thoughtful and assertive ways.

[63] *But see* Al-Haramain Islamic Found., Inc. v. Bush, 507 F.3d 1190, 1205 (9th Cir. 2007). *Al-Haramain* is the exception that proves this rule: The government accidentally revealed to the Al-Haramain Foundation that it was spied upon; even still, the foundation was prevented from using that information, despite its disclosure, due to the successful invocation of the State Secrets Privilege. *Id.*

[64] David Kris, who served as the United States Assistant Attorney General for National Security from 2009–2011, and was previously the Associate Deputy Attorney General for national security issues from 2000–2003, wrote an insightful and comprehensive article on this topic in 2006. David S. Kris, *The Rise and Fall of the FISA Wall*, 17 STAN. L. & POL'Y REV. 487 (2006).

Congress in 1978, generated a "conceptual dichotomy between law enforcement methods and all other lawful methods of protecting national security."[65] This separation of intelligence and law enforcement, supported by the legislative and judicial branches for decades, remained durable even after 9/11—until 2002, when the Department of Justice convened the Foreign Intelligence Surveillance Court of Review ("FISCR") for the first time since it was established in 1978.[66] The FISCR ruled that the FISA wall's legal basis was faulty, a decision that allowed for far greater coordination between intelligence and law enforcement agencies than was previously allowed.[67]

More generally, there is tremendous pressure for all agencies and departments with national security responsibilities—entities that fulfill roles as disparate as spying on the streets of Tehran and patrolling neighborhoods in Brooklyn—to collaborate in counter-terrorism efforts. The threat of terrorism has caused a major realignment of law enforcement priorities,[68] as well as a marked shift in the extent to which collaboration between government entities that follow different constitutional and statutory rules is accepted,[69] creating the potential for extensive overlap.

The resulting blurring of the line between foreign intelligence (whose primary purpose is gathering information) and law enforcement (traditionally focused on apprehending and convicting criminals) puts courts more squarely in the midst of intelligence than ever before. Just a decade ago, judges rarely had the occasion to evaluate intelligence methods, products, and analysis; when they did, it was either under a rigorous statutory scheme (CIPA) or in the context of a deferential but relatively infrequent[70] civil scheme (SSP). Today, there is greater interaction between criminal and intelligence bureaucracies and

---

[65] *Id.* at 487–88.

[66] *Id.* at 488.

[67] *Id.*

[68] *See, e.g., Department of Justice Oversight: Hearing Before the S. Judiciary Comm.*, 109th Cong. (2006) (statement of Alberto Gonzales, Att'y Gen. of the United States) ("[T]he War on Terror is our Number One priority at Justice . . . ."), *available at* http://judiciary.senate.gov/hearings/testimony.cfm?renderforprint=1&id=e655f9e2809e5476862f735da118b546&wit_id=e655f9e2809e5476862f735da118b546-1-1.

[69] *See* Kris, *supra* note 64, at 527.

[70] In recent years, however, use of SSP in civil cases has increased. *See supra* notes 25–26 and accompanying text.

dramatic augmentation of legal efforts against suspected terrorists. There are also frequent challenges to the legal foundations and processes resulting from these structural changes.[71] Media and judicial focus on detainees notwithstanding, these shifts are hardly limited to important but still relatively unusual situations like Guantanamo Bay incarcerations; in the nine years "[s]ince 9/11, the Department of Justice has indicted 998 defendants in terrorism prosecutions."[72]

These kinds of cases, where intelligence and law enforcement efforts are most likely to overlap, extend beyond high-profile militants to include financing, embryonic planning, and a vast array of "material support"[73] crimes.[74] They are also investigated in ways not limited by jurisdiction, either literal or figurative; terrorist financing, for example, can be investigated concurrently by intelligence and law enforcement agencies, both domestically and abroad, with the dual goals of prosecution and information gathering. Although these objectives are certainly not mutually exclusive, nor are they always compatible—especially when the government commences prosecution.

These types of terrorism prosecutions are frequent, broad-based, and here to stay.[75] Following a drop in the number of indictments after the initial post-9/11 reaction, terrorism cases

---

[71] *See, e.g.*, *In re* Sealed Case, 310 F.3d 717, 719 (FISA Ct. Rev. 2002).

[72] CTR. ON LAW & SEC., N.Y. UNIV. SCH. OF LAW, TERRORIST TRIAL REPORT CARD: SEPTEMBER 11, 2001–SEPTEMBER 11, 2010, at 4 (Karen J. Greenberg ed., 2010), *available at* http://www.lawandsecurity.org/Portals/0/documents/01_TTRC2010Final1.pdf (footnote omitted).

[73] It is a crime for any person to knowingly provide "material support or resources" to any foreign organization that has been designated by the Secretary of State as a "foreign terrorist organization." *See* 18 U.S.C.A. § 2339B (West 2011). "Material support or resources," for purposes of Section 2339B is defined as "any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel (1 or more individuals who may be or include oneself), and transportation, except medicine or religious materials [.]" 18 U.S.C.A. § 2339A(b)(1) (West 2011).

[74] TERRORIST TRIAL REPORT CARD: SEPTEMBER 11, 2001–SEPTEMBER 11, 2010, *supra* note 72, at 12.

[75] While NYU's Center on Law and Security published a 2010 edition of its annual "Terrorist Trial Report Card," *id.* at 1, the most recent comprehensive analysis is contained in the 2009 edition. CTR. ON LAW & SEC., N.Y. UNIV. SCH. OF LAW, TERRORIST TRIAL REPORT CARD: SEPTEMBER 11, 2001–SEPTEMBER 11, 2009, at iv (Karen J. Greenberg ed., 2010), *available at* http://www.lawandsecurity.org/Portals/0/documents/02_TTRCFinalJan142.pdf [hereinafter REPORT CARD].

have shown no signs of abating.[76] Such cases also are not limited in ways one might imagine: of the 804 individual terrorism-related defendants from 2001 to 2009 whose citizenship was identifiable, by far the most common citizenship was American.[77] Additionally, although fewer than half of the defendants had an identifiable alleged affiliation with a terrorist group, of those, the most common was not with a Jihadist faction, but rather with the Revolutionary Armed Forces of Columbia, or FARC, a group of Marxist insurgents.[78]

The potential for judicial exposure to intelligence practices and materials is substantial and growing. Given the nature of the fight against terrorist activities, and the dim prospect for a traditional victory or truce, it is also likely to continue indefinitely. Due to the increased number and variety of cases dealing with classified and otherwise protected information, the need for judicial understanding of the processes and products of the intelligence community is critical.

2. The Impact of Increased Government Secrecy

The massive recent increase in government secrecy is another critical reason why it is vital to consider judicial treatment of protected information. The importance of secrecy in many areas of national security policy and action is intuitively obvious, and much of the information claimed by the government as protected is classified. This secrecy can be manifested in virtually every stage of the production of classified material. In many instances, the sources of information are secret, the identities and motivations of the people gathering information are secret, the identities and motivations of those who analyze the collected information are secret, the policy decisions made based upon that analysis are secret, and actions resulting from those policies are secret. As a consequence of so much opacity, it is difficult for attorneys, judges, and juries to evaluate classified information.

---

[76] *See* REPORT CARD, *supra* note 75, at 3.
[77] *Id.* at 20.
[78] *Id.* at iii.

Government secrecy is nothing new, as events such as the Moynihan Commission and the Pentagon Papers demonstrate,[79] but in recent years, government secrecy has exploded. According to Ted Gup's *Nation of Secrets,* between 1997 and 2007, classification decisions more than doubled, and the government's figures indicate that in 2005 the United States established classifications an astonishing 14.2 million times.[80] As he notes, "That's 39,000 a day, or 1,600 every hour of the night and day. Four out of five of those documents were classified 'Secret' or 'Top Secret.' By definition, their disclosure threatens the security of the nation."[81]

In addition to the dramatic increase in the number of documents marked as classified, especially since 9/11, these materials are often grossly over-classified. Gup provides a particularly entertaining example in the context of explaining the excessive government focus on secrecy: "When it comes to secrecy and history, every historian has his own list of ludicrous cases. The James Madison Project's list is as good as any: on it is a Pentagon report classified 'top secret' that criticizes the excessive use of classification in the military . . . ."[82] Like government secrecy more broadly, this issue is not new; as far back as 1956, a Defense Department report warned, "overclassification has reached serious proportions."[83] The problem has continued, however, and as the number of classification designations has increased dramatically in recent years, so too has the problem of overclassification.[84] In 2007, Mark Agrast, who has since been appointed Deputy Assistant Attorney General in charge of national security issues, testified about this topic before the House Homeland

---

[79] Justice Potter Stewart's concurring opinion in the Pentagon Papers case was scathing on this point: "[W]hen 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." N.Y. Times Co. v. United States, 403 U.S. 713, 729 (1971) (Stewart, J., concurring).

[80] GUP, *supra* note 29, at 8.

[81] *Id.*

[82] *Id.* at 111.

[83] COMM. ON CLASSIFIED INFO., REPORT TO THE SECRETARY OF DEFENSE BY THE COMMITTEE ON CLASSIFIED INFORMATION 6 (1956), *available at* http://bkofsecrets.files.wordpress.com/2010/07/coolidge_committee.pdf.

[84] Steven Aftergood, Policy Essay, *Reducing Government Secrecy: Finding What Works*, 27 YALE L. & POL'Y REV. 399, 401 (2009) ("In recent years, in fact, classification—specifically overclassification—has increased, not diminished.").

Security Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment.[85] He condemned what he called an "epidemic of over-classification" stemming in part from "rules that resolve all doubts in favor of non-disclosure."[86] According to his testimony before Congress, there were nearly three times as many classification actions in 2004 as in the last year of the Clinton presidency.[87]

In 2006, following the release of heavily redacted Senate reports on the Iraq war, Senator Ron Wyden called the edits "a textbook case of abuse of the classification system," further elaborating, "[u]nfortunately, this sort of intelligence abuse has gone on for years."[88] Senator Carl Levin said that the classified portions contained "deeply disturbing information" and "cover[ed] up certain highly offensive activities . . . the public is entitled to the full picture."[89] This sentiment is not limited to politicians or to political progressives, either. In 1989, Erwin Griswold, former Solicitor General under President Nixon, wrote, "It quickly becomes apparent to any person who has considerable experience with classified material that there is massive overclassification and that the principal concern of the classifiers is not with national security, but rather with governmental embarrassment of one sort or another."[90] And in my personal experience,

---

[85] *Over-Classification and Pseudo-Classification: Making DHS the Gold Standard for Designating Classified and Sensitive Information: Hearing Before the Subcomm. on Intelligence, Info. Sharing, and Terrorism Risk Assessment of the H. Comm. on Homeland Sec.*, 110th Cong. (2007) (testimony of Mark D. Agrast, Senior Fellow, Ctr. for Am. Progress), *available at* http://www.americanprogress.org/issues/2007/06/pdf/Agrast_Testimony_0628.pdf.

[86] *Id.*at 2–3; *Over-Classified and Pseudo-Classified: Testimony of Mark Agrast*, CTR. FOR AM. PROGRESS, http://www.americanprogress.org/issues/2007/06/overclassified.html (last visited Mar. 24, 2012).

[87] *Over-Classification and Pseudo-Classification: Making DHS the Gold Standard for Designating Classified and Sensitive Information: Hearing Before the Subcomm. on Intelligence, Info. Sharing, and Terrorism Risk Assessment of the H. Comm. on Homeland Sec.*, 110th Cong. 3 (2007) (testimony of Mark D. Agrast, Senior Fellow, Ctr. for Am. Progress).

[88] Press Release, Office of Senator Ron Wyden, Wyden: Intelligence Reports Overclassified, Public Should Have Access to More (Dec. 6, 2006), *available at* http://wyden.senate.gov/newsroom/press/release/?id=d5875b96-6aba-48c5-9bd6-7e13e7760a30.

[89] Press Release, Office of Senator Carl Levin, Senate Floor Statement on the Senate Intelligence Committee's Phase II Report (Sept. 8, 2006), *available at* http://levin.senate.gov/newsroom/release.cfm?id=262690.

[90] Erwin N. Griswold, Editorial, *Secrets Not Worth Keeping; The Courts and Classified Information*, WASH. POST, Feb. 15, 1989, at A25.

while an analyst at the Defense Intelligence Agency ("DIA"), I was sometimes told by superiors to increase the level of classification on my reports for reasons completely unrelated to the informational content. As someone with the kind of "considerable experience with classified material"[91] that Griswold mentions, I wholly agree with his sentiments, and the post-9/11 governmental reaction has likely made this problem worse than ever before.

This is not to say that no information, debate, or decisions should be confidential, of course. But the huge growth in volume of secret materials, the classifications of which are too often of dubious legitimacy or origin, has profound implications for the responsibility of courts to understand the content of intelligence materials. This is especially true given the increasingly blurred line between law enforcement and intelligence roles and actions, as well as the expansion of international investigations in law enforcement efforts. Many observers have suggested ways to stem the tide of overclassification, perhaps most notably Steven Aftergood, who has made a number of trenchant suggestions; those avenues should be evaluated and pursued where appropriate.[92] Meanwhile, in the absence of effective reform—or even in conjunction with it—there will be tremendous amounts of classified information in government, much of which could end up involved in legal processes. The large number of terrorism-related prosecutions, massive increase in government classifications, and conflation of policing and spying all strongly indicate that courts will continue to encounter protected materials. Judges must therefore be prepared to engage with them in a sophisticated manner.

3. Advocacy for Greater Judicial Responsibility

Judicial attitudes regarding protected information have been, with limited exceptions, tremendously deferential to the Executive branch. Beginning with the *Reynolds* case, where the Supreme Court declined to even look at the allegedly secret evidence upon which it would base its sweeping and influential ruling,[93] and continuing in the decades after that ruling, courts have mostly avoided significant engagement with secret

---

[91] *Id.*

[92] *See, e.g.*, Aftergood, *supra* note 84, at 411.

[93] United States v. Reynolds, 345 U.S. 1, 10–11 (1953).

materials.[94] Judges generally have been content to accept government claims, perhaps influenced by inexperience in the workings of this kind of information and the lack of guidance or support by *Reynolds* and its progeny for delving into the details of protected information.[95] Cases involving CIPA can be an exception to this rule, generally because the government has an incentive to admit classified materials—or acceptable substitutes—in order to continue with prosecutions. But even in CIPA, there is broad deference to government claims of secrecy, and, importantly, the statute contains no standards for a court to apply to evaluate whether an assertion of the privilege is actually valid.[96]

This persistent acquiescence, however, now faces growing challenges from Congress, academics, and even courts themselves in rare but important instances. Law journals are replete with criticisms of the SSP and the increased use of classified information more generally, and scholars have suggested a number of ways to reform the process of admitting protected material into evidence. These writers propose a variety of changes, such as codification of a more structured, CIPA-like process for SSP; administrative approaches to evidence evaluation; and greater use of courts' existing ability to review protected materials in a wide range of contexts.[97]

Additionally, while some observers expected policies in this area of the law to shift under President Obama, the continuation of many national security and secrecy policies from the previous administration makes it likely that the scholarly chorus for change will continue—and perhaps intensify. Lay observers have voiced concerns similar to those of legal scholars, even in the wake of Executive branch reforms, which the *New York*

---

[94] *See* Weaver & Pallitto, *supra* note 31 ("Even though *Reynolds* held that 'judicial control over the evidence in a case cannot be abdicated to the caprice of executive officers,' the practical effect of the decision is to cause precisely that result."); *see also supra* notes 42 & 44 and accompanying text.

[95] *See* Weaver & Pallitto, *supra* note 31, at 101–02.

[96] LIU, *supra* note 19, at 7.

[97] *See, e.g.*, J. Steven Gardner, Comment, *The State Secret Privilege Invoked in Civil Litigation: A Proposal for Statutory Relief*, 29 WAKE FOREST L. REV. 567, 601–09 (1994) (advocating compensation schemes in connection with state secrets invocation); D.A. Jeremy Telman, *Our Very Privileged Executive: Why the Judiciary Can (and Should) Fix the State Secrets Privilege*, 80 TEMP. L. REV. 499, 527 (2007) (arguing for judicial solutions regarding the privilege); George, *supra* note 59, at 1716–23 (suggesting administrative options).

Times criticized as "hardly a total fix."[98] Rather than alleviating concerns about government abuse of these processes, the actions of the Obama administration have reinforced them.[99]

Congress has joined the reform effort as well; bills introduced in both the House and the Senate in the most recent two full sessions of Congress would provide some direction and transparency in the use of the SSP.[100] According to the Congressional Research Service ("CRS"), this legislation would codify the SSP, which, despite decades of recognition and use, remains unaddressed by Congress.[101] The laws would ostensibly limit the use of the privilege to evidence the government could demonstrate would cause "significant" harm to national security if revealed, a standard that appears higher than what is now required by *Reynolds* and related cases.[102] It is therefore possible that the bills would require both greater government proof and a higher actual level of harm to be demonstrated before the privilege would apply.[103] Also, because a large amount of classified information might not cause "significant" harm to national security if revealed,[104] some classified material might not be protected.[105]

---

[98] *See* Editorial, *An Incomplete State Secrets Fix*, N.Y. TIMES, Sept. 29, 2009, at A38.

[99] *See id.*; John Schwartz, *Obama Backs Off a Reversal on Secrets*, N.Y. TIMES, Feb. 10, 2009, at A12 (noting surprise and displeasure from some observers when President Obama declined to alter the approach to the SSP, upon taking office, in a pending case).

[100] *See supra* notes 4, 55–57 and accompanying text.

[101] *See* LIU, *supra* note 19, at 12.

[102] *See id.* ("Both bills would also require a showing of 'significant harm' before the privilege may apply. In contrast, courts applying *Reynolds* have generally not required that the harm to national security be 'significant' in magnitude.").

[103] *Id.*

[104] For example, by definition, information classified as "[c]onfidential," the lowest level of classification, is that which "could be expected to cause damage to the national security," a standard which might not meet the requirements of the proposed legislation in certain circumstances. *See* Exec. Order No. 12,958, 60 Fed. Reg. 19,825, § 1.3(a)(3) (Apr. 17, 1995), *repealed by* Exec. Order No. 13,526, 75 Fed. Reg. 707, § 1.2(a)(3) (Dec. 29, 2009).

[105] This is neither surprising nor necessarily problematic; classified information that would not cause significant harm to national security arguably ought to yield to the interests of justice and fairness in a court of law, if the information is vital to the case and the government cannot show that it should be concealed for legitimate security reasons.

The proposed legislation mandates judicial review of the information claimed to be privileged and requires the Attorney General to notify Congress of any assertion of the SSP within thirty days of the invocation.[106] The bills would further allow federal courts to order the government to provide a redacted, unclassified, or summary substitute of filings or motions to other parties, and would give judges the power to determine which evidence could be submitted and examined *ex parte*.[107] The proposed laws also formalize long-accepted elements of the privilege, such as authorizing the United States to intervene in any civil suit to protect information that may include state secrets and requiring that the head of an agency formally assert the privilege after actual consideration.[108] If the bills were enacted in anything close to their forms as previously introduced, judicial responsibility for evaluating and making determinations about protected information would increase dramatically.[109]

Finally, some courts are beginning to assert themselves in this area, due to practical or statutory influences or, in some instances, obvious frustration with Executive overreach regarding classified materials.[110] Some of these cases will be examined in depth in Part III, but here it suffices to say that court action itself—halting and infrequent as it may be—is another indicator of the growing pressure for, and likelihood of, an increased judicial role in managing the use of government secrets in litigation.

All of these forces are working toward reform of legal structures and practices regarding secret information. Success in these efforts, from any of the current sources of advocacy, would substantially alter the judicial environment when protected information is at issue. Even under the current approaches and structures, there is an increasing need for participants in the legal system to have an understanding of government secrecy. And implementation of *any* of the proposed changes could drastically augment the interaction between courts and protected information.

---

[106] State Secrets Protection Act, S. 417, 111th Cong. § 4058(a)(1) (2009).

[107] *Id.* § 4052(a)–(b).

[108] *Id.* § 4053.

[109] These proposals, however, have languished; none of the four bills introduced, two each in the Senate and House in consecutive congressional sessions, has reached the floor for a vote. *See* supra note 4.

[110] *See supra* note 2 and accompanying text.

The many forces arguing for change, in addition to the increase in the use of protected information and the cases that involve it, demonstrate that the treatment of government secrets is a vital and growing part of our judicial system. In addition to being one of the most important elements of modern jurisprudence, however, it is also one of the least discussed and understood. It is therefore critical for lawyers, judges, and legal academics to better understand what "intelligence" is—how it is cultivated and produced, how it should be understood, and, most importantly, how it can be utilized. There are certain practices and pathologies involved in protected information, particularly classified intelligence products, that are new and unusual for courts. These elements of classified and secret materials, including content and procedure alike, are neither self-explanatory nor intuitively obvious. They must therefore be explained and analyzed.

II. UNITED STATES INTELLIGENCE: WHO, WHAT, AND HOW . . . AND WHY IT MATTERS

Knowing how to view, evaluate, and understand classified information is neither intuitive nor widely understood in the legal community, and judges, clerks, lawyers, and litigants are increasingly likely to encounter protected materials in important legal situations. Accordingly, some guidance regarding the world of intelligence may be useful. The following is an attempt to provide a brief introduction, with particular attention to issues of legal relevance.

A. Classifications

The general rules governing classified information are updated regularly through Executive Orders; as of this writing, the most recent issuance of these rules was by President Obama on December 29, 2009, via Executive Order 13,526.[111] Those with the authority to classify information may do so when, among other things, its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to national security.[112] In general, such information must pertain to military particulars, intelligence activities, foreign government

[111] *Supra* note 104.

[112] Exec. Order No. 13,526, 75 Fed. Reg. 707, §§ 1.2, 1.4 (Dec. 29, 2009).

information, technology and weapons of mass destruction, and the like.[113] Information may not be designated as classified for reasons including concealing violations of law or governmental error; preventing embarrassment to a person, organization, or agency; or restraining competition.[114]

Classified information is generally designated in one of three categories: Confidential, the lowest classification level, includes information that would "damage" national security if revealed;[115] Secret, the middle level classification, is information whose disclosure would cause "serious damage" to national security;[116] and Top Secret ("TS"), the highest security designation category that is publicly disclosed, covers information that would cause "exceptionally grave damage" if divulged.[117] There are also some restrictions on unclassified materials, including designations that apply to court orders, ongoing investigations, and information not subject to Freedom of Information Act requests.[118] Access to classified material is granted generally on a "need-to-know" basis; [119] that is, a person with a TS clearance generally has access only to Top Secret materials that are relevant to her work. These restrictions against information disclosure are designed to protect, among other things, "sources" or "methods" of intelligence collection, whether technological or human.[120]

Additional classifications, including "code word" designations, are subsets, or "compartments," of material within these broader designations. Code words are not themselves designators of classification levels, but they can help organize access to certain projects or subjects, or identify the

---

[113] *Id.* § 1.4.

[114] *Id.* § 1.7(a).

[115] *Id.* § 1.2(a)(3).

[116] *Id.* § 1.2(a)(2).

[117] *Id.* § 1.2(a)(1).

[118] These restricted unclassified designations include, but are not limited to, For Official Use Only ("FOUO"), Sensitive But Unclassified ("SBU"), and Law Enforcement Sensitive ("LES"). On May 7, 2008, President Bush issued a directive to consolidate some classification categories, including the three listed here, into a single designation: Controlled Unclassified Information ("CUI"). Memorandum on Designation and Sharing of Controlled Unclassified Information (CUI), 44 WEEKLY COMP. PRES. DOC. 673 (May 12, 2008) (establishing a new framework for "Controlled Unclassified Information").

[119] Exec. Order No. 13526 § 4.1(a), 75 Fed. Reg. 707 § 4.1(a).

[120] *Id.* § 1.4.

source of certain information; code words themselves are sometimes classified.[121] In addition, the designations "Sensitive Compartmented Information" ("SCI") and "Special Access Program" ("SAP") are identifiers, not classification levels, though additional screening processes can be required to access those categories of information. For example, to become an intelligence officer with DIA, I had to pass an initial security background check for a Top Secret/Secure Compartmented Information ("TS/SCI") clearance level; once I had that clearance, additional "code word" inclusions could be added as needed.

Classification authority can be either "original," where information is designated classified for the first time, or "derivative," where previously classified information is used or incorporated in new materials.[122] Original classification authority is ostensibly very restricted, available only to the President, Vice President, agency heads, and government officials delegated this authority under limited circumstances.[123] In reality, this prerogative is extensively transferred; the sheer volume of new intelligence information requires frequent delegation of original classification authority. Derivative classification is simply the product of existing classified information being reproduced, used, or summarized in new or additional work.[124] A classified document as a whole is marked at the highest classification of any of its contents; for example, if a twenty-page report contains information from unclassified, Secret, and Top Secret sources, its overall classification is Top Secret.[125] Most classified materials are subdivided by designation, so each heading and paragraph, for example, may have its own classification label.[126]

---

[121] *See, e.g.*, Memorandum from the Chief of Naval Operations, Dep't of the Navy, OPNAV Instruction 5511.37D, 5(b) (Jan. 30, 2007), *available at* http://www.fas.org/irp/doddir/navy/opnavinst/5511_37d.pdf ("A code word is a single word assigned a classified meaning by appropriate authority to ensure proper security concerning intentions and to safeguard information pertaining to actual, real-world military plans or operations classified as CONFIDENTIAL or higher once activated.").

[122] Exec. Order No. 13,526 §§ 1.1, 2.1, 6.1(o), 6.1(ff), 75 Fed. Reg. 707 §§ 1.1, 2.1, 6.1(o), 6.1(ff) (Dec. 29, 2009).

[123] *Id.* § 1.3(a)–(c).

[124] *Id.* § 2.1(a).

[125] *Id.* § 2.1(b)(3)(a)–(b).

[126] *See, e.g.*, INFO. SEC. OVERSIGHT OFFICE, MARKING CLASSIFIED NATIONAL SECURITY INFORMATION 4 (Oct. 2007) ("The first step in the marking process is to

In theory, this is a highly controlled and regulated practice; the laws and executive orders governing classified information appear to severely limit the people who can create classifications and the ways they can do so. In practice, however, it is relatively easy for analysts and officials to assign classifications with little rhyme or reason, other than making sure any derivative classification is at least as high as the source material. In my team at DIA, for example, it was not uncommon for analysts to make decisions about classifications on original documents, and we would often increase the designations beyond those of the source material. It was widely understood that consumers—the word used for those who would read the materials we created—were likely to dismiss unclassified analysis, believing it unimportant if it did not come from classified sources. So even if a product was based on unclassified, or "open source," information, it was not unusual for analysts to label it Top Secret to increase its perceived validity or importance, either by our own volition or at the direction of superiors. This problem, along with a number of others beyond my personal experience, led to the extensive overclassification described above.[127]

B. The Intelligence Community

The entities that produce and use secret information for analysis and action fall almost exclusively under the purview of the Executive branch. Congress has oversight authority through, among other things, committees on intelligence and the armed services, and the judiciary sometimes becomes involved with intelligence policy and practices, but government secrets are primarily created and used by Executive branch entities. There are seventeen distinct agencies, departments, and elements that collectively make up a group generally referred to as the "intelligence community." That includes well-known components such as the CIA and FBI, as well as lesser-known entities, many of which are parts of the Department of Defense.[128] Although

identify the classification level of each portion. A portion is ordinarily defined as a paragraph, but also includes charts, tables, pictures, and illustrations, as well as subjects and titles."), *available at* http://www.archives.gov/isoo/training/marking-booklet.pdf.

[127] *See supra* Part I.B.2.

[128] The complete list is as follows: Central Intelligence Agency ("CIA"), an independent agency; Army Military Intelligence ("MI"), Marine Corps Intelligence Activity ("MCIA"), Office of Naval Intelligence ("ONI"), Air Force Intelligence,

these groups are governed by their home departments and agencies, they are also overseen generally by the Director of National Intelligence ("DNI"), a cabinet-level official who is responsible for advising the President, managing intelligence collection and analysis activities, and facilitating coordination between the entities, many of which have historical bureaucratic rivalries with one another.[129] Collectively, individuals in these entities gather, create, and analyze classified materials.

Individual roles are broadly separated into two categories, each having very different responsibiliteis: collectors of raw intelligence and producers of "finished" intelligence. Collection occurs in a variety of ways, and the government's intelligence community website lists six basic sources: Signals Intelligence ("SIGINT"), the interception of signals between people and/or machines; Imagery Intelligence ("IMINT"), the representation of objects reproduced electronically or by optical means, such as via visual photography, radar sensors, infrared sensors, or electro-optics; Measurement and Signature Intelligence ("MASINT"), which focuses on distinctive characteristics of specific targets, such as nuclear, radio frequency, acoustic, or seismic identifications; Geospatial Intelligence ("GEOINT"), involving imagery and mapping data of the earth; Open-Source Intelligence ("OSINT"), from publicly

---

Surveillance and Reconnaissance Agency ("AFISRA"), National Geospatial Intelligence Agency ("NGA"), National Reconnaissance Office ("NRO"), National Security Agency ("NSA"), and Defense Intelligence Agency ("DIA")—all of which are elements of the Department of Defense; Office of Intelligence and Counterintelligence ("OICI") in the Department of Energy; Coast Guard Intelligence ("CGI") and Office of Intelligence and Analysis ("I&A"), both in the Department of Homeland Security; Federal Bureau of Investigation ("FBI") and Drug Enforcement Administration ("DEA"), both in the Department of Justice; Bureau of Intelligence and Research ("INR"), of the Department of State; and Office of Intelligence and Analysis ("INA") in the Department of the Treasury. *Member Agencies: Our Strength Lies in Who We Are*, INTELLIGENCE.GOV, http://intelligence.gov/about-the-intelligence-community/member-agencies/ (last visited Mar. 25, 2012) [hereinafter IC Website].

[129] The DNI position was created by the Intelligence Reform and Terrorism Prevention Act of 2004 ("IRTPA") and strengthened by Executive Order 13,470, signed by President Bush on July 30, 2008. *See* Exec. Order No. 13,470, 73 Fed. Reg. 45,325 (July 30, 2008).

available information; and, most famously, Human-Source Intelligence ("HUMINT"), information derived from human sources.[130]

Measured by budget and manpower, the overwhelming focus of United States intelligence is on SIGINT. Although precise employment and budget numbers for these entities are classified, the NSA is widely reported to employ around 30,000 people, making it by far the largest intelligence community member, and NRO reportedly has the largest budget; these two agencies lead the way in technology-based spying.[131] HUMINT, despite conjuring up images of James Bond or Jason Bourne, is often collected by overt actors such as diplomats and military attaches. A large amount of HUMINT is produced from "walk-in" sources, individuals who make themselves available to American personnel for ideological or financial reasons.[132]

Still, despite being a relatively small part of United States intelligence as measured by budget and manpower, HUMINT is instrumental in the formation of predictive and, especially, investigatory analysis. While satellite photos and communication intercepts are critical for strategic purposes and high-level spying, at the ground level, intelligence agencies tend to get information about individuals the same way law enforcement entities do: from people. And with relatively little information about sources passing between collectors to analysts, as well as no opportunity for anything like the cross-examination right found in our criminal justice system, there is great opportunity for sources to promulgate misinformation due to error or self-interest.

---

[130] *Data Gathering*, INTELLIGENCE.GOV, http://intelligence.gov/about-the-intelligence-community/how-intelligence-works/data-gathering.html (last visited Mar. 25, 2012).

[131] *See, e.g.*, RICHARD A. CLARKE, YOUR GOVERNMENT FAILED YOU: BREAKING THE CYCLE OF NATIONAL SECURITY DISASTERS 95 (2008) ("The National Reconnaissance Office (NRO), widely thought to be the most expensive of the agencies, builds and runs satellites that collect intelligence from space."); Vernon Loeb, *Critics Questioning NSA Reading Habits; Politicians Ask if Agency Sweeps in Private Data*, WASH. POST, Nov. 13, 1999, at A03 ("[T]he NSA . . . [has] well over 30,000 employees . . . .").

[132] EDWARD WALTZ, KNOWLEDGE MANAGEMENT IN THE INTELLIGENCE ENTERPRISE 37–38 (2003) ("HUMINT sources may be . . . recruited or 'walk-in' volunteers who act for a variety of ideological, financial, or personal motives.").

The goals of the intelligence community are straightforward. Most broadly, it aims to protect the national security of the United States. That involves knowing about other countries and non-state actors—what they are doing, planning, and thinking about; where they are; and the extent of their capabilities. This can have military, diplomatic, or political implications, and the objective is to have the maximum amount of information about others while revealing the minimum possible to external forces.

More specifically, intelligence is geared toward three categories of analysis: retrospective, current, and predictive. Retrospective analysis looks back at events of behaviors and attempts to put them in context, explaining the relevant factors and causes. This can include meta-analysis—looking at whether/how/why the United States did or did not predict the analytical subject. Naturally, retrospective evaluation informs contemporary and forward-looking judgments. Current analysis covers a range of subjects and issues, including biographical assessments, determining the location and force constructions of foreign militaries, leadership and succession structures of nations and non-state actors, and any number of other contemporaneous subjects. Notably, it also includes investigative efforts, such as attempting to determine whether a detainee is an enemy combatant. Predictive intelligence looks ahead to future events, attempting to foresee events and behaviors based on current and retrospective evaluation.

1. "Finished" Analysis

All of those types of assessments go from collection to production and dissemination through a complex and often lengthy process. The result is called "finished intelligence."[133] The days of an analyst are spent sifting through classified materials, delivered to various electronic accounts by way of targeted searches and filters in report aggregators and product repositories. There is no shortage of available classified information; analysts' attempts to convert the flood of information into relevant, usable products are often compared

[133] *Analysis and Reporting*, INTELLIGENCE.GOV, http://intelligence.gov/about-the-intelligence-community/how-intelligence-works/analysis-reporting.html (last visited Mar. 25, 2011).

to trying to drink from a fire hose.[134] Analysts sift through information for hours every day, working on current intelligence products (such as daily PowerPoint slides or quick-turnaround reports) as well as long-term papers that can take weeks or months to complete. As Richard Clarke, former chief counter-terrorism advisor on the National Security Council, put it: "All of that collection of intelligence (the signals, the pictures, the spies) is designed to give the other side of the intelligence community the raw material to do its job. The other side, which is far smaller in terms of people and budget, is analysis."[135]

The United States intelligence community website describes the conversion of source materials into finished documentation thusly: "This includes integrating, evaluating, and analyzing all available data—which is often fragmented and even contradictory—and distilling it into the final intelligence products, which highlight information on topics of immediate importance or make long-range assessments."[136] Analysts work within their respective fields, integrating data "into a coherent whole," providing context and personal evaluation into a resultant finished product "that includes assessments of events and judgments about the implications of the information for the United States (U.S.)."[137] Or, as Clarke more succinctly states: "Analysis is meant to answer questions that decision makers ask—or should ask. . . . That is what intelligence is all about: answering important questions, often based on hard-to-get information, and providing warnings to policy makers."[138]

The late General William Odom, former director of the NSA and assistant chief of staff for intelligence in the United States Army, lamented influences unrelated to the needs of policymakers: "Structural problems afflict not only intelligence

---

[134] *See, e.g.*, Joseph S. Nye, Jr., *Peering into the Future*, FOREIGN AFFAIRS, July–Aug. 1994, at 82, 91 (1994) ("They spend their days drinking from a fire hose of information."); Spencer Ackerman, *Is this Really an Intelligence Failure? Real Talk on Abdulmutallab*, WASH. INDEP. (Dec. 31, 2009, 9:09 AM), http://washingtonindependent.com/72807/is-this-really-an-intelligence-failure-real-talk-on-abdulmutallab ("The intelligence community is drinking from a fire hose of data . . . .").

[135] CLARKE, *supra* note 131, at 96.

[136] *Analysis and Reporting*, *supra* note 133.

[137] *Id.*

[138] CLARKE, *supra* note 131, at 96.

collection but also intelligence analysis."[139] These structural difficulties, not surprisingly, sometimes produce unsound results. When "Rick MacKenzie" (a pseudonym), a very high-level analyst for DIA—and an attorney—retired in 2006 after thirty-eight years of intelligence work, he sent an email to many of his colleagues that discussed, in part, some of the challenges facing the intelligence community: "Something remains fundamentally wrong with analysis. . . . One must sense a crisis in analysis, in the management of analysis, in the training of analysts and in the intellectual curiosity of analysts . . . . As near as I have been able to judge, the pathology affects all agencies."[140]

These problems and criticisms are noted not to criticize intelligence agencies or their employees—who are overwhelmingly hard-working and principled—but rather to counter the notion that classified intelligence should be accepted uncritically, or even that it should be granted special accreditation due to its clandestine provenance. Indeed, the unilateral aspects of intelligence analysis, which can be both produced and exacerbated by persistent structural problems or individual political/careerist motivations, make it vital that courts thoroughly evaluate finished intelligence.

Clarke, though neither a lawyer nor focused on the role of intelligence in courts, made this point implicitly but insightfully in the context of discussing problems resulting from groupthink:

> A bad detective decides who is guilty and then sets about to prove it, unjustly accusing an innocent man. Yet in criminal cases, the prosecution is legally required to provide the defense with any exculpatory evidence it turns up. The cops have to give the defense counsel anything they have that could prove the accused to be innocent. Not so in bad intelligence analysis.[141]

---

[139] WILLIAM E. ODOM, FIXING INTELLIGENCE: FOR A MORE SECURE AMERICA 5 (2d ed. 2003). Odom, U.S. Army (Ret.), was formerly the director of the National Security Agency.

[140] A. J. ROSSMILLER, STILL BROKEN: A RECRUIT'S INSIDE ACCOUNT OF INTELLIGENCE FAILURES, FROM BAGHDAD TO THE PENTAGON 176 (2008).

[141] CLARKE, *supra* note 131, at 130–31. Joseph F. Nye, former chairman of the National Intelligence Council, makes a similar metaphorical point: "Why take the risks [of estimative analysis]? Why not stick strictly to the facts? One reason is that facts about crucial international issues are rarely conclusive. There is often enough evidence to indict, rarely enough to convict." Nye, *supra* note 134, at 83.

This is a critical point and a useful comparison when considering both the weight and the probative effect of protected materials.

In criminal investigations, the "beyond a reasonable doubt" standard required for conviction drives the evidentiary process. The government's incentive to convict is balanced by a number of factors, including the professional duties of prosecutors to act in the interests of justice—as well as to disclose exculpatory evidence[142]—rather than just their "side" of the litigation. The government is also constrained by the weighty constitutional protections of the Fourth, Fifth, Sixth, and Fourteenth Amendments. Civil law provides its own protections, most notably in the general prohibition of punitive measures beyond monetary penalties, as well as the extensive requirements of civil discovery. In addition, parties in any civil or criminal proceeding must craft a narrative from demonstrable evidence and provable facts, giving judges or juries the responsibility of deciding questions of fact.

Conversely, these kinds of protections—the right of confrontation, discovery, *Brady* rules, specified burdens of proof, etcetera—do not exist in the *formation* of intelligence. If the protected material is raw intelligence, such as a satellite photo or a transcript of an intercepted communication, this problem may be mitigated. With "finished" intelligence, however, or even raw HUMINT, sources are generally subsumed in the broader analysis, precluding examination of the information's origins. A court would be appalled if the proof offered against an average criminal defendant consisted of a summary analysis of the evidence by a detective, concluding that the suspect was guilty based on physical and testimonial evidence that could not be evaluated or challenged. And yet that is how many courts treat intelligence reports under current laws and practices.[143] In intelligence, the analyst is the fact-finder, so when those judgments enter the judicial system, they have circumvented the usual checks and protections we normally value so highly.

---

[142] Brady v. Maryland, 373 U.S. 83, 87–88 (1963).

[143] Benjamin Wittes et al., *The Emerging Law of Detention: The Guantánamo Habeas Cases as Lawmaking* 35–37, 40–41 (Brookings Governance Studies Paper, 2010), *available at* http://www.brookings.edu/~/media/Files/rc/papers/2010/0122_guantanamo_wittes_chesney/0122_guantanamo_wittes_chesney.pdf.

2. Reliability and Credibility

In addition to the structural elements implicated by court use of intelligence materials, there are also individualized factors to consider. A draft piece of finished intelligence is only the beginning of the analytical process, and innumerable people and influences can shape the content of a product as it is finalized. While specific methods vary by office, in my experience—and that of many colleagues—the process of editing and approval for publication was nebulous, convoluted, and, at times, intensely political.[144]

For a written paper, an analyst would either address a subject she felt was important based on incoming information, or "traffic", or a supervisor would assign a subject. After being researched and written, the paper would begin its march up the chain of command. It would first go to an analyst's immediate supervisor, her team chief, who would return it with edits and comments to incorporate. A revised version would then go to the immediate team members, usually three to five people, for additional input. After those changes were incorporated, it would go to a broader group, allowing another 20 to 25 people to comment. Upon approval from that larger group, the product would be sent to the senior analyst and deputy team chief of the division, reflecting the dual track of management and analytical leadership, and they would make edits. Through this stage of the process, comments and suggestions were "optional," such that if the author disagreed, she could argue against the changes.

Following those layers of editing, the paper would go to division leadership, a senior manager and senior analyst. At that level, disputing changes was theoretically possible but rarely attempted, and the power asymmetry became substantial. After the approval of those two leaders, the product would move to office-level personnel—the entire Iraq section of the Agency, including managers and analysts. Paradoxically, at this stage, while everyone had input, any of the office-level senior analysts ("OSAs") could approve the product for publication. Analysts therefore worked to ascertain the specific views and predilections of each OSA, quickly becoming adept at assessing the likely

[144] The following description borrows from my book, ROSSMILLER, *supra* note 140, at 135–36.

respective responses to an argument or position. We could then game the system by making sure the product moved up the chain of command when the desired OSA was on duty.

No matter which OSA reviewed the product, however, edits could be bounced back and forth indefinitely between analyst and OSA until the latter granted publication approval. As I later described while writing about this system, "The process was extensive and often convoluted. Much as with judges or baseball umpires, people were ostensibly adhering to the same conventions, but their interpretations and personal preconceptions could greatly affect both the pace and direction of a product . . . . Not surprisingly, this process continually broke down."[145]

Many intelligence products are written without bias or insidious external influences; some, however, are affected by factors that threaten the reliability and credibility of the analysis. In particular, when judgments are likely to be made public or used for a specific purpose such as court proceedings, rather than the more general (and infinitely more common) goal of informing policymakers, problems can result.[146] There is less room for manipulation—by analysts or managers at any stage of the process—when addressing a question like, "What are the primary current political goals of Country X?" than one such as, "Is Detainee Y an enemy combatant?," simply because everyone knows the "right" (that is, desired) answer in the latter example.[147]

---

[145] *Id.* at 136. *But see* CLARKE, *supra* note 131, at 345 (discussing the potential benefits of extensive review and editing processes).

[146] *See, e.g.*, John McCreary & Richard A. Posner, *The Latest Intelligence Crisis*, 23 INTELLIGENCE & NAT'L SECURITY 371 (June 2008) (questioning the validity of intelligence judgments that are likely to be made public).

[147] *See, e.g.*, Reply to Opposition to Petition for Rehearing at app. vi, Al Odah v. United States, No. 06-1196, 2007 WL 4790792 (June 22, 2007) (declaration of Stephen Abraham, Lieutenant Colonel, United States Army Reserve, describing events regarding Combat Status Review Tribunal ("CSRT") procedures: "It was well known by the officers in OARDEC that any time a CSRT panel determined that a detainee was not properly classified as an enemy combatant, the panel members would have to explain their finding to the OARDEC Deputy Director. There would be intensive scrutiny of the finding by Rear Admiral McGarrah who would, in turn, have to explain the finding to his superiors, including the Under Secretary of the Navy.").

In any analysis, there can be problems of cherry-picking facts, omitting certain materials, failing to appropriately scrutinize sources, or being provided erroneous information, among other things. These problems and influences in analysis are well-documented, and Clarke explained the potential negative consequences when products are insufficiently rigorous or transparent: "The rationale for decisions, dissents, and alternatives, the weight given various considerations, the accuracy of facts, the expertise brought to bear, excursions considering unexpected results should all be transparent to decision makers. Without such information, decision makers must, by definition, make uninformed choices."[148] The fact that Clarke recommends this approach as part of his suggestions for intelligence reform strongly indicates that it is sometimes not done this way. Similarly, when courts use protected materials that fail to meet this bar, they too make uninformed choices.

Analysis can be affected by all kinds of influences—including structural as well as personal factors—in ways that are generally absent from the types of evidence usually presented in court. Critically, analytical judgments about questions like "is this detainee an enemy combatant?," or "did this suspect have ties to terrorist groups?," are themselves conclusions made based on accumulated evidence that often would not meet the standards of reliability and credibility usually required in a court of law. For policymaking, acting based on analysts' best estimates makes sense and is necessary. But history is replete with examples of intelligence getting it wrong, and for courts to grant *extra* deference—and perhaps even extra probative value—to protected materials effectively short-circuits principles of evidence and burdens of proof that are otherwise considered sacrosanct.[149]

C. Reading and Understanding Intelligence Products

While it may seem superfluous to discuss the literal composition of intelligence products, these kinds of materials are often written in a mannered and idiosyncratic fashion. Not understanding the particularities of language and structure in

---

[148] CLARKE, *supra* note 131, at 346.

[149] *See, e.g.*, 1 CLIFFORD S. FISHMAN & ANNE T. MCKENNA, JONES ON EVIDENCE § 5:1–26 (7th ed. 2011); 2 CHRISTOPHER B. MUELLER & LAIRD C. KIRKPATRICK, FEDERAL EVIDENCE § 5:54 (3d ed. 2011); 2 DAVID M. GREENWALD, ET AL., TESTIMONIAL PRIVILEGES § 9:16 (3d ed. 2010).

analysis can easily lead to misinterpretation, so it is worthwhile to briefly address these elements of protected information. Analytical judgments are estimates: the products of assembled evidence that is often confusing, contradictory, or of questionable origin. One of the most important elements of an analyst's job is to separate good raw intelligence from bad raw intelligence—to have a combination of knowledge and intuition that allows for accurate and efficient processing of a vast stream of information. Due to the nature of that information, much of which is often ambiguous or uncertain, as well as the common problem of missing pieces, conclusions are necessarily equivocal.

Major estimates are built on multiple component evaluations, and as those informed guesses are stacked upon one another, deductive foundations can become unsteady. As Clarke has written, as long as products are transparent and properly qualified, that is sufficient for the goals of intelligence analysis; but for policy matters, decisions have to be made based on best estimates, not certainties.[150]

For courts, however, not only is this level of uncertainty usually inadequate, but the language used to communicate caveats can also be confusing or misleading. When the United States releases unclassified versions of intelligence reports, particularly "National Intelligence Estimates" ("NIEs"),[151] it sometimes includes an "explanation of estimative language."[152]

---

[150] CLARKE, *supra* note 131, at 346; *see also* Nye, *supra* note 134, at 82–83 ("Like all kinds of intelligence, estimative intelligence starts with the available facts, but then it trespasses into the unknown and the unknowable—the regions where we simply lack facts.... [P]olicymakers are under enormous pressure to make decisions. In some cases they can wait for more information, but in others waiting is itself a decision with irreversible consequences.... To help policymakers interpret the available facts ... to provide informed assessments of the range and likelihood of possible outcomes—these are the roles of estimative intelligence.").

[151] Unclassified versions of NIEs generally contain the following descriptive explanation: "National Intelligence Estimates (NIEs) are the Intelligence Community's (IC) most authoritative written judgments on national security issues and designed to help US civilian and military leaders develop policies to protect US national security interests. NIEs usually provide information on the current state of play but are primarily 'estimative'—that is, they make judgments about the likely course of future events and identify the implications for US policy." NAT'L INTELLIGENCE COUNCIL, NATIONAL INTELLIGENCE ESTIMATE: IRAN: NUCLEAR INTENTIONS AND CAPABILITIES (2007), *available at* http://www.dni.gov/press_releases/20071203_release.pdf.

[152] *Id.*; NAT'L INTELLIGENCE COUNCIL, NATIONAL INTELLIGENCE ESTIMATE: PROSPECTS FOR IRAQ'S STABILITY: A CHALLENING ROAD AHEAD (2007), *available at* http://www.dni.gov/press_releases/20070202_release.pdf; NAT'L INTELLIGENCE

This statement is not attached to all classified documents, but it offers an instructive commentary on language and analysis, explaining:

> We use phrases such as *we judge*, *we assess*, and *we estimate*—and probabilistic terms such as *probably* and *likely*—to convey analytical assessments and judgments. Such statements are not facts, proof, or knowledge. These assessments and judgments generally are based on collected information, which often is incomplete or fragmentary. Some assessments are built on previous judgments. In all cases, assessments and judgments are not intended to imply that we have "proof" that shows something to be a fact or that definitively links two items or issues.[153]

The "explanation of estimative language" goes on to describe the scope of probabilistic vocabulary, offering a spectrum ranging from "remote" to "almost certainly" and accompanying descriptive terms, as well as the definitions of confidence levels, including "high," "moderate," and "low."[154] The terms flanking "even chance" on the spectrum are "unlikely" and "probably/likely," and these words, designating slightly more or less than "even chance," are ubiquitous in analysis.[155] The terms "*might*" and "*may*" are examples of even more ambiguous judgments, reflecting "situations in which we are unable to assess the likelihood, generally because relevant information is unavailable, sketchy, or fragmented," and these descriptors are also deployed regularly.[156] Analysts might use these qualifiers to protect themselves against reproach if they are wrong, or they might use them because the source material is ambiguous, or because the conclusions result from combining relatively reliable judgments that become less certain when they are stacked upon each other. Whatever the reason for these "weasel words,"

COUNCIL, NATIONAL INTELLIGENCE ESTIMATE: THE TERRORIST THREAT TO THE US HOMELAND (2007), *available at* http://www.dni.gov/press_releases/20070717_release.pdf.

[153] NAT'L INTELLIGENCE COUNCIL, NATIONAL INTELLIGENCE ESTIMATE: IRAN: NUCLEAR INTENTIONS AND CAPABILITIES (2007), *available at* http://www.dni.gov/press_releases/20071203_release.pdf.

[154] *Id.*

[155] *Id.*

[156] *Id.*

readers can only get a sense of reliability and credibility by looking thoroughly and deeply at the bases for analytical conclusions.

Notably, when intelligence is prepared specifically for legal use, the qualifications normally inherent to intelligence conclusions are sometimes expunged or omitted, giving an inappropriate impression of certainty. In the 2002 Declaration of Michael Mobbs regarding intelligence information about Jose Padilla,[157] approximately three pages of analytical conclusions—not including a caveat-laden footnote about two confidential sources—the words "likely/unlikely," "may," "could," "might," and "probably" are used a combined *zero* times.[158] Similarly, the 2002 Declaration of Mobbs regarding Yaser Hamdi[159] contains zero uses of any of those words.[160] The declarations available to the public are unclassified versions, but that may make the lack of any reservation even more striking.

In multiple rulings on Padilla's case in federal court, then-District Judge Michael Mukasey, who can hardly be accused of having a political bias against the Bush administration, was extraordinarily critical of the evidence presented. In an initial opinion, in the context of examining the Government's claim that Padilla should be prevented from communicating with counsel, Mukasey's disapproval was concealed only slightly by mellifluous phrasing: "the government's conjecture is," he wrote, "on the facts presented to me in [the Mobbs Declarations], gossamer speculation."[161] Similarly, in a subsequent, related ruling, Mukasey noted the speculative nature of the predictions of Vice

---

[157] Padilla is a detainee originally categorized as an enemy combatant who was ultimately convicted of terrorism-related crimes in federal court in 2007.

[158] Respondents' Response to, and Motion to Dismiss, the Petition for a Writ of Habeas Corpus, Unclassified Declaration of Michael H. Mobbs, Special Advisor to the Under Secretary of Defense for Policy, Padilla *ex rel.* Newman v. Bush, 233 F. Supp. 2d 564 (S.D.N.Y. 2002), *opinion adhered to on reconsideration sub nom.* Padilla *ex rel.* Newman v. Rumsfeld, 243 F. Supp. 2d 42 (S.D.N.Y. 2003), *available at* http://www.cnss.org/Mobbs%20Declaration.pdf.

[159] Yaser Hamdi is a United States citizen who was detained as an enemy combatant after being captured in Afghanistan in 2001 and released to Saudi Arabia in 2004 on the condition that he relinquish his United States citizenship.

[160] Respondents' Response to, and Motion to Dismiss, the Petition for a Writ of Habeas Corpus, Unclassified Declaration of Michael H. Mobbs, Special Advisor to the Under Secretary of Defense for Policy, Hamdi v. Rumsfeld, 243 F. Supp. 2d 527 (E.D. Va. 2002), *rev'd*, 316 F.3d 450 (4th Cir. 2003), *vacated*, 542 U.S. 507 (2004), *available at* http://www.cbsnews.com/htdocs/pdf/hamdimobbs2.pdf.

[161] *Padilla*, 233 F. Supp. 2d at 604.

Admiral Lowell Jacoby, then the Director of the Defense Intelligence Agency, regarding the potential impact of any interruption in Padilla's interrogations: "the forecast speculates not about an intelligence-related matter, in which Admiral Jacoby is expert, but about a matter of human nature—Padilla's in particular—in which, most respectfully, there are no true experts."[162]

Courts must be vigilant and circumspect when they read intelligence products. There is a unique language to this kind of analysis, one that is neither intuitively obvious nor immediately transparent. An assessment with an overabundance of qualifiers and "weasel words" should be examined closely, with particular attention to the source material; furthermore, intelligence judgments with no indication of the analysts' confidence in assessments—no "estimates of likelihood" at all—should be viewed with considerable skepticism. The only thing more worrisome than an intelligence judgment suffused with qualifiers is one with none at all.

III. HOW COURTS SHOULD ASSESS PROTECTED INFORMATION

Courts' attitudes toward and treatment of protected information is a critical part of modern jurisprudence, including in vital questions of constitutional law, the separation of powers, and major criminal and civil proceedings. The vagaries and challenges of intelligence analysis are myriad, and courts must have an understanding and a model for dealing with them if they are to successfully navigate the potential minefield of protected information. The following examination aims to furnish the beginnings of a framework for its judicial management.

A Three Straightforward Steps for Courts

1. Review the Information in Question

The most important step, and the easiest in terms of both procedure and judicial expertise, is simply for courts to look at the material the government claims is or should be protected. Whether under existing CIPA and SSP structures, according to new legislation, or by way of implemented academic proposals,

---

[162] *Padilla*, 243 F. Supp. 2d at 52.

courts should—and mostly already can—look at the materials in question to evaluate government claims that the information should not be admitted and/or shared with certain parties.

In criminal law, CIPA generally provides for this kind of judicial appraisal.[163] As discussed in Part I, CIPA requires the court to conduct a pretrial proceeding to assess the admissibility of classified information.[164] That proceeding may occur *in camera* if the Attorney General certifies that a public hearing would result in disclosure of the information, and the Government may make an *ex parte* written submission to the court explaining the national security sensitivity of the materials in question.[165] Additionally, the Government may move to submit a substitute; whether an unclassified summary or an admission of the relevant facts the protected information would prove, either option requires court approval.[166] There are a number of safeguards included to protect against public revelation of the information, and several options are available for the government to avoid exposing state secrets.

The critical element of CIPA review for the purposes of this analysis, however, is that nothing in the statute prevents courts from viewing and assessing the claimed protected materials; indeed, the language of CIPA strongly suggests that courts should and will do so. The provisions for *in camera* and *ex parte* proceedings, as well as the requirement that courts conduct a proceeding to determine the admissibility of the information, suggest an active role for courts in evaluating intelligence. In particular, courts are tasked with the responsibility of determining whether a government statement admitting the relevant facts proven by the disputed information or a summary of the material is sufficient for use in prosecution; it is hard to imagine how courts could do this without seeing—or at least thoroughly understanding—the underlying information along with the admission or summary. Additionally, CIPA authorizes the Government to make an *ex parte* written submission to the

[163] 18 U.S.C. app. 3 § 6(a)–(c) (2006).
[164] *Id.* §§ 2, 5–6.
[165] *Id.* § 6(c).
[166] *Id.*

court explaining why the information at issue is of sensitive national security value, further involving courts in the assessment and evaluation of intelligence.[167]

In other areas of the law, there is neither a mandate for nor a prohibition against courts examining claimed protected material. Still, when confronted with the SSP, courts are overwhelmingly deferential to government claims of secrecy and privilege.[168] The *Reynolds* decision is ambiguous on the issue of judicial engagement with protected materials, warning that "[j]udicial control over the evidence in a case cannot be abdicated to the caprice of executive officers," while in the very next sentence adding a caveat: "Yet we will not go so far as to say that the court may automatically require a complete disclosure to the judge before the claim of privilege will be accepted in any case."[169] Still, in more than fifty years of jurisprudence since *Reynolds*, no court has been challenged for requiring judicial examination of the information in question, and there is no other significant Supreme Court guidance about what type of information, if any, courts are prevented from viewing in civil proceedings.[170]

This lack of challenge against courts for viewing protected materials is likely a result, however, of judges declining to examine the information at all; courts review the documents involved in state secret claims in fewer than one-third of the instances of privilege invocation.[171] There is simply no good reason why judges should abdicate their responsibility to evaluate SSP claims. The *Reynolds* court reasoned that judicial review of such information, even *in camera* and *ex parte*, was unnecessary and potentially dangerous when "from all the circumstances of the case, [the court is satisfied] that there is a reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged."[172] In that instance, the court apparently was satisfied by the totality of the circumstances, because it failed to examine the information; had it done so, perhaps it would have seen the dubious claim of privilege for what it was.[173]

---

[167] *Id.* § 6(c)(2).

[168] *See, e.g.*, Kasza v. Browner, 133 F.3d 1159, 1166 (9th Cir. 1998).

[169] United States v. Reynolds, 345 U.S. 1, 9–10 (1953).

[170] *See* Liptak, *supra* note 24; *supra* note 24 and accompanying text.

[171] Weaver & Pallitto, *supra* note 31.

[172] *Reynolds*, 345 U.S. at 10.

[173] *See infra* Part III.B.4.

It is hard to conceive how a judge—with appropriate clearances and in a secure area—creates a security risk merely by viewing classified information;[174] conversely, it is easy to imagine the potential for abuse when the government knows the materials it seeks to protect likely will be seen by no one as long as the privilege is asserted. This is also true, and perhaps even more important, in nontraditional legal settings, such as the processes for detainees alleged to be enemy combatants. Because the intelligence analysis used as evidence against these detainees has repeatedly proven deficient when examined, as discussed below in Part III, it deserves careful review rather than apathy or deference. Viewing the underlying information is a crucial initial step to combat inefficiencies, lopsided incentives, and abuse in the area of protected materials—and doing so is a step already permitted by existing statutes and case law.

2. Apply Appropriate Skepticism

When courts examine protected information, they should assess its reliability and credibility as they would any other evidence, rather than granting additional credence or deference based on its secret provenance. Not all intelligence is created equal; there are ways to differentiate good analysis from bad and to independently assess specific elements of protected materials.

The kind of language used in assessments will often help telegraph the level of confidence in conclusions or predictions. As discussed above, an excess of "weasel words" and qualifiers, rather than clear, declarative statements, is evidence of analytical uncertainty. The more conditional the language, the more likely that the sources and/or conclusions are uncertain. Policymakers and courts have different standards of proof for taking action, and the intelligence process is geared decidedly toward informing the former more so than the latter. This makes sense, of course, but it means that protected materials should be evaluated differently than other kinds of evidence. For example, if an intelligence estimate indicates a seventy-five percent

[174] There are more than 850,000 Americans with Top Secret security clearances. Dana Priest & William M. Arkin, *A Hidden World, Growing Beyond Control*, WASH. POST, July 19, 2010, at A1. It seems doubtful that there is an insufficient number of Senate-confirmed, Article III judges with credentials and trustworthiness to join this club of nearly one million people in order to view protected materials when necessary.

likelihood that something is true, it is also saying that there is a twenty-five percent chance that it is *not* true. A good assessment will provide substantial evidence and reasoning for both possibilities, allowing policymakers to decide how to use that information in conjunction with the probability of the conclusion being correct.

Unlike in many legal and courtroom scenarios, which tend to have binary outcomes, the consequences resulting from intelligence analysis are multivariable, making probabilities useful in a qualitatively different way. For example, if the intelligence community views it as a forty percent chance that Terrorist Group X will acquire a nuclear weapon within a month absent any intervention, policymakers may decide that the use of force is the appropriate response given the potential dangers, even though it is more likely than not that the group will not obtain the weapon. Conversely, if some problematic but less threatening possibility is pegged at an eighty percent likelihood, it may not be useful to act even with much higher odds of occurrence, depending on a host of factors.

Probabilities are evaluated differently in court because the outcomes are usually binary and zero-sum. Intelligence analysts are not generally required to think in terms of "beyond a reasonable doubt," much less whether the evidentiary chain of custody is reliable, what the burden of proof is, etcetera. Additionally, regular consumers of intelligence recognize that the "conclusion" of any particular product is really an estimate whose likelihood is indicated—often in subtle or jargon-filled ways—in the context of the broader analysis. Those conclusions are often not unanimously agreed upon, and courts should also take note of dissenting opinions in assessments. In inter-agency reports, disagreements about the ultimate conclusion by specific participants in the analysis—whether individual or agency-level—are sometimes included as a footnote or in-text entry. These differing views can help highlight fault lines, weaknesses, or omissions in the overall assessments.

As noted above, when intelligence is produced specifically for legal purposes, caveats, disclaimers, and dissenting views can sometimes disappear.[175] Intelligence analysis is hardly ever certain, and aside from obvious examples such as photographs or

[175] *See, e.g.*, *supra* notes 148–149 and accompanying text.

voice intercepts, it is usually not based upon the kind of scientific evidence courts are used to, such as fingerprints or DNA. Accordingly, assessments should be forthright about information sources as well as caveats. When analyses such as the Mobbs Declarations addressing Hamdi and Padilla evince virtually no qualifiers whatsoever,[176] courts should wonder how and why the conclusions are concurrently nonspecific and unequivocal.

More broadly, assessments that address sensitive or controversial topics may lose some objectivity as a result of individual or institutional pressures and incentives. The command-and-control structure of a Congolese insurgent faction is not likely to be controversial; whether a Guantanamo Bay detainee was a member of the Taliban or just an innocent Afghan farmer who was in the wrong place at the wrong time, conversely, is a question that engenders intense political and legal passions.[177] Individual or structural pressures, or even mere attention, can result in factors other than just the available facts influencing assessments. The context of bureaucratic and government incentives should always be considered.

Finally, prospective analysis is often more speculative and less informed than retrospective assessments. Predictive intelligence—such as estimations of likely recidivism when examining the detention of accused enemy combatants—is naturally conjectural.[178] By contrast, demonstration of acts or associations already undertaken is, or at least can be, founded upon concrete evidence. With all intelligence, and especially with prospective analysis, assessments should include explanations of the level of confidence of conclusions as well as of the component estimative parts that led to the judgments. Where such explanations of confidence level are lacking, courts should proceed with caution; conversely, intelligence that is straightforward, well-sourced, and candid about strengths and weaknesses should be afforded greater credence.

---

[176] *See supra* notes 158, 160 and accompanying text.
[177] *See supra* notes 145–148 and accompanying text.
[178] *See supra* note 157–164 and accompanying text.

3. Examine Source Material

Courts cannot assess the validity of protected information without having a sense of its origins. As noted above, source material is a critical indicator of validity, and courts should not hesitate to review it when it is available. The government may want to avoid revealing certain "sources" and "methods" information, but to the extent that the inferences and conclusions from those sources are being provided, the foundational intelligence should be made available. Even if unclassified or lesser-classified summaries are provided, details about informational origin are an essential element of determining reliability and authenticity.

A common problem with intelligence is "circular reporting" or "circular sourcing," where information appears to come from multiple independent sources but in fact derives from a single source.[179] This kind of false confirmation can result from careless analysis or, in some circumstances, may be intentionally caused by the original source of the information. If the meaning or derivation of source material is unclear, courts should require further explanation or clarification, and when appraising sources, courts should not mistake ambiguity or impenetrability for sophistication. Legitimacy and veracity of some sources will be intuitively obvious; pictures or recordings, for example, while not inevitably representative of what they purport to demonstrate, are more likely reliable than, say, a description from an unnamed individual who may have any number of motivations to lie or mislead. Other sources will be harder to evaluate, to be sure, but courts can only make appropriate judgments if they venture beyond the conclusions into the underlying analysis and source material. How courts can and do achieve this, and under what circumstances they have tried—and succeeded and failed—is discussed more thoroughly in Part IV.

---

[179] *See, e.g.*, Bob Drogin & Tom Hamburger, *The Nation; Niger Uranium Rumors Wouldn't Die*, L.A. TIMES, Feb. 17, 2006, at A1 (addressing the persistent intelligence reporting—ultimately proved false—that Saddam Hussein sought uranium from Niger). According to a United States intelligence official, "This became a classic case of circular reporting . . . . It seemed like we were hearing it from lots of places. People didn't realize it was the same bad information coming in different doors." *Id.* (internal quotation marks omitted).

If information about underlying intelligence is unavailable or not provided, courts should recognize that may be because the analysis is unreliable, misleading, or not thoroughly sourced. Protected information lacking context or explanation should be treated the same way any other similarly-presented evidence would be: skeptically. Rather than being instinctively credulous or impressed when faced with a document stamped CLASSIFIED, courts must be mindful of the importance of examining sources, considering incentives, and paying close attention to language cues. Courts should also have the confidence—as they already have the authority—to ask for more information or explanation regarding protected information when it is unclear or incomplete. Similarly, government claims that secret material is unreviewable ought to be accompanied by thorough and persuasive explanations, or else rejected. Underlying sources and analyses should be examined, and when assessments and conclusions are unsourced or thinly-sourced, they should not be considered reliable without excellent justification for such deficiencies.

B. Selected Instances of Court Engagement with Protected Materials

Courts have confronted and managed protected materials in a wide variety of circumstances and contexts. Many judges decline to even view the underlying information at issue, especially in SSP cases, while others, particularly in criminal cases where CIPA applies, deal with intelligence as a matter of course. In recent years, non-traditional proceedings, specifically those dealing with detainee rights and other "War on Terror" issues, have created new and unusual contexts for the use of this kind of information. Few courts, however, address in depth how they view or analyze protected material. It is therefore useful to briefly examine instances in which courts discuss their engagement with classified evidence, whether effectively or ineffectively, and to examine types of approaches.

1. *Parhat v. Gates*

Perhaps the best example of a court engaging with intelligence materials thoughtfully and comprehensively is *Parhat v. Gates*.[180] Judge Merrick Garland's opinion for the D.C. Circuit of the United States Court of Appeals evinces precisely the kind of careful analysis—and healthy skepticism—advocated by this Article, and if the decision reads as critical of the government, it is only because, in this particular instance, the government used profoundly inadequate intelligence to advance a deficient legal argument. The court in *Parhat* approached the protected information in just the right way, insisting upon evaluating not just the conclusions of the multiple intelligence documents submitted, but also the underlying sources and methods, for reliability and breadth. The court obviously took seriously the responsibility to *evaluate* government claims, rather than accepting them at face value.

The court noted at the beginning of its opinion—in explaining that it was reviewing the decision of a Guantanamo Bay detainee's Combatant Status Review Tribunal ("CSRT")—that a Tribunal's ruling "must be based on evidence that both the Tribunal and the court can assess for reliability."[181] The Circuit Court took seriously this directive, analyzing the intelligence with a level of detail and care that few courts attempt. Even with the relaxed CSRT standards—including a rebuttable presumption that government evidence is genuine and accurate, allowance of hearsay evidence, etcetera—the court found the proof insufficient for continued detention, focusing especially on the deficiencies of intelligence materials that ostensibly supported the CSRT finding that Parhat was an enemy combatant.[182]

That evidence, the court noted, came "from four U.S. government intelligence documents, one from the Department of State and three from components of the Department of Defense."[183] These reports were heavily classified, so their contents, as well as the elements of the court's decision specifically discussing them, are unavailable to the public. The opinion, however, addresses the evidence more generally, and

---

[180] 532 F.3d 834 (D.C. Cir. 2008).
[181] *Id.* at 836.
[182] *Id.* at 846–50.
[183] *Id.* at 844.

it discusses a number of factors discussed in this Article. Regarding ambiguous and hedged language, Judge Garland wrote: "The documents repeatedly describe [the] activities and relationships as having 'reportedly' occurred, as being 'said to' or 'reported to' have happened, and as things that 'may' be true or are 'suspected of' having taken place."[184]

As discussed previously, even equivocal language and conclusions can be extremely useful, depending on context and underlying support. Something can be "said to" have occurred by a single, unreliable source, or by several individuals with a proven track record of reliability and veracity. Due to the constraints of custom and language, there may not be a way to immediately identify the difference between those two possibilities, or the virtually endless range of possibilities between and beyond them, without looking at the underlying bases for the judgments. Which is precisely what the *Parhat* court did, finding that "in virtually every instance, the documents do not say who 'reported' or 'said' or 'suspected' those things. Nor do they provide any of the underlying reporting upon which the documents' bottom-line assertions are founded, nor any assessment of the reliability of that reporting."[185]

The approach regarding protected information taken by the court in *Parhat*—and more generally advocated by this Article—differs little from that used with any other kind of evidence. In his discussion of the preponderance standard, Judge Garland cited the Supreme Court opinion in *Concrete Pipe & Products of California, Inc., v. Construction Laborers Pension Trust for Southern California*, which explained: "Before any such burden can be satisfied . . . the factfinder must evaluate the raw evidence, finding it to be sufficiently reliable and sufficiently probative to demonstrate the truth of the asserted proposition with the requisite degree of certainty."[186] In *Parhat*, not only was there precious little concrete evidence to support sweeping

---

[184] *Id.* at 846.

[185] *Id.* at 846–47.

[186] *Id.* at 847 (quoting Concrete Pipe & Prods., Inc. v. Constr. Laborers Pension Trust, 508 U.S. 602, 622 (1993)).

accusations against the defendant, but the court was profoundly unimpressed with the government's claims that the intelligence was reliable:

> First, the government suggests that several of the assertions in the intelligence documents are reliable because they are made in at least three different documents. We are not persuaded. Lewis Carroll notwithstanding, the fact that the government has "said it thrice" does not make an allegation true. In fact, we have no basis for concluding that there are independent sources for the documents' thrice-made assertions. To the contrary, . . . many of those assertions are made in identical language, suggesting that later documents may merely be citing earlier ones, and hence that all may ultimately derive from a single source. . . .
>
> Second, the government insists that the statements made in the documents are reliable because the State and Defense Departments would not have put them in intelligence documents were that not the case. This comes perilously close to suggesting that whatever the government says must be treated as true . . . .
>
> . . . .
>
> We . . . reject the government's contention that it can prevail by submitting documents that read as if they were indictments or civil complaints, and that simply assert as facts the elements required to prove [the allegations].[187]

The court went on to note that it was not "suggest[ing] that the government must always submit the underlying basis for its factual assertions in order to make such an assessment [of reliability] possible."[188] There are myriad ways the government might demonstrate the veracity of intelligence materials—or that analytical judgments can self-authenticate through explanations of sourcing and analysis. The court made no specific demands regarding demonstration of reliability, but rather "merely reject[ed] the government's contention that it can prevail by submitting documents that read as if they were indictments or civil complaints, and that simply assert as facts the elements required [for proof]."[189]

---

[187] *Id.* at 848–50.
[188] *Id.* at 849.
[189] *Id.* at 850.

The court in *Parhat* applied appropriate skepticism in its evaluation of classified intelligence that was superficially assertive but, upon closer examination, suffused with caveats. When the court attempted to determine the reliability of the statements by reviewing the underlying information, it found that much of the raw intelligence was unavailable and/or suggestive of circular reporting.[190] While this may seem like a logical or unremarkable approach, many judges confronted with disputed protected material decline even to review it, and it is still more unusual for courts to explore the basis for intelligence conclusions rather than accepting them at face value. The end result of this kind of process is by no means biased toward rejecting government evidence; indeed, were the conclusions of the classified materials in *Parhat* better supported by underlying sources, there is every reason to believe the government would have won a resounding victory. In the next case illustration, for example, a judge analyzing evidence against multiple defendants found that the information supported the accusations against one but not the others. But judges and courts can only determine reliability if they have all the information available, and if they can appropriately decipher those materials in their analysis. In *Parhat*, the court was unusually rigorous on both counts.

2. *Boumediene v. Bush*

Another example of a court frankly discussing the issues associated with classified evidence comes from a surprising source: Judge Richard Leon, of the United States District Court for the District of Columbia. Judge Leon was appointed by President George W. Bush, was Deputy Chief counsel for Republicans on the Iran-Contra Committee in 1987, and worked in the Department of Justice under Presidents Reagan and George H.W. Bush.[191] Additionally, in Judge Leon's initial rulings regarding indefinite detention of terrorist suspects, he granted the government's motion to dismiss detainees' petitions for writs of habeas corpus—a decision made without viewing any

[190] *Id.*

[191] *See* District Judge Richard J. Leon, UNITED STATES DISTRICT COURT, http://www.dcd.uscourts.gov/dcd/leon (last visited Mar. 28, 2012).

underlying substantive evidence.[192] He is, in short, an unlikely person to convey a decisive indictment of protected material offered by the government against accused terrorists.

And yet that is precisely what Judge Leon delivered in his opinion in *Boumediene v. Bush*, a case involving the habeas corpus petition of Lakhdar Boumediene and five other Guantanamo Bay detainees accused of being terrorist supporters of al Qaeda.[193] On remand from the Supreme Court, which had found that these detainees had the right to appeal their detention status, Judge Leon presided over the required habeas hearing.[194] Pursuant to that inquiry, the Government submitted "approximately 650 pages of exhibits and a 53-page narrative, setting forth the Government's alleged legal and factual basis for holding the six petitioners as 'enemy combatants,' " and the court heard several days of testimony and argument.[195] The government needed only to prove the lawfulness of detention by a preponderance of the evidence.[196]

Despite this apparently voluminous evidence against the detainees, Judge Leon found that the defendants' alleged plan to travel to Afghanistan to fight American and allied forces was based "exclusively on the information contained in a classified document from an unnamed source. This source is the only evidence in the record directly supporting each detainee's alleged knowledge of, or commitment to, this supposed plan."[197] The opinion expressed skepticism about this source, saying that the government had "not provided the Court with enough information to adequately evaluate the credibility and reliability of this source's information" and that "the Court was not provided with adequate corroborating evidence that these petitioners knew of and were committed to such a plan."[198] Judge Leon acknowledged that because the evidence was classified, he could not be more specific about its deficiencies, but he noted that the exclusive basis upon which the detainees had been held for

---

[192] *See* Khalid v. Bush, 355 F. Supp. 2d 311, 314 (D.D.C. 2005), *vacated*, Boumediene v. Bush, 476 F.3d 981 (D.C. Cir. 2007), *rev'd*, 553 U.S. 723 (2008).

[193] Boumediene v. Bush, 579 F. Supp. 2d 191, 193–94 (D.D.C. 2008), *rev'd*, Bensayah v. Obama, 610 F.3d 718 (D.C. Cir. 2010).

[194] *Id.* at 191–92.

[195] *Id.* at 193, 195.

[196] *Id.* at 196.

[197] *Id.* at 197.

[198] *Id.*

seven years "rest[ed] on so *thin* a reed" as to be insufficient for even a preponderance standard.[199]

Additionally, Judge Leon came to a different conclusion when analyzing the evidence surrounding one of the six petitioners involved in the case. The government had provided additional evidence regarding Belkacem Bensayah, including "a series of other intelligence reports based on a variety of sources and evidence."[200] Given this apparently substantial and reliable evidence against Bensayah, beyond the insufficient proof offered against the other detainees, he found that Bensayah was appropriately categorized as an enemy combatant.[201] Rigorous examination of protected materials will of course lead to particularized and specific differentiation.

This kind of thorough, considered analysis of a vast amount of classified evidence was crucial to a fair and reasoned determination in *Boumediene*. Judge Leon examined the information available, and he noted that it was impossible to properly evaluate critical intelligence claims for credibility or corroboration because the government could not—or would not—provide information enabling him to do so. Had Judge Leon not rigorously examined the materials provided, or been overwhelmed or persuaded by the sheer volume of the government's presentation of secret information, he might have accepted even the "thin reed"[202] as adequate and perpetuated unreasonable and unlawful incarcerations; conversely, had he been dismissive of all the intelligence, or doubtful of all evidentiary submissions due to government overreach in some aspects of the case, he might have ordered the release of an individual for whom there was sufficient evidence to continue detention. Instead, Judge Leon seems to have taken the kind of methodical and comprehensive approach required for just results.

---

[199] *Id.*
[200] *Id.* at 198.
[201] *Id.*
[202] *Id.* at 197.

3. *Mohammed v. Jeppesen* and *Al-Haramain Islamic Foundation, Inc. v. Bush*

Unlike the issues presented in the flurry of "nontraditional," post-9/11 cases, most of which involved questions of constitutional and international law apart from traditional civil or criminal proceedings, matters involving the SSP have confronted courts for more than fifty years. As discussed in Part I above, the SSP has expanded in recent years, both in frequency of use and breadth of applicability. While the privilege was once used rarely and only as a challenge to specific pieces of evidence, generally during discovery, recent government invocation of the SSP has prevented lawsuits from even reaching the discovery phase.[203] The privilege has become a means to have entire cases dismissed, sometimes even without a thorough examination of whether plaintiffs have enough evidence to move forward without—or with an unclassified summary of—the disputed protected information.[204]

The *Jeppesen* and *Al-Haramain* cases[205] are addressed jointly here because they contain similar issues and, together, represent how careful, conscientious, and healthily skeptical treatment of government state secret claims can result in different results despite similar—and similarly appropriate—judicial management.[206] They also demonstrate the typical perspectives and rulings on these issues, evidenced by district court decisions, followed by unusual, conscientious, and laudable treatments on appeal.

In *Jeppesen*, five individuals alleged that they were victims of "extraordinary rendition," a practice of apprehension and detention of foreign nationals suspected of involvement in terrorist activities.[207] Under this program, suspects were allegedly arrested and secretly transported to prisons operated abroad by the CIA or by foreign countries, some of which were

---

[203] *See supra* notes 25, 37–38 and accompanying text.

[204] *See supra* note 38 and accompanying text.

[205] Mohamed v. Jeppesen Dataplan, Inc., 579 F.3d 943 (9th Cir. 2009), *rev'd en banc*, 614 F.3d 1070 (9th Cir. 2010), *cert. denied*, 131 S. Ct. 2442 (2011); Al-Haramain Islamic Found., Inc. v. Bush, 507 F.3d 1190 (9th Cir. 2007).

[206] Note: This analysis is of the April 2009 opinion (unanimous panel decision), not the 6-5 en banc reversal of September 2010, which affirmed the district court ruling.

[207] *Jeppesen*, 579 F.3d at 949–51.

known to torture detainees.[208] These individuals allegedly included Binyam Mohamed, who filed suit against Jeppesen Dataplan, Inc., a subsidiary of Boeing Company, alleging that Jeppesen knowingly assisted these renditions by providing logistical support to flights used by the CIA.[209] The United States invoked the state secrets privilege, claiming that litigation would undermine national security even though many of the details alleged—and claimed by the government to be classified—had already been made public by the media.[210] This SSP claim was initially invoked by the Bush Administration, but was also continued, to the surprise of many observers—including the presiding judges—by the Obama administration.[211]

In *Al-Haramain*, the Al-Haramain Islamic Foundation, which says that it is a charity but is alleged by the United States to have links to terrorist organizations, claimed that the federal government spied on the group and its officials using illegal electronic surveillance.[212] In a legal proceeding separate from the surveillance lawsuit, a classified document indicating that the group was indeed the subject of electronic surveillance was mistakenly disclosed to Al-Haramain's attorneys; the government subsequently reclaimed the document and declared its contents an inadmissible state secret.[213]

In both cases, the district courts granted the government's motions to apply the SSP.[214] In *Al-Haramain*, that ruling was limited; Judge King agreed to apply the privilege to the classified document in question, but refused to dismiss the case in its

---

[208] *Id.*

[209] *Id.* at 949, 951.

[210] *Id.* at 951.

[211] *See* Schwartz, *supra* note 99 ("The Bush administration argued that the [*Jeppesen*] case should be dismissed because even discussing it in court could threaten national security and relations with other nations. During the campaign, Mr. Obama harshly criticized the Bush administration's treatment of detainees, . . . [b]ut a government lawyer, Douglas N. Letter, made the same state-secrets argument on Monday, startling several judges on the United States Court of Appeals for the Ninth Circuit. 'Is there anything material that has happened' that might have caused the Justice Department to shift its views, asked Judge Mary M. Schroeder, . . . coyly referring to the recent election. 'No, your honor,' Mr. Letter replied. Judge Schroeder asked, 'The change in administration has no bearing?' Once more, he said, 'No, Your Honor.' ").

[212] Al-Haramain Islamic Found., Inc. v. Bush, 507 F.3d 1190, 1194–95 (9th Cir. 2007).

[213] *Id.*

[214] *Jeppesen*, 579 F.3d at 951; *Al-Haramain*, 507 F.3d at 1195–96.

entirety, advancing the novel proposal that plaintiffs' attorneys file affidavits describing their memories of the document to prove that the Foundation was surveilled.[215] The circuit court, while sympathetic to the "commendable effort to thread the needle[,]"[216] disallowed that approach, ruling that it "countenance[d] a back door around the privilege," which "[o]nce properly invoked and judicially blessed, . . . is not a half-way proposition."[217] It otherwise agreed with the district court, finding that while the very subject matter of the litigation was not a state secret—the surveillance program having been widely reported in the media and then acknowledged by the Bush administration—the classified document in question was protected by SSP and therefore inadmissible.[218]

Crucially, the court explained its process and reasoning in coming to this conclusion regarding the document, which it reviewed *in camera*:

> We take very seriously our obligation to review the documents with a very careful, indeed a skeptical, eye, and not to accept at face value the government's claim or justification of privilege. Simply saying 'military secret,' 'national security' or 'terrorist threat' or invoking an ethereal fear that disclosure will threaten our nation is insufficient to support the privilege. Sufficient detail must be—and has been—provided for us to make a meaningful examination. . . .
>
> . . . .
>
> We have spent considerable time examining the government's declarations (both publicly filed and those filed under seal). We are satisfied that the basis for the privilege is exceptionally well documented.[219]

It is impossible to know, of course, precisely what proof the government offered to the court, and in particular whether there were deficiencies of the type that, for example, the court in

---

[215] Al-Haramain Islamic Found., Inc. v. Bush, 451 F. Supp. 2d 1215, 1229 (D. Or. 2006).

[216] *Al-Haramain*, 507 F.3d at 1204.

[217] *Id.* at 1193.

[218] *Id.* at 1204–05 ("The Sealed Document, its contents, and any individuals' memories of its contents, even well-reasoned speculation as to its contents, are completely barred from further disclosure in this litigation by the common law state secrets privilege.").

[219] *Id.* at 1203.

Parhat recognized.[220] But as a matter of process, courts should take a careful, skeptical and thorough approach when evaluating classified material, and should include some explanation and acknowledgment of these elements in their opinions.[221]

The district court in *Jeppesen* upheld an even more sweeping SSP claim, ruling that "the issues involved . . . are non-justiciable because the very subject matter of the case is a state secret."[222] The opinion provided only a brief explanation for finding that the plaintiffs were barred from having their day in court against government contractors that allegedly assisted in their torture: "The Court's review of [CIA Director] General Hayden's public and classified declarations confirm that proceeding with this case would jeopardize national security and foreign relations and that no protective procedure can salvage this case."[223]

On appeal, the Ninth Circuit of the United States Court of Appeals declined to delve into the details of the substantive claims, instead finding that under state secrets precedent, the government could not prevent a lawsuit simply because it made allegations regarding a secretive program. The court stated:

> At base, the government argues here that state secrets form the subject matter of a lawsuit, and therefore require dismissal, any time a complaint contains allegations, the truth or falsity of which has been classified as secret by a government official. . . . This sweeping characterization of the "very subject matter" bar has no logical limit . . . . According to the government's theory, the Judiciary should effectively cordon off all secret government actions from judicial scrutiny, immunizing the CIA and its partners from the demands and limits of the law. We reject this interpretation . . . .[224]

---

[220] Parhat v. Gates, 532 F.3d 834, 842 (D.C. Cir. 2008).

[221] Although the SSP claim was upheld in *Al-Haramain*, on remand a district court later ruled that the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1810—which allows damage lawsuits by targets of illegal government surveillance—displaces the state secrets privilege. *See* Al-Haramain Islamic Found., Inc. v. Obama (*In re* Nat'l Sec. Agency Telecomms. Records Litig.), 700 F. Supp. 2d 1182, 1184 (N.D. Cal. 2010). In 2010, after protracted battles between the court and the government regarding the classified document in dispute, the government was found to have broken the law in its monitoring of the Foundation. *Id.*

[222] Mohamed v. Jeppesen Dataplan, Inc., 539 F. Supp. 2d 1128, 1134–35 (N.D. Cal. 2008), *rev'd*, 563 F.3d 992 (9th Cir. 2009), *rev'd en banc*, 614 F.3d 1070 (9th Cir. 2010), *cert. denied*, .131 S. Ct. 2442 (2011).

[223] *Id.* at 1135.

[224] *Jeppesen*, 579 F.3d at 955.

Instead, the court noted, the state secrets privilege should, except in extraordinary circumstances,[225] be used regarding specific pieces of evidence "on an item-by-item basis, rather than foreclosing litigation altogether at the outset . . . ."[226] The court went on to refuse the government's request that the case be dismissed at its outset even if the subject matter was not found to be a state secret. Because the state secrets privilege, like any other privilege, " 'extends only to [evidence] and not to facts,' it cannot be invoked to prevent a litigant from persuading a jury of the truth or falsity of an allegation by reference to non-privileged evidence, regardless whether privileged evidence might also be probative of the truth or falsity of the allegation."[227]

Court rejections of SSP invocations are so extraordinarily rare that this ruling, while perhaps superficially unremarkable, is an atypical and important example for how courts should view far-reaching government claims of secrecy in the legal process. It was also, however, short-lived; seventeen months later, following the grant of an appeal for *en banc* rehearing, a closely divided panel voted 6-5 to overturn the panel decision, affirming the district court's dismissal of the entire claim.[228]

4. *United States. v. Reynolds* and *El-Masri v. United States*

The instances in which courts have granted the government's request to apply the SSP while declining to look at the substantive materials covered by invocations—or viewing the intelligence in a cursory and unquestioning fashion—are so numerous that it might seem superfluous to discuss specific examples. However, for the sake of comparison with the above-mentioned cases, and so readers do not mistake a handful of sagacious but anomalous decisions for predominance or a trend, it is useful to examine two cases as bookend examples of well-intentioned but inadequate approaches.

---

[225] *Id.* at 956 (such as if a lawsuit is predicated on the existence of a secret agreement between a plaintiff and the government).

[226] *Id.* at 955.

[227] *Id.* at 957–58 (alteration in original) (quoting Upjohn Co. v. United States, 449 U.S. 383, 395–96 (1981)).

[228] *See supra* notes 205–206 and accompanying text.

The foundational case for the SSP doctrine, as discussed briefly in Part I.A.2, is *United States. v. Reynolds*.[229] In *Reynolds*, the Supreme Court established the doctrine for the SSP, and in doing so it set an ignoble precedent for the treatment of classified intelligence. *Reynolds* is a kind of original sin with regard to protected material; not only is it a vague and equivocal opinion, it established—in what would be an ironic twist if it were not so predictable given the government's incentives to conceal mistakes and negligence—an exceedingly credulous example for dealing with claims of secrecy in a case where the underlying information actually had no apparent relation whatsoever to secrets implicating national security.

In 1948, three Air Force contractors were killed when a B-29 Superfortress crashed in Georgia.[230] Their widows filed suit against the government for negligence, and they requested the production of the government's accident reports.[231] The Air Force refused to produce the documents, claiming that to reveal them would threaten national security due to the electronics secrets involved.[232] The trial court rejected the claim of privilege, holding in favor of the plaintiffs and ordering the government to produce the documents so the court could determine whether they contained legitimately secret information.[233] The Third Circuit of the United States Court of Appeals affirmed, both regarding the question of document production and the disposition due to the government's refusal to produce the requested materials.[234]

The Supreme Court, as discussed above, determined that it did not need to review the documents to establish the legitimacy of the privilege claim, finding that in "a time of vigorous preparation for national defense" there was "a *reasonable danger* that the accident investigation report would contain references to the secret electronic equipment which was the primary concern of the mission."[235] Reinforcing this weak standard—even while

---

[229] *Supra* notes 19–20 and accompanying text.

[230] Brauner v. United States, 10 F.R.D. 468, 469 (E.D. Pa. 1950), *aff'd sub nom.*, Reynolds v. United States, 192 F.2d 987 (3d Cir. 1951), *rev'd sub nom.*, United States v. Reynolds, 345 U.S. 1 (1953).

[231] *Id.*

[232] *Id.* at 472.

[233] *Id.*

[234] *Reynolds*, 192 F.2d at 998.

[235] *Reynolds*, 345 U.S. at 10 (emphasis added).

granting that in many circumstances it would be not only allowable but important for courts to review the disputed information—the decision went on to state that "under circumstances indicating a reasonable possibility that military secrets were involved, there was certainly a sufficient showing of privilege to cut off further demand for the document . . . ."[236] These comments, providing largely dubious and unhelpful guidance even at the time, border on farcical given the reality of the documents' contents.

In February 2000, Judy Palya Loether, the daughter of Al Palya, one of the contractors killed in the B-29 crash, was searching online for information about the accident.[237] She had done so occasionally for years out of curiosity about a father she had never known, a man who died when she was just seven weeks old.[238] At the time, she did not even know there had been an accident report, had no knowledge about the *Reynolds* case, and had no idea that the government had refused to produce relevant documents nearly fifty years before.[239] On that day, she stumbled upon a website that advertised declassified military accident reports from 1918 to 1955. Curious about her father's work, with no thought to the cause of the crash, Ms. Loether bought a copy of the report.[240]

To her surprise, and disappointment, there was nothing that seemed secret or even interesting, no information about her father or his work. What the report did detail, however, was an extraordinary amount of negligence and mistakes that led to the fatal crash. Maintenance problems. Fire hazards. The wrong engine shutting down in the midst of an emergency. The report detailed exactly the kind of negligence alleged decades before and made no mention of secret electronic equipment. The foundational case of the SSP was, by all appearances, based on government dissembling to the Supreme Court. The descendents of the contractors later brought an action against the United States for misrepresenting the classified material. The Third Circuit of the United States Court of Appeals found that the

---

[236] *Id.* at 10–11.

[237] Barry Siegel, *The Secret of the B-29; A Daughter Discovers what Really Happened*, L.A. TIMES, Apr. 19, 2004, at A1.

[238] *Id.*

[239] *Id.*

[240] *Id.* The account in the following paragraph is likewise from Barry Siegel's article.

actions of the Air Force officials did not meet the stringent test of fraud upon the court;[241] Senator Specter of Pennsylvania called this decision "a little mystifying."[242]

Whether or not the Third Circuit of the United States Court of Appeals was correct in finding that "there is an obviously reasonable truthful interpretation of the statements made by the Air Force,"[243] a conclusion the court made based on a much broader reading of the statement than the Supreme Court appears to have made in the original case, it seems extraordinarily likely that the analysis would have been different had the Supreme Court looked at the documents at issue in 1953. It is also obvious that the government claim that the airplane involved had been carrying "confidential equipment" and that "any disclosure of its mission . . . operation or performance" would *for that reason* be against public interest[244] implied that the report itself involved information about the secret electronic equipment.

It is undoubtedly true that the legal system sometimes makes mistakes, particularly when not all the relevant information is accessible. After cases are decided, facts can reveal a wrong decision, and we accept this possibility as part of a judicial system that values and respects finality except in the most unusual or unjust scenarios. In instances like *Reynolds*, however, to get it right, judges merely have to look at information that is readily available. Courts should not allow themselves to be bullied or condescended to; they are permitted—and in some cases required—to consider protected information, and they are qualified to do so, whether based on experience and judgment or with the assistance of others.

More than fifty years after *Reynolds*, the Supreme Court similarly declined to view the intelligence upon which an SSP claim was based, despite an offer from the Solicitor General to show the justices, "under appropriate security measures," the classified declaration used in the lower courts to support the

---

[241] Herring v. United States, 424 F.3d 384, 392 (3d Cir. 2005).

[242] *Examining the State Secrets Privilege: Protecting National Security While Preserving Accountability: Hearing Before the S. Comm. on the Judiciary*, 110th Cong. 4 (2008) (statement of Sen. Arlen Specter).

[243] *Herring*, 424 F.3d at 392.

[244] Brief for the United States at 43, United States. v. Reynolds, 345 U.S. 1 (1953) (No. 21), 1952 WL 82378.

privilege claim.[245] In *El-Masri*,[246] the Court denied certiorari of the circuit court decision without comment and without reviewing the materials at issue.[247] In contrast to the Ninth Circuit's analysis in *Jeppesen*, the Eastern District of Virginia and the Fourth Circuit dismissed the *El-Masri* case before discovery[248]; each court held that a plaintiff who alleged systematic torture and abuse at the hands of the government could not sue the United States because the very subject of his suit was a state secret.[249] El-Masri claimed that he was subject to the widely-reported "extraordinary rendition" program, and although his story was well known, the district court held—and the Fourth Circuit affirmed—that allowing his lawsuit to proceed would threaten United States national security.[250]

It is impossible to know how comprehensive or persuasive the government's explanation was of why "damage to the national security could result if the defendants . . . were required to admit or deny El-Masri's allegations."[251] The district court explained that the *ex parte* classified declaration by the Director of Central Intelligence was "a detailed explanation of the facts and reasons underlying the assertion of the privilege."[252] This author wonders whether, as the *El-Masri* court wrote, "any admission or denial of these allegations by defendants in this case would reveal the means and methods employed pursuant to this clandestine program and such a revelation would present a grave risk of injury to national security[,]"[253] but the court insisted that its conclusion "finds firm support in the details disclosed in the DCI's classified *ex parte* declaration."[254] In addition to the broad understanding of what would threaten

---

[245] Linda Greenhouse, *Justices Turn Aside Case of Man Accusing C.I.A. of Torture*, N.Y. TIMES, Oct. 10, 2007, at A20.

[246] 552 U.S. 947 (2007).

[247] Greenhouse, *supra* note 245.

[248] *See* El-Masri v. United States, 479 F.3d 296, 311 (4th Cir. 2007); El-Masri v. Tenet, 437 F. Supp. 2d 530, 539 (E.D. Va. 2006).

[249] *See El-Masri v. United States*, 479 F.3d at 311; *El-Masri v. Tenet*, 437 F. Supp. 2d at 539.

[250] *See El-Masri v. United States*, 479 F.3d at 312; *El-Masri v. Tenet*, 437 F. Supp. 2d at 537.

[251] *El-Masri v. Tenet*, 437 F. Supp. 2d at 537.

[252] *Id.*

[253] *Id.*

[254] *Id.*

national security and the apparent lack of interest in the underlying source material, the use of SSP essentially as a motion to dismiss is deeply troubling.

The Ninth Circuit panel decision addressed this point in *Jeppesen*, stating that no case law indicated that the subject matter of a lawsuit can be a state secret, outside the limited context of secret contracts, as in *Totten v. United States*.[255] That court further explained: "The Supreme Court's 'very subject matter' language appeared in a footnote in *Reynolds*, where the Court simply characterized [the subject of *Totten* as a state secret]. That brief passage did not signal a deliberate expansion of *Totten's* uncompromising dismissal rule beyond secret agreements with the government . . . ."[256] By contrast, the Fourth Circuit in *El-Masri* concluded, without any apparent proof, that the plaintiff would need to access and use extensive amounts of protected material to advance his case.[257] This kind of speculative and conclusory judgment takes the place of precisely what the SSP process should do—apply specific rulings to specific pieces of evidence. Instead, the *El-Masri* court assumed that the evidence needed to establish a prima facie case could only come from protected materials, a conclusion made without examination of that information on an individualized basis.[258]

Engaging in still more conjecture, the *El-Masri* decision went on to claim, again without any apparent examination of the evidence ostensibly at issue, that even if El-Masri could establish a prima facie case without state secrets, "the defendants could not properly defend themselves without using privileged evidence."[259] Astonishingly, the court said that its hypothetical rendering of the course of the case, were it to go forward, "illustrate[s] that virtually any conceivable response to El-

---

[255] *See* Mohamed v. Jeppesen Dataplan, Inc., 579 F.3d 943, 954 (9th Cir. 2009) (discussing Totten v. United States, 92 U.S. 105 (1875), and how separate from a privilege or rule of evidence, the case establishes the non-justiciability of suits against the government based on covert espionage agreements even in the absence of a formal claim of privilege), *rev'd en banc*, 614 F.3d 1070 (9th Cir. 2010), *cert. denied*, 131 S. Ct. 2442 (2011).

[256] *Id.* (quoting United States v. Reynolds, 345 U.S. 1, 11 n.26 (1953)).

[257] El-Masri v. United States, 479 F.3d 296, 309 (4th Cir. 2007) ("Even marshalling the evidence necessary to make the requisite showings would implicate privileged state secrets . . . .").

[258] *See id.* at 311.

[259] *Id.* at 309.

Masri's allegations would disclose privileged information."[260] It is hard to imagine another context in which a court could get away with presuming all possible courses of litigation and then dismissing a case based on that speculation.

Additionally, there is no indication that the court examined evidence beyond the DCI Declaration. Indeed, the court employed a kind of circular argument regarding viewing underlying materials—it twice quoted a passage from *Reynolds* that " '[w]hen . . . the occasion for the privilege is appropriate, . . . the court should not jeopardize the security which the privilege is meant to protect by insisting upon an examination of the evidence, even by the judge alone, in chambers."[261] After information falls under the privilege, the court said, it is protected from disclosure, even including, the court argued, *in camera* examination.[262] It is hard to imagine how a court could determine, in most instances, whether the SSP applies to evidence without having some sense of what the information is, but courts from *Reynolds* to *El-Masri* have seemingly been untroubled by this paradox, granting the application of the privilege to unseen evidence based on governmental pronouncements.[263]

Although this kind of analysis may be deeply flawed, it is by no means uncommon. The Fourth Circuit of the United States Court of Appeals in *El-Masri* cites a number of decisions in which suits were dismissed at the pleadings stage based on SSP invocations,[264] and this is consistent with the broad deference and acquiescence practiced by courts in matters of national security. However, as this Article demonstrates, there are better ways to handle these kinds of cases and materials.

CONCLUSION

Protected information should be treated, to whatever extent possible under the law, like any other kind of evidence: evaluated for reliability, not presumed accurate on its face. This Article has discussed the current legal and conceptual frameworks

---

[260] *Id.* at 310.

[261] *Id.* at 306 (quoting United States v. Reynolds, 345 U.S. 1, 10 (1953) (second and third alterations in original)).

[262] *See id.*

[263] *See id.* at 310–11.

[264] *See id.*

regarding judicial treatment of this kind of information, outlined the structure and roles of the producers of classified materials, and raised questions about how courts should view and analyze material that may be privileged or protected. In answering those questions, this Article has discussed the analytical process, examined some of the various incentives and influences involved with classified information, and addressed how some courts have engaged with these issues. Without court engagement with—and skepticism of—information and materials that the government would prefer to keep secret, incentives and results alike will continue to perpetuate excessive judicial deference as well as unjust results. Like all other evidence, information allegedly having implications for national security involves a variety of personal and institutional biases, incentives, and errors. When there are no checks on—or even consideration of—such factors, these possibilities and problems are exacerbated.

In order to effectively engage with these kinds of materials, courts, as well as many attorneys, must have an understanding of what they are looking at when they consider protected information. Accordingly, this Article has attempted to provide a brief overview of the process of intelligence analysis, production, and dissemination. The language and form of classified material is neither intuitive nor widely understood in the legal community, and this Article provides an initial blueprint for comprehending and engaging it. As briefly described, some courts have been assertive and penetrating when confronted with claims of privilege, while others have been timid or credulous, sometimes only to discover later that they have been misled.

The principle that power corrupts is universally accepted; the phrase itself is an often-used idiom. The idea that secrecy corrupts, however, is not quite as prevalent—but it should be. Judges should not be awed or intimidated by the CLASSIFIED stamp, and excessive deference leads to increased opportunities for government misbehavior generally and unjust judicial results specifically. Courts should have the confidence and knowledge to assertively grapple with these issues, and members of the legal community should participate in a discussion about protected materials themselves. While there is substantial scholarship addressing what kind of protected information should be admissible and what standards and processes should control

those judgments, there is too little discussion of the protected material itself—a type of evidence that is here to stay, and which has huge implications across the jurisprudential spectrum.