ESSAY

NATIONAL SECURITY TRIALS: A JUDGE'S PERSPECTIVE

T.S. Ellis, III[*]

NATIONAL Security cases present challenging problems for federal courts—case management problems and problems raised by the novel and difficult legal issues these cases typically present. My very modest goal today is to identify some of these problems, to describe how courts have dealt with them, and along the way, to offer some observations and suggestions based chiefly on my personal experiences in presiding over some of these cases.

A useful starting point is to define what constitutes a National Security case. Here, definition by example works well. To be sure, the National Security label fits at least the following:

(1) criminal prosecutions for terrorist acts, including conspiracies to commit such acts;[1]

(2) criminal prosecutions for providing aid to designated terrorist organizations;[2]

(3) criminal prosecutions for espionage, including conspiracies to gain unauthorized access to classified information that qualifies as National Defense Information ("NDI"), in violation of the Espionage Act, 18 U.S.C. § 793 (2006);[3]

[*] Senior United States District Judge, Eastern District of Virginia. This is a lightly-edited version of the Ola B. Smith Lecture presented at the University of Virginia School of Law on April 15, 2013. I want to express my gratitude to the Virginia Law Review and the Student Legal Forum for inviting me to participate in the event. I also want to thank my law clerks—Martha Kidd, Lucas Beirne, and Erica Petri—for the substantial assistance they provided to me in this effort. I owe a special thanks to Tim Reagan of the Federal Judicial Center. His thorough research in this area has been of great assistance to me and other judges tasked with trying National Security cases. Of course, responsibility for the views expressed and any remaining errors are solely mine.

[1] See, e.g., United States v. Yousef, 327 F.3d 56, 79–80 (2d Cir. 2003) (plot to bomb U.S. airlines serving Southeast Asia routes); United States v. Salameh, 261 F.3d 271, 274 (2d Cir. 2001) (first World Trade Center bombing); United States v. Rahman, 189 F.3d 88, 104–11 (2d Cir. 1999) (conspiracy to bomb New York federal facilities, tunnels, and landmarks).

[2] See, e.g., 18 U.S.C. § 2339B (2006); United States v. Lindh, 212 F. Supp. 2d 541, 547 (E.D. Va. 2002).

[3] See United States v. Rosen, 445 F. Supp. 2d 602, 607 (E.D. Va. 2006).

(4) criminal prosecution of an Islamic charity for providing material aid to designated terrorist organizations;[4]
(5) civil damage actions for death or injury allegedly caused by terrorist acts;[5]
(6) civil damage actions against the United States for wrongful rendition or harsh interrogation methods;[6] and
(7) civil actions for writ of habeas corpus on behalf of numerous Guantanamo Bay detainees.[7]

Now, to put some flesh on the bones of these types of cases, let me briefly describe some specific cases that merit the National Security label.

Many of you will remember that terrorists exploded a bomb in the parking garage of the World Trade Center in New York City in 1993, killing six people and injuring more than 1000 others. This led to the prosecution of a number of people in the Southern District of New York, four of whom where ultimately convicted—others were fugitives—and those convicted received sentences ranging from 108 years to 117 years.[8]

Similarly, and also in the Southern District of New York, a number of conspirators were charged with planning to bomb certain New York landmarks, including the United Nations, the Federal Building, the Federal Bureau of Investigation ("FBI") headquarters, the diamond district, and the Lincoln and Holland Tunnels. This led to a nine-month trial (four days per week) and convictions of several of the plotters on various charges and sentences varying from twenty-five years to life.[9]

Perhaps the most famous case that merits the National Security label is the prosecution in the Eastern District of Virginia of Zacarias Moussaoui, the so-called Twentieth Hijacker of the 9/11 attacks.[10] This celebrated and protracted case was ably presided over by my colleague, Judge Leonie Brinkema. Ultimately, after protracted litigation, including

[4] See United States v. El-Mezain, 664 F.3d 467, 483 (5th Cir. 2011).
[5] See, e.g., In re Terrorist Attacks on September 11, 2001, 538 F.3d 71, 75 (2d Cir. 2008), abrogated by Samantar v. Yousuf, 130 S. Ct. 2278, 2286–89 (2010).
[6] See, e.g., El-Masri v. United States, 479 F.3d 296, 300–01 (4th Cir. 2007).
[7] See, e.g., Rasul v. Bush, 542 U.S. 466, 484 (2004) (holding that federal courts have jurisdiction over habeas petitions filed on behalf of Guantanamo Bay detainees).
[8] See United States v. Salameh, 261 F.3d 271, 275 (2d Cir. 2001).
[9] See United States v. Rahman, 189 F.3d 88, 103, 111 (2d Cir. 1999).
[10] United States v. Moussaoui, No. 01-455-A, 2003 WL 21263699, at *1–2 (E.D. Va. Mar. 10, 2003).

two interlocutory appeals,[11] Moussaoui pled guilty to conspiring to kill Americans (although he adamantly denied involvement in the 9/11 attacks).[12] In the ensuing capital sentencing proceeding, a jury unanimously agreed that Moussaoui was eligible for the death penalty because he had lied to federal agents knowing that people would die as a result of his lie.[13] In the end, the jury returned a verdict of life in prison.[14]

To finish putting flesh on the bones of the category of National Security cases, let me mention briefly: (1) the successful prosecution in the Eastern District of North Carolina of a Central Intelligence Agency ("CIA") contractor, who, while serving in Afghanistan, brutally assaulted an Afghan he was interrogating;[15] and (2) the prosecution in the Eastern District of Virginia of an American of Jordanian descent for plotting to kill President George W. Bush, which resulted in a conviction and a life sentence.[16]

The brief description of these cases suffices, I believe, to define what I mean by the label "National Security cases." An important thread that ties the cases in this category together is that they involve the use or potential use of classified information and materials in discovery, in hearings, and at trial. And it is this aspect of National Security cases that presents the most formidable set of challenges to federal courts, as I will explain shortly in more detail in the context of three cases over which I presided. I should also note that another characteristic common to National Security cases is that they understandably and appropriately receive and deserve substantial media attention and public scrutiny. This factor, as we shall see, can, and often does, clash with the need to use classified material in these cases.

Finally, let me note briefly that National Security cases are not a new phenomenon; they have always been with us. Recall, for example, the trial of Aaron Burr for treason, presided over (ironically)[17] by circuit-

[11] See United States v. Moussaoui, 382 F.3d 453, 462 (4th Cir. 2004); United States v. Moussaoui, 333 F.3d 509, 513–14 (4th Cir. 2003).

[12] United States v. Moussaoui, 591 F.3d 263, 266, 297 (4th Cir. 2010).

[13] See id. at 301.

[14] See id. at 302.

[15] See United States v. Passaro, 577 F.3d 207, 211 (4th Cir. 2009).

[16] See United States v. Abu Ali, 528 F.3d 210, 221, 223–24, 262, 269 (4th Cir. 2008).

[17] The irony arises from the following: Jefferson and Marshall did not like each other. See Robert K. Faulkner, John Marshall and the Burr Trial, 53 J. Am. Hist. 247, 247 (1966). Marshall's biography of Washington, commissioned by Bushrod Washington, Marshall's fellow sitting Justice, relegated Jefferson to a footnote on the Declaration of Independence. 3 Albert

riding Chief Justice Marshall,[18] and more recently, the Espionage Act trial of Ethel and Julius Rosenberg for passing classified H-bomb secrets to the then-Soviet Union.[19] Although National Security cases are not new, they are now more numerous in the Age of Terrorism.

The first case I want to raise in my discussion of the challenges and problems presented by National Security cases is *United States v. Lindh*,[20] the so-called American Taliban case. Lindh was born in the District of Columbia, schooled in California, and converted from Catholicism to Islam in his teens. At eighteen years old, he moved to Yemen to study Arabic and from there he moved to Pakistan to study at a Madrasah. He volunteered to fight with the Taliban in Afghanistan and was sent to the front lines as part of an Arabic-speaking group of Taliban and Al-Qaeda fighters. He was captured in Afghanistan by forces of the Northern Alliance, materially aided by U.S. personnel, weapons, and air support. After his capture, he was placed in a prison compound in Afghanistan and interviewed by a CIA officer, who was shortly thereafter killed by Taliban and Al-Qaeda prisoners in a melee that erupted at the prison. In due course, Lindh was transferred to a Navy ship (*U.S.S. Peleliu*), where he was interrogated and then flown back to the United States and the Eastern District of Virginia. There he was indicted on multiple charges, including: (i) conspiracy to murder U.S. nationals, including American military personnel and other governmental employees serving in Afghanistan following the September 11, 2001 terrorist attacks, in violation of 18 U.S.C. § 2332(b)(2); (ii) conspiracy to provide material support and resources to a foreign terrorist organization, in violation of 18 U.S.C. § 2339B; (iii) conspiracy to contribute services to

J. Beveridge, Conflict and Construction, 1800–1815, *in* The Life of John Marshall 244–45 (1919). Marshall was also critical of Jefferson's conduct during the Revolutionary War. 1 Albert J. Beveridge, Frontiersman, Soldier, Lawmaker, 1755–1788, *in* The Life of John Marshall 143–45 (1919). Jefferson and his Party enacted the 1802 Judiciary Act, which reinstated circuit-riding for Justices, a feature that did not please Marshall. Beveridge, Conflict and Construction, supra, at 56, 72. Jefferson hated Burr and wanted to see him convicted of treason. Id. at 388. Indeed, Jefferson, in his 1807 State of the Union message, pronounced Burr guilty of treason. President Thomas Jefferson, Seventh Annual Message (Oct. 27, 1807), available at http://www.presidency.ucsb.edu/ws/index.php?pid=29449. So, it is ironic that Jefferson's desire to punish Adams' judicial appointees by requiring circuit-riding led to Marshall presiding over the Burr trial and acquitting Burr. For a persuasive defense of Marshall's legal position in acquitting Burr, see Faulkner, supra, at 255–56.

[18] See United States v. Burr, 25 F. Cas. 55, 55 (C.C.D. Va. 1807) (No. 14,692D).

[19] See United States v. Rosenberg, 195 F.2d 583, 608–09 (2d Cir. 1951).

[20] 227 F. Supp. 2d 565 (E.D. Va. 2002).

Al-Qaeda, in violation of 31 C.F.R. §§ 595.204 and 595.205 and 50 U.S.C. § 1705(b); (iv) conspiracy to supply services to the Taliban, in violation of 31 C.F.R. §§ 545.204, 545.206(b), and 50 U.S.C. § 1705(b); and (v) using and carrying firearms and destructive devices during crimes of violence, in violation of 18 U.S.C. § 924(c).[21]

At the time the indictment was filed, the Lindh case was assigned to me. After substantial pretrial proceedings, including discovery and motions to suppress, Lindh pled guilty, not to any of the charges in the indictment, but instead to a criminal information charging him with carrying an explosive during the commission of a felony which may be prosecuted in a U.S. court—namely, supplying services to the Taliban—in violation of 18 U.S.C. § 844(h)(2). In the end, Lindh was sentenced to serve twenty years in prison, and in the course of the sentencing hearing, he admitted, under oath, each of the factual elements of the offense, and also tearfully admitted he had made a mistake in joining the Taliban.[22]

The first challenge the Lindh case presented arose in the course of discovery when Lindh's experienced and able counsel sought leave to interview Guantanamo Bay detainees who had been at the prison at the time the CIA agent was killed or who had fought with Lindh. Lindh's counsel proposed that they travel to the Guantanamo Bay facility to accomplish this. The government opposed defense counsel's proposal, explaining that interrogations of detainees in Guantanamo Bay were well underway there, that this was an important national security endeavor, and that defense counsel, by appearing there and interrupting this process, would undermine the goals and objectives of the Guantanamo Bay interrogation effort. The challenge, then, was to devise a means by which defense counsel could obtain the discovery they sought, and were entitled to,[23] without disrupting the government's ongoing Guantanamo Bay interrogation effort.

This challenge was met first by establishing a group of Department of Justice ("DOJ") and Department of Defense ("DOD") attorneys who were separate and independent from—indeed firewalled off from—the attorneys who represented the government in the Lindh prosecution, and then by implementing the following procedure: First, defense counsel

[21] See id. at 566 & n.2.

[22] See id. at 566, 572; Transcript of Sentencing Hearing at 42–47, United States v. Lindh, 227 F. Supp. 2d 565 (2002) (No. 02-37-A); 'I Made a Mistake by Joining the Taliban': Apologetic Lindh Gets 20 Years, Wash. Post, Oct. 5, 2002, at A1.

[23] See Fed. R. Crim. P. 16.

were permitted to submit to the firewalled DOJ and DOD attorneys a list of proposed written questions to be put to each of the Guantanamo Bay detainees designated by defense counsel. These questions were then screened by the firewalled DOJ and DOD attorneys and, in the event the firewalled attorneys had any objections to the proposed questions, those objections were submitted to me under seal with access limited to defense counsel and me. Defense counsel were then required to file a prompt response to these objections, after which I, equally promptly, resolved the objections. All of defense counsel's proposed questions, except those to which an objection was sustained (in the end, there were no objections), were put to the various designated detainees by DOD interrogators, who were given the discretion to interweave the questions submitted by defense counsel with other portions of the government's ongoing interrogation of those detainees. The firewalled DOD and DOJ attorneys then provided defense counsel with a written summary of each detainee's response to the questions submitted. After that, defense counsel were afforded a brief opportunity to submit to the firewalled attorneys any written follow-up questions they wanted to ask any detainee, subject to the same objection and court-review process that applied to defense counsel's initial questions. Once any further objections were resolved (again, there were none), the DOD interrogators put defense counsel's follow-up questions to the designated detainees, and as soon as practicable thereafter, the firewalled attorneys furnished defense counsel with a video recording of the pertinent portions of the interrogations of each designated detainee. In the end, this procedure proved to be a satisfactory solution to the problem, although it is important to note that this solution might well not be adequate or work well in all contexts.

The second challenge the Lindh case presented arose in the circumstances of Lindh's motion to suppress statements that he made to covert government personnel and others, including a CNN reporter and an FBI agent, in the two-week period immediately following his capture in Afghanistan and prior to his transfer to a Navy ship. The government expressed concern that the identity of certain covert government personnel would be disclosed in the course of any evidentiary hearing held in connection with defendant's suppression motion. To address this concern, the following procedure was devised, designed to accommodate both Lindh's Sixth Amendment confrontation right and the government's interest in preserving the secret identity of any covert government employee whose testimony might be required at the hearing. First, any such

witness would enter the courtroom by way of the prisoner's elevator, which is both separate from the elevators used by the public, and not visible to the public. The witness would then walk to the witness stand, staying always behind a curtain that concealed the witness from the view of those seated in the gallery of the courtroom. This curtain also prevented the witness from being seen by anyone in the gallery throughout his or her testimony. Lindh and his counsel, however, would be seated in the jury box, directly across from the witness, and would therefore be able to observe the witness throughout the testimony. The witness would then testify using a pseudonym and an electronic voice distortion device.

Not by any means a perfect solution, but a reasonable one, and a practical means of preserving Lindh's Sixth Amendment confrontation right, while still also preserving the secret identity of any covert government witness. As it happens, on the day of the scheduled suppression hearing, Lindh entered a guilty plea and the suppression hearing was therefore unnecessary.

National Security cases often present novel legal issues. The Lindh case was no exception. Lindh, by counsel, argued that Count One of the indictment—conspiracy to murder nationals of the United States, including American military personnel and other governmental employees serving in Afghanistan following the September 11, 2001 terrorist attacks, in violation of 18 U.S.C. § 2332(b)(2)—had to be dismissed because Lindh, as a Taliban soldier, was a lawful combatant and therefore entitled to the affirmative defense of lawful combatant immunity. Lawful combatant immunity grants immunity to soldiers for their lawful, belligerent acts committed during the course of armed conflicts against legitimate military targets.[24]

After argument and briefing, I found that Lindh's status as a Taliban fighter did not make him eligible for immunity from prosecution, and I did so for three reasons: (1) because the President had determined that Lindh was an unlawful combatant and this determination, under well-settled law, was entitled to deference as a reasonable interpretation and

[24] See Geneva Convention Relative to the Treatment of Prisoners of War art. 4–5, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter Geneva Convention] (providing that only lawful combatants are eligible for immunity from prosecution); Ex Parte Quirin, 317 U.S. 1, 30–31 (1942) ("Lawful combatants are subject to capture and detention as prisoners of war by opposing military forces. Unlawful combatants are likewise subject to capture and detention, but in addition they are subject to trial and punishment by military tribunals for acts which render their belligerency unlawful.").

application of the Geneva Convention;[25] (2) because Lindh had not met his burden of demonstrating that he was a lawful combatant given the criteria set forth in the Geneva Convention;[26] and (3) because the Taliban/Al-Qaeda did not meet the Convention's criteria for determining entitlement to lawful combatant status.[27]

Although the question whether a member of the Taliban, Al-Qaeda, or other terrorist organization is entitled to lawful combatant immunity remains relevant today, the focus in cases involving these sorts of defendants has shifted to whether these defendants can be tried in military commissions or must instead be tried in federal courts.[28]

If the Lindh case involved a substantial mound of classified documents and information—and it did—the case of *United States v. Rosen*[29] involved a veritable mountain of such material, and the focus of my remarks now shifts to the problems raised by a court's need to deal with classified information in pretrial and trial proceedings. But first, a brief summary of the *Rosen* case is appropriate.

Steven Rosen and Keith Weissman were policy analyst employees[30] with the American Israel Public Affairs Committee ("AIPAC"), a lobby-

[25] *Lindh*, 212 F. Supp. 2d at 556–58 ("[C]ourts have long held that treaty interpretations made by the Executive Branch are entitled to some degree of deference."). See, e.g., Kolovrat v. Oregon, 366 U.S. 187, 194 (1961) ("While courts interpret treaties for themselves, the meaning given them by the departments of government particularly charged with their negotiation and enforcement is given great weight."). This result is also consistent with the deference afforded executive branch agencies by *Chevron USA, Inc. v. Natural Res. Def. Council*, 467 U.S. 837, 843 (1984).

[26] *Lindh*, 212 F. Supp. 2d at 558. Defendants bear the burden of establishing affirmative defenses. See, e.g., Mullaney v. Wilbur, 421 U.S. 684, 697–99 (1975); Smart v. Leeke, 873 F.2d 1558, 1565 (4th Cir. 1989).

[27] *Lindh*, 212 F. Supp. 2d at 558. Under Article 4(A)(2) of the Geneva Convention, an organization must meet four requirements:

> (1) the organization must be commanded by a person responsible for his subordinates;
> (2) the organization's members must have a fixed distinctive emblem or uniform recognizable at a distance;
> (3) the organization's members must carry arms openly; and
> (4) the organization's members must conduct their operations in accordance with the laws and customs of the war.

Geneva Convention, Relative to the Treatment of Prisoners of War art. 4(A)(2), Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135.

[28] See, e.g., Boumediene v. Bush, 553 U.S. 723, 736 (2008).

[29] See United States v. Rosen, 445 F. Supp. 2d 602 (E.D. Va. 2006).

[30] Rosen was AIPAC's Director of Foreign Policy Issues, exercised policymaking authority over issues of interest to AIPAC, and was primarily engaged in lobbying officials of the

ing group that advocates pro-Israel policies to Congress and the executive branch of the United States. Rosen and Weissman were interested in, and working on, the threats posed to this country and to Israel by Iran and other Middle Eastern entities.

A superseding indictment issued in 2005, naming Rosen, Weissman, and Lawrence Franklin, an official from the DOD,[31] alleged that they violated the Espionage Act by engaging in a conspiracy to communicate NDI to persons not entitled to receive it, in violation of 18 U.S.C. § 793(g). In essence, this appeared to be yet another, not uncommon case of Washington backchannel unauthorized disclosure of classified information designed to influence government policy.[32] Franklin, on the basis of his knowledge and experience, considered that Iran posed a very serious threat to this country and to peace in the Middle East, and was concerned that the State Department's policy toward Iran did not accurately assess and weigh this threat. Franklin discussed this situation with Rosen and Weissman, whose somewhat more hardline views on Iran were more aligned with Franklin's. Franklin apparently hoped that by disclosing certain classified material to Rosen and Weissman, they (Rosen and Weissman) would be able to influence U.S. government policy to move to a position more in accord with his (Franklin's) view with respect to Iran.[33]

executive branch. Weissman was AIPAC's Senior Middle East Analyst and worked closely with Rosen in lobbying members of the executive branch. Id. at 608.

[31] Franklin worked on the Iran desk in the Office of the Secretary of the Department of Defense. Id. at 608.

[32] See United States v. Rosen, 520 F. Supp. 2d 802, 808 (E.D. Va. 2007) ("[D]efendants claim that . . . the overt acts reflect nothing more than the well-established official Washington practice of engaging in 'back channel' communication with various non-governmental entities and persons for the purpose of advancing U.S. foreign policy goals."); Neil A. Lewis, Trial to Offer Look at World of Information Trading, N.Y. Times, Mar. 3, 2008, at A14 ("The defense's goal is to demonstrate that the kind of conversations in the indictment are an accepted, if not routine, way that American policy on Israel and the Middle East has been formulated for years."). For a discussion of backchannel communications, see, e.g., Max Frankel, The Washington Back Channel, N.Y. Times, Mar. 25, 2007, at 40 ("'High officials of the government reveal secrets in the search for support of their policies, or to help sabotage the plans and policies of rival departments. . . . Though not the only vehicle for this traffic in secrets—the Congress is always eager to provide a forum—the press is probably the most important.'").

[33] For a thorough and insightful discussion of unauthorized disclosure of classified information by government personnel to the press and others, see Gabriel Schoenfeld, Necessary Secrets: National Security, the Media, and the Rule of Law 17–26 (2010).

For his part, Franklin pled guilty to three charges, namely: (i) conspiracy to communicate National Defense Information to persons not entitled to receive it, in violation of 18 U.S.C. § 793(g); (ii) conspiracy to communicate classified information to an agent of a foreign government, in violation of 18 U.S.C. § 371; and (iii) unlawful retention of National Defense Information, in violation of 18 U.S.C. § 793(e).[34] Franklin also agreed to cooperate with the government in the prosecution of Rosen and Weissman. Thereafter, the prosecution proceeded apace with the parties, who raised, briefed, and argued a full menu of challenging issues, including: (i) the constitutionality of the Espionage Act;[35] (ii) whether disclosure to the defense of certain Foreign Intelligence Surveillance Act ("FISA") applications, orders, and other materials was warranted;[36] (iii) whether trial subpoenas should issue to Condoleezza Rice and nineteen other high-ranking government officials from the Department of State and the DOD;[37] and (iv) whether Rosen and Weissman were deprived of their Sixth Amendment right to compulsory process by the government's refusal to invoke the Mutual Legal Assistance Treaty between Israel and the United States to request that Israel compel three Israeli government officials to provide deposition testimony that Rosen and Weissman believed would be exculpatory.[38]

[34] *Rosen*, 520 F. Supp. 2d at 804 n.3.

[35] See United States v. Rosen, 445 F. Supp. 2d 602, 645 (E.D. Va. 2006) (holding that "the balance struck by [18 U.S.C.] § 793 between these competing interests [the First Amendment and National Security] is constitutionally permissible").

[36] See United States v. Rosen, 447 F. Supp. 2d 538, 546–47 (E.D. Va. 2006) (holding that "disclosure of the FISA materials to defendants is not warranted in this case" because the materials "presented none of the concerns that might warrant disclosure to defendants" and the government has a "legitimate national security interest in maintaining the secrecy of the information contained in the FISA applications"); see also United States v. Dumeisi, 424 F.3d 566, 578 (7th Cir. 2005) (finding that the district court did not abuse its discretion in "substituting the government's summary of classified information . . . for the actual information"); United States v. Damrah, 412 F.3d 618, 625 (6th Cir. 2005) (affirming district court's denial of motions "to compel [production of] FISA materials and suppress FISA evidence"); United States v. Squillacote, 221 F.3d 542, 554 (4th Cir. 2000) (denying appellants' "request for disclosure of the FISA materials").

[37] See *Rosen*, 520 F. Supp. 2d at 814–15 (issuing trial subpoenas to certain high-ranking government officials and stating that the specific reasoning and ruling for each witness subpoena would be set forth in a "classified and sealed order").

[38] See United States v. Rosen, 240 F.R.D. 204, 214 (E.D. Va. 2007) (holding that "denial of defendants' motion to compel the U.S. government to invoke the [Mutual Legal Assistance] Treaty for defendants' benefit will not cause the loss of favorable testimony" and that "the right to compulsory process extends only to forms of process a court can issue of its

Yet, in the end, after more than three and a half years of litigation, the government, rather abruptly, decided to abandon the prosecution and sought dismissal of the indictment against Rosen and Weissman. I granted this request.[39] The government was neither required to give reasons for dismissing the indictment, nor did it do so.

There are, to be sure, many practical problems relating to a court's handling, storing, and limiting access to classified information. Although federal judges do not require any background check or clearance to see Top Secret/Sensitive Compartmented Information,[40] law clerks, court reporters, and deputy clerks involved in the handling of classified information must all undergo background investigations and receive appropriate clearances for such material.[41] Government and defense counsel must also receive appropriate clearances.[42] Defendants, of course, are

own power, not to forms of process that require the cooperation of the Executive Branch or foreign courts").

[39] See Order, United States v. Rosen, No. 1:05cr225 (E.D. Va. May 1, 2009). Following his plea, Franklin was initially sentenced to a total of 151 months imprisonment, consisting of concurrent 120-month sentences on each of the two § 793 charges, and 31 consecutive months on the § 371 charge. See Judgment, United States v. Franklin, Nos. 1:05CR00421-001 & 1:05CR00225-001 (E.D. Va. Jan. 20, 2006). Later, after the charges against Rosen and Weissman were dismissed, the government appropriately moved to reduce Franklin's previously imposed sentence. This motion was granted and Franklin's 151-month custody sentence was accordingly reduced to two years of supervised probation, with the special conditions that he serve ten months in community confinement and perform 100 hours of community service. See Order, United States v. Franklin, Nos. 1:05cr421 & 1:05cr225 (E.D. Va. June 11, 2009). And, with respect to the community service portion of his sentence, Franklin was specifically directed to give lectures about, and otherwise publicize, the importance of public officials adhering to the rule of law and the importance of not mishandling or improperly disclosing classified information. Id. at 2.

[40] "Top Secret Information" is defined as "information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security." Exec. Order No. 13,526, 75 Fed. Reg. 707, 707 (Dec. 29, 2009). "Sensitive Compartmented Information" is not a classification, but is instead a process for handling particular types of classified information.

[41] For a helpful and thorough summary of this topic, see Robert Timothy Reagan, Federal Judicial Center, Keeping Government Secrets: A Pocket Guide on the State-Secrets Privilege, the Classified Information Procedures Act, and Classified Information Security Officers 1–3 (2d ed. 2013), available at http://www.fjc.gov/public/pdf.nsf/lookup/keeping-government-secrets-2d-reagan-2013.pdf/$file/keeping-government-secrets-2d-reagan-2013.pdf.

[42] See id. at 2.

not cleared to have access to classified information and courts generally agree that this presents no due process problem.[43]

Also, classified documents must be handled and stored with appropriate safeguards. For this purpose, courts handling National Security cases typically have a Sensitive Compartmented Information Facility—commonly referred to as a SCIF. A SCIF is a fully enclosed area within a building that is used to store and process classified information. A SCIF is typically subject to an electronic security system and also has multiple combination locks, both on the door leading into the SCIF and on each of the individual file cabinets located within the SCIF. A log records every entry into the SCIF, including the name of the person who entered and the precise time the person entered and exited. In essence, a classified document must never be out of the possession of a cleared person, must never be disclosed or exposed to an unauthorized, uncleared person, must never be removed from the courthouse, and must be stored in the SCIF when not in use.[44]

Courts now routinely and effectively deal with the problems associated with handling, storing, and restricting access to classified information. Thus, my focus today is on the more difficult problems posed by the need to use classified information in the trial of National Security cases.

First, let me make a general observation. On the basis of my exposure to classified information over a number of years, especially the *Rosen* case, I have a firm suspicion that the executive branch over-classifies a great deal of material that does not warrant classification. It is important

[43] See United States v. Moussaoui, 591 F.3d 263, 290 (4th Cir. 2010) ("The Government's interest in protecting the classified information during the discovery and appeal process justified the limited restrictions upon [defendant's] right to communicate with counsel pending completion of the CIPA process and preparation of unclassified substitutions." (citing United States v. Abu Ali, 528 F.3d 210, 254 (4th Cir. 2008))); *Abu Ali*, 528 F.3d at 254 ("A defendant and his counsel, if lacking in the requisite security clearance, must be excluded from hearings that determine what classified information is material and whether substitutions crafted by the government suffice to provide the defendant adequate means of presenting a defense and obtaining a fair trial. Thus, the mere exclusion of [defendant] and his uncleared counsel from the CIPA hearings did not run afoul of CIPA or [defendant's] Confrontation Clause rights.").

[44] An exception to this is that Court Security Officers ("CSOs") are authorized to deliver classified material to, or remove such material from, the courthouse. CSOs are security experts provided by DOJ to aid courts in storing and handling classified information. See 18 U.S.C. app. 3 § 9 notes (2006) (Court Security Officer, Custody and Storage of Classified Materials).

to keep in mind that the classification of material is exclusively the province of the executive branch; courts have no power or authority to classify or to declassify material. And, as I noted, I suspect that despite the regulation that requires doubts about classification to be resolved against designating material as classified,[45] classifying officials often seem to apply the reverse of this regulation, namely doubts about whether materials should be classified are, more often than not, resolved not against, but in favor of classification. Understandably perhaps, classifying officials may consider that errors stemming from over-classification are less consequential than errors stemming from a failure to classify material that warrants classification.

But it is important to emphasize that my suspicion that over-classification is endemic is just that—a suspicion—for I have seen only a miniscule subset of the vast universe of materials that are classified by the executive branch.[46] Also, I am not privy to all of the considerations that must be taken into account by a person making the classification determination with respect to each specific candidate document or piece of information. Especially important here is the need to avoid disclosure of information that might reveal to an enemy analyst our country's *sources and methods* of obtaining intelligence information. This is often a subtle matter and it is not obvious to an inexperienced person that disclosure of some document might disclose our country's sources and methods, even though the information contained in the document might now appear fairly innocuous. If disclosure of information or documents allows an enemy analyst to discern this country's sources and methods for gathering intelligence information, the enemy can then undertake countermeasures, which, significantly, may include identifying and silencing or terminating human intelligence sources.

In summary on this point, let me say the following: This country has, and must have and must safeguard, necessary secrets—secrets necessary, indeed vital to our national security. The classification and declassification processes are and have been governed for decades by Executive Orders, the most recent of which issued in December 2009. This Executive Order on its face appears to establish reasonable and sound

[45] See Exec. Order No. 13,526, 75 Fed. Reg. 707, 707 (Dec. 29, 2009) (providing that "[i]f there is significant doubt about the need to classify information, it shall not be classified").

[46] In 2005, the United States established classifications 14.2 million times, which amounts to an average of "39,000 a day, or 1,600 every hour of the night and day." Ted Gup, Nation of Secrets: The Threat to Democracy and the American Way of Life 8 (2007).

regulations governing the executive branch's designation of classified material, the handling of such material, the duration of classification, and importantly, a mandatory process for automatic and systematic declassification of classified material over time.[47] But there is reason to believe that these regulations are not working effectively, and I note that I am not a lone voice in expressing the opinion that over-classification of documents and information has occurred and is occurring; other observers of this scene have reached the same conclusion. Thus, the Public Interest Declassification Board, an advisory committee established by Congress to promote public access to information concerning U.S. national security decisions and activities, published a recent report to the President. One of the Board's findings was that "present practices for classification and declassification of national security information are outmoded, unsustainable and keep too much information from the public."[48] The Board's recommendations are far-reaching and, it seems to me, quite sensible.[49] Central to any reform effort should be the need to establish a declassification authority that is separate and independent from the classification authority. We should all watch with interest to see whether the Board's recommendations are implemented and whether they are effective to reduce the plague of over-classification.

Now let me turn to the use of classified information in the litigation process. The centerpiece here is the Classified Information Procedures Act ("CIPA"),[50] which provides a detailed procedure for using classified information in a criminal prosecution.[51] In essence, CIPA prescribes a detailed procedure for identifying and protecting classified information that is relevant and merits use as evidence at trial. Thus, each party is required to designate any classified information they expect to use or disclose during pretrial proceedings or trial.[52] Once the parties identify the classified material thought to be relevant and necessary, the court must

[47] See Exec. Order No. 13,526, 75 Fed. Reg. 707 (Dec. 29, 2009).

[48] Public Interest Declassification Board, Report to the President from the Public Interest Declassification Board 1 (2012), http://www.archives.gov/declassification/pidb/recommendations/transforming-classification.pdf; see also Steven Aftergood, Reducing Government Secrecy: Finding What Works, 27 Yale. L. & Pol'y Rev. 399, 415–16 (2009).

[49] See Public Interest Declassification Board, supra note 48, at 2–5.

[50] 18 U.S.C. app. 3 §§ 1–16 (2006).

[51] Id. § 46.

[52] Id. §§ 5, 6(a).

hold a sealed hearing concerning the relevance, admissibility, and use of the classified information.[53]

If the court determines that a particular piece of classified information is relevant and may be used as evidence, the government may acquiesce and declassify the information, or it has several options to prevent the disclosure of that classified information. Specifically, the government may file a motion requesting that the court substitute in lieu of specific classified information, either (i) a statement admitting relevant facts that the classified information would tend to prove or (ii) a summary of the classified information that adequately masks the essential secret information.[54] The court will authorize the substitution if it finds that the substitution "will provide the defendant with substantially the same ability to make his defense as would disclosure of the specific classified information."[55]

If the court denies the government's motion for substitution or otherwise requires disclosure of classified information, the government may then file an affidavit of the Attorney General certifying that the disclosure of the classified information at issue would pose a danger to national security and objecting to the disclosure of the classified information.[56] If such an affidavit is filed, the court must prohibit the defendant from disclosing or causing the disclosure of the classified information at issue.[57] But that prohibition comes at a cost to the government. Once the court prohibits the disclosure of the classified information, the court may either dismiss the indictment or take some other action the court determines is required in the interests of justice.[58] CIPA provides that those actions may include, but are not limited to: (i) "dismissing specified counts of the indictment or information"; (ii) finding against the government on the issue as to which the classified information relates; or (iii) "striking or precluding all or part of the testimony of a witness."[59]

The government may take an interlocutory appeal from a decision or order of the district court authorizing the disclosure of classified information, imposing sanctions for nondisclosure of classified information,

[53] Id. § 6(a).
[54] Id. § 6(c)(1).
[55] Id.
[56] Id. § 6(c)(2).
[57] Id. § 6(e)(1).
[58] Id. § 6(e)(2).
[59] Id.

or refusing a protective order sought to prevent the disclosure of classified information.[60] These interlocutory appeals stay the trial until the appeals are resolved.[61]

On the whole, CIPA, in my experience, works well. It is, however, very labor intensive for judges and counsel. Thus, in the *Rosen* case, there were a total of thirty-five sealed CIPA hearings consuming many hours over the course of forty-five days. Those hearings resulted in the issuance of numerous orders including, on one occasion, a 278-page sealed, classified CIPA order,[62] which the Fourth Circuit affirmed on the government's interlocutory appeal.[63]

Although CIPA is comprehensive in the criminal context,[64] some courts have nonetheless found it useful to supplement CIPA and create what is now commonly known as the "Silent Witness Rule." Under this judicially created rule, the court, witnesses, counsel, and the jurors are given unredacted classified documents, but the public can see only redacted versions of the documents. Then, when counsel or a witness

[60] Id. §7.

[61] Id.

[62] Many of the briefs, documents, and orders or portions thereof from the *Rosen* case are currently sealed because they contain classified information. In two years, ten years will have passed since the filing of the *Rosen* indictment, and pursuant to § 1.5 of the existing Executive Order, some or all of that material may be subject to declassification. See Exec. Order No. 13,526, 75 Fed. Reg. 707, 709 (2009). The Executive Order provides that at the time a document is classified, the original classification authority must establish a specific date or event for declassification based on the duration of the national security sensitivity of the information. See id. When that date is reached, the information is automatically declassified, unless there is a particular reason that it should not be declassified. Id. Information must be marked for declassification ten years from the date of the original classification if an earlier specific date or event triggering declassification cannot be determined. Id. Thus, a document will originally be given a classification period of ten years or less unless the document falls into one of several particularly sensitive categories. Id. Given that much of the currently sealed classified material in the record of the *Rosen* case may no longer warrant classification, and because no case file should remain perpetually sealed, I intend, upon the ten-year anniversary of the *Rosen* case filing, to issue an order requiring the government to identify those pleadings and documents that have been declassified and to explain why other documents must remain classified. See generally T.S. Ellis, III, Sealing, Judicial Transparency and Judicial Independence, 53 Vill. L. Rev. 939, 949 (2008) ("Permanent sealing is as unnecessary as it is pernicious. . . . If records are to be placed under seal, the seal should continue only as long as reasonably necessary in light of the reasons that originally warranted sealing.").

[63] See United States v. Rosen, 557 F.3d 192, 200 (4th Cir. 2009).

[64] By its terms, CIPA applies only to criminal cases. A regulation at 28 C.F.R. § 17.17(c) (2012) provides for CIPA-like procedures to be used in civil cases.

seeks to direct the jury's attention to a classified portion of a document, counsel or the witness would refer only to the page, paragraph, and line number of the pertinent document. If the witness needed to refer to specific language, or content that was classified, the witness would use code names such as "Country A," "Report X," or "Foreign Person Y" to conceal the classified information. This coding would also change with different witnesses so that what was "Country A" with one witness might be referred to as "Country B" by another.

The government in *Rosen* proposed widespread use of the Silent Witness Rule to protect classified information and I rejected that effort as it would effectively and impermissibly close the courtroom.[65] Nonetheless, I did approve a far more limited use of the Rule to protect a very small amount of the classified information.[66]

If CIPA is a statute that works reasonably well and merits a passing grade of, say, B or B-, the Espionage Act is a statute that, in its current form, does not work well and deserves a failing grade; it stands in urgent need of study and revision. In the course of assessing the Act's constitutionality, I expressed my agreement with those critics who have labeled it "excessively complex, confusing, indeed impenetrable."[67] Nor am I alone in criticizing the Espionage Act; Justice Harlan, joined by Chief Justice Burger and Justice Blackmun, described the Act as a "singularly opaque statute."[68] Also, in a concurring Fourth Circuit opinion in 1988, Judge James Dickson Phillips described the Espionage statutes as "un-

[65] See United States v. Rosen, 520 F. Supp. 2d 786, 788 (E.D. Va. 2007).

[66] Some courts have referenced, but not explicitly approved or endorsed, the Silent Witness Rule ("SWR"). See, e.g., United States v. Fernandez, 913 F.2d 148, 162 (4th Cir. 1990) (rejecting the proposed use of the SWR as untimely, but noting that the government's proposal was "ingenious"); United States v. Zettl, 835 F.2d 1059, 1063, 1067 (4th Cir. 1987) (noting the district court's approval of limited use of the SWR and affirming the district court on other grounds); United States v. North, 1988 WL 148481, at *3 (D.D.C. Dec. 12, 1988) (rejecting the SWR in "this particular case which will involve thousands of pages of redacted material and numerous substitutions" without addressing the SWR's applicability in other contexts). Other courts, without using the term "Silent Witness Rule," have approved the presentation of evidence in one form to the jury and in another form to the public. See, e.g., United States v. George, Nos. 91-0521 & 92-0215, 1992 WL 200027, at *3 (D.D.C. July 29, 1992) (withholding witnesses' names from the public, but disclosing them to defendant, the court, and the government's counsel via a "key card" filed under seal); United States v. Pelton, 696 F. Supp. 156, 156–59 (D. Md. 1986) (allowing recorded conversations containing classified information to be played only to the court, counsel, defendant, and the jury, while making only a redacted trial transcript available to the public).

[67] United States v. Rosen, 445 F. Supp. 2d 602, 613 (E.D. Va. 2006).

[68] New York Times Co. v. United States, 403 U.S. 713, 754 (1971) (Harlan, J., dissenting).

wieldy and imprecise instruments for prosecuting government 'leakers' to the press."[69] All of these criticisms are well-founded and I agree with Judge Phillips and with knowledgeable commentators that the proper solution is for Congress to amend the Espionage Act "through carefully drawn legislation."[70]

In the *Rosen* case, very able defense counsel challenged the constitutionality of the Act on several grounds. Although I ultimately rejected all of these grounds and found the Act constitutional,[71] I also found it necessary to add judicial glosses to the statute that included heightening the scienter requirement in order to save the Act's constitutionality.[72]

Although a detailed history and analysis of the Espionage Act and specific recommendations for revision of the Act are beyond the scope of this lecture,[73] let me nonetheless offer three modest general observations.

First, the revised Act should incorporate the judicial glosses with respect to the scienter required for criminal liability that I and at least one other judge[74] found necessary for the Act to pass constitutional muster.

Second, a revised Act should extend explicitly to unauthorized oral or other intangible disclosures of NDI, as well as to unauthorized disclosures of tangible NDI such as documents, flash or thumb drives, etc.[75]

Third, a revised Act should criminalize unauthorized disclosures, not of classified information, but of NDI, as does the current Act. But the current statutory definition of NDI stands in need of careful review and revision. Importantly, by limiting criminal responsibility to unauthorized disclosure or receipt of material that is NDI, rather than material that is classified, criminal liability is determined not by the executive branch, but in the first instance, by Congress and, ultimately, by a jury, which will not convict unless the government proves beyond a reasonable

[69] United States v. Morison, 844 F.2d 1057, 1085 (4th Cir. 1988) (Phillips, J., concurring).

[70] Id. at 1086 (majority opinion).

[71] See *Rosen*, 445 F. Supp. 2d at 645.

[72] Id. at 617–35.

[73] Let me note, however, that this topic would make an excellent subject for a semester course or a faculty or student research project.

[74] See *Morison*, 844 F.2d at 1083–84 (Wilkinson, J., concurring).

[75] See *Rosen*, 445 F. Supp. 2d at 614–17 (construing the term "information" as used by § 793 of the Espionage Act to include unauthorized intangible, that is, oral, disclosures of NDI).

doubt all the elements of the offense, including that the material in question is NDI.[76]

Let me also note that commentators have focused considerable attention and criticism on the potential application of the Espionage Act to the prosecution of reporters who publish leaked classified information.[77] This attention is not misplaced; let me illustrate this with a hypothetical. Let us suppose that a government DOD or DOJ employee has detailed, top-secret information concerning the drone program to kill members of Al-Qaeda and other terrorists overseas, including those who might be American citizens. Also assume that this information included the time and place of the drone attacks, the subject of the drone attacks, and information that might disclose the source of this intelligence. And assume further that this employee strongly objects to this program on moral, legal, or other grounds, and decides, at the request of a like-minded journalist friend, to leak this information to the journalist for publication with the aim of frustrating or preventing the program. The question this

[76] For a recitation of the elements of the offense of conspiracy to violate §§ 793(d) and (e) of the Espionage Act by orally disclosing NDI, see United States v. Rosen, 520 F. Supp. 2d 786, 793 (E.D. Va. 2007).

[77] See, e.g., William E. Lee, Probing Secrets: The Press and Inchoate Liability for Newsgathering Crimes, 36 Am. J. Crim. L. 129, 167–76 (2009) ("[N]ovel problems are presented by criminalization of the activities of outsiders, such as journalists, who solicit classified information or cultivate relationships with insiders to receive leaks. . . . [T]he right of the press to publish confidential information is well established. There is, however, a paucity of constitutional doctrine protecting newsgathering activities that seek the leaking of confidential information."); Mary-Rose Papandrea, Lapdogs, Watchdogs, and Scapegoats: The Press and National Security Information, 83 Ind. L.J. 233, 237, 298–305 (2008) (arguing that "prosecutions against nongovernmental actors for inchoate crimes of conspiracy and aiding and abetting violations of the Espionage Act and related laws violate the First Amendment because they are backdoor attempts to punish the publication of classified information in situations when a prosecution based on publication would be impermissible"); Derigan A. Silver, National Security and the Press: The Government's Ability to Prosecute Journalists for the Possession or Publication of National Security Information, 13 Comm. L. & Pol'y 447, 483 (2008) (suggesting that Congress amend statutes such as the Espionage Act to include "specific provisions designed to prevent the possibility that the broad language of all the identified statutes might be used to prevent the disclosure of information that sheds light on government incompetence or corruption"); Christina E. Wells, Contextualizing Disclosure's Effects: Wikileaks, Balancing, and the First Amendment, 97 Iowa L. Rev. Bull. 51, 56 (2012) (noting that "Rosen's balancing test is actually quite malleable and can result in substantial deference to government officials' claims of threats to national security"); Keith Werhan, Rethinking Freedom of the Press After 9/11, 82 Tul. L. Rev. 1561, 1583 (2008) (noting that "lack of doctrinal clarity surrounding the press's First Amendment right to receive, possess, and publish classified information helps sustain the Justice Department's publicly announced threat of prosecution").

hypothetical poses is whether the government employee and the journalist are subject to prosecution under the Act for engaging in a conspiracy to disclose NDI without authorization.[78]

Under the Act as it currently exists, the answer to this question is clearly, *yes*. And interestingly, whether these individuals turn out to be heroic whistleblowers or criminal leakers depends first on whether the government decides to prosecute, which for various reasons it may decide not to do.[79] But if the government decides to prosecute, then whether the person is a criminal leaker or a heroic whistleblower depends on whether the government proves to the jury beyond a reasonable doubt all of the elements of the offense under the Espionage Act, including whether the information was NDI. In other words, neither journalists nor anyone else has a First Amendment right to receive unauthorized disclosures of NDI or to make unauthorized disclosures of NDI to foreign governments, sympathetic journalists, or indeed anyone. If a journalist engages in conduct that satisfies all the elements of an offense under the Act, he or she is liable to be prosecuted and he or she could be convicted if the jury finds that the government has proved those elements beyond a reasonable doubt. In that event, the hypothetical journalist might well appropriately be labeled a criminal leaker and not a heroic whistleblower.

[78] In this regard, it is well to remember that a conviction for engaging in a criminal conspiracy does not depend on proof that the conspiracy succeeded. See United States v. Min, 704 F.3d 314, 321–22 (4th Cir. 2013); see also United States v. Rosen, 599 F. Supp. 2d 690, 694 n.6 (E.D. Va. 2009) (citing United States v. Nicoll, 664 F.2d 1308, 1315 (5th Cir. 1982)), overruled on other grounds by United States v. Henry, 749 F.2d 203, 205–06 (5th Cir. 1984). Thus, conspirators who plot to obtain NDI may be convicted under the Act even though they never succeed in obtaining the NDI they sought.

[79] An example of this is the well-known Pentagon Papers incident in which classified documents were disclosed to *The New York Times* and no prosecution occurred. Note, however, that it is doubtful that *The New York Times* conspired with Daniel Ellsberg to obtain the Pentagon Papers; rather, it appears the papers were in effect left on *The New York Times*'s doorstep. See, e.g., David Rudenstine, The Book in Retrospect, 19 Cardozo L. Rev. 1283, 1292 (1998) ("Although the Government did not charge that the newspapers had committed trespass or fraud to obtain the [Pentagon Papers], the newspapers insisted that they had done nothing improper to obtain a copy of the study."). Thus, there was no proof that the *The New York Times* was a conspirator or had the requisite scienter, and it is also questionable whether the material satisfied the NDI requirement. The potential for executive branch embarrassment is not a valid basis for either classification or qualification as NDI.

The final case that merits mention here is *El-Masri v. Tenet*.[80] Khaled El-Masri, a German citizen of Lebanese dissent, filed suit in the Eastern District of Virginia, claiming that on December 31, 2003, he was seized by Macedonian authorities while he was on vacation in Macedonia, and held for twenty-three days during which time he was brutalized and mistreated, and then handed over to the CIA.[81] El-Masri claimed that the CIA flew him to a detention facility near Kabul, where he was held against his will, brutally mistreated and interrogated, until May 28, 2004, when he was taken to a remote area in Albania and released.[82]

In his lawsuit, El-Masri alleged three causes of action. First, he alleged a *Bivens* claim,[83] asserting that former Director of the CIA George Tenet and ten unnamed CIA employees violated his Fifth Amendment right to due process.[84] In his second cause of action, El-Masri asserted a claim under the Alien Tort Statute,[85] alleging that Director Tenet and others had violated international legal norms prohibiting arbitrary detention.[86] And finally, he alleged a second Alien Tort Statute claim, stating that defendants had violated international legal norms prohibiting cruel and inhuman or degrading treatment.[87] The government filed a statement of interest in the case, a formal claim of the state secrets privilege, and a motion to intervene in the suit pursuant to Federal Rule of Civil Procedure 24(a), to protect state secrets. The motion to intervene was granted, as settled and controlling authority required.[88] The government also moved for dismissal or for summary judgment on the ground that maintenance of the suit would lead to disclosure of state secrets.

After full briefing and argument, I concluded that the state secrets privilege had been properly invoked and that dismissal was necessary to prevent public disclosure of state secrets. The Fourth Circuit, on appeal,

[80] El-Masri v. Tenet, 437 F. Supp. 2d 530 (E.D. Va. 2006), aff'd sub nom. El-Masri v. United States, 479 F.3d 296 (4th Cir. 2007).

[81] Id. at 532.

[82] Id. at 534.

[83] Bivens v. Six Unknown Named Agents, 403 U.S. 388 (1971).

[84] *El-Masri*, 437 F. Supp. 2d at 534–35.

[85] 28 U.S.C. § 1350 (2006).

[86] *El-Masri*, 437 F. Supp. 2d at 535. In 2004, the Supreme Court held that the Alien Tort Statute, 28 U.S.C. § 1350, merely "furnish[ed] jurisdiction for a relatively modest set of actions alleging violations of the law of nations." Sosa v. Alvarez-Machain, 542 U.S. 692, 720 (2004). In any event, the threshold dismissal of the *El-Masri* case rendered it unnecessary to reach or decide whether his allegations stated valid claims under the Alien Tort Statute.

[87] *El-Masri*, 437 F. Supp. 2d at 535.

[88] Id.

agreed and affirmed the dismissal.[89] But I was not at all pleased with this result, although I felt it was compelled by well-established law. Thus, in dismissing the case, I said the following:

> [I]t is worth noting that putting aside all the legal issues, if El-Masri's allegations are true or essentially true, then all fair-minded people, including those who believe that state secrets must be protected, that this lawsuit cannot proceed, and that renditions are a necessary step to take in this war, must also agree that El-Masri has suffered injuries as a result of our country's mistake and deserves a remedy. Yet, it is also clear from the result reached here that the only sources of that remedy must be the Executive Branch or the Legislative Branch, not the Judicial Branch.[90]

Although I am not certain, I believe that the government did offer El-Masri a settlement on the condition that he remain silent about his experience, an offer it appears he declined. I also note El-Masri recently received a judgment of approximately $78,000 against Macedonia in the European Court of Human Rights.[91]

My remarks on National Security cases were perhaps too long and somewhat tedious and undeserving of the attention you have paid to them, and thus, I especially appreciate your presence and attention. Let me end by noting that I did not address, and did not intend to address, whether National Security cases are more appropriately tried by military commissions, rather than in federal court. That subject is beyond the scope of my remarks.[92] Perhaps it is enough to note that history makes clear that federal courts can and do try National Security cases more or less successfully. But, of course, that does not mean that all National Security cases should be tried in federal courts. Suggestions to the contrary remind me of the advice that an old Navy squadron mate of mine was fond of giving me when I proposed to do something he thought foolish.

---

[89] El-Masri v. United States, 479 F.3d 296, 311 (4th Cir. 2007) (holding that the state secrets privilege applied to the discovery sought by El-Masri and that dismissal was therefore required because the case could not be litigated without the disclosure of state secrets).

[90] *El-Masri*, 437 F. Supp. 2d at 541.

[91] Nicholas Kulish, Court Finds Rights Violation in C.I.A. Rendition Case, N.Y. Times, Dec. 14, 2012, at A12.

[92] For a discussion of forum choice for national security trials, see Aziz Z. Huq, Forum Choice for Terrorism Suspects, 61 Duke L.J. 1415, 1446–48 (2012) (discussing, inter alia, jurisdictional redundancy for national security trials between Article III courts and military commissions).

He said, "Yes, you can spit into the wind if you want to. You can do it. But you may not like the results."

So, you can try any or all National Security cases in federal court, but you may not, in all instances, like the result. There may be some National Security cases that are best tried elsewhere.[93]

Thank you for granting me the honor of addressing this gathering at the University of Virginia School of Law. I will be pleased now to answer your questions.

***

EPILOGUE

Barely three months after this lecture was given, a divided panel of the Court of Appeals for the Fourth Circuit issued opinions in an interlocutory appeal stemming from the Espionage Act prosecution[94] of former CIA agent Jeffrey Sterling, who is accused of illegally disclosing classified information that constituted NDI,[95] about a covert CIA operation pertaining to the Iranian nuclear weapons program to James Risen, a *New York Times* reporter.[96] Because the panel's various opinions address issues related to matters touched on in the course of the lecture, a brief epilogue is warranted.

[93] For an interesting discussion of the mix of motives that led to the use of a military commission to try the World War II Nazi saboteurs (as related in *Ex parte Quirin*, 317 U.S. 1 (1942)), see Michal R. Belknap, The Supreme Court Goes to War: The Meaning and Implications of the Nazi Saboteur Case, 89 Mil. L. Rev. 59, 63–67 (1980). It appears that President Franklin D. Roosevelt ordered the use of a military commission because he favored the imposition of the death penalty and was advised by the Attorney General and others that this could not be done in federal court. It also appears that FBI Director J. Edgar Hoover favored a military commission because its secret proceedings would mask the fact that the saboteurs were discovered not by virtue of the expertise and effort of the FBI, but rather because one of the saboteurs called the FBI and turned himself in. Even so, the FBI considered the saboteur's original call to be a crank call and generally acted incompetently and delayed the capture of the saboteurs. Hoover hoped to prevent this fiasco from becoming public and instead to bask in the glow of the public's mistaken admiration for the FBI's efforts in connection with the saboteurs. See id. at 66–67.

[94] The defendant was prosecuted for violations of the Espionage Act, 18 U.S.C. § 793(d)–(e) (2006).

[95] For a discussion of the legal distinction between NDI and classified information, see supra text accompanying note 77.

[96] United States v. Sterling, No. 11-5028, 2013 WL 3770692 (4th Cir. July 19, 2013).

In *Sterling*, the government appealed three district court interlocutory orders: (i) an order quashing the trial subpoena issued to James Risen; (ii) an order denying the government's motion to withhold from Sterling and the jury the true names and identities of several covert CIA agents and contractors whom the government intended to present to testify at trial; and (iii) an order suppressing the testimony of two government witnesses as a sanction for the government's late disclosure of impeachment material.[97] It is the panel majority's rulings with respect to the first and second orders that bear on matters addressed in the lecture.[98]

First, Chief Judge William Traxler, joined by Judge Albert Diaz, reversed the district court's order quashing the trial subpoena for James Risen, holding that:

> There is no First Amendment testimonial privilege, absolute or qualified, that protects a reporter from being compelled to testify by the prosecution or the defense in criminal proceedings about criminal conduct that the reporter personally witnessed or participated in, absent a showing of bad faith, harassment, or other such non-legitimate motive, even though the reporter promised confidentiality to his source.[99]

The panel also declined to recognize a "qualified, federal common-law reporter's privilege protecting confidential sources."[100]

Although the question of a First Amendment or common law reporter's privilege was not addressed in the lecture, the Fourth Circuit panel's decision in this regard is related to the lecture remarks focusing on whether journalists incur any risk of criminal liability under the Espionage Act by obtaining and disclosing classified information that consti-

[97] Id. at *3–4.

[98] With respect to the district court's order suppressing the testimony of two government witnesses as a sanction for the government's late disclosure of impeachment material, the *Sterling* court held that "although the district court did not abuse its discretion by imposing a sanction, the sanction that it chose to impose was simply too severe a response to conduct that was not undertaken in bad faith . . . ." Id. at *25.

[99] Id. at *5 (citing Branzburg v. Hayes, 408 U.S. 665, 667 (1972)). It is worth noting that a substantially similar claim was raised—and an essentially similar result was reached—in the *Lindh* case. See United States v. Lindh, 210 F. Supp. 2d 780, 784 (E.D. Va. 2002).

[100] Sterling, 2013 WL 3770692, at *11. Judge Gregory dissented, finding a "qualified reporter's privilege in the criminal context" under the First Amendment, and "a common law privilege protecting a reporter's sources pursuant to Federal Rule of Evidence 501." Id. at *38, *43 (Gregory, J., dissenting).

tutes NDI. The hypothetical provided in the lecture was designed to make unmistakably clear that the First Amendment does not license journalists to violate the Espionage Act.[101] A journalist who engages in conduct that meets all of the elements of a Section 793(d) or (e) offense, including the requisite scienter, has no First Amendment shield against criminal liability.

Chief Judge Traxler's majority opinion in *Sterling* now makes clear that a journalist also cannot rely on the First Amendment or a federal common law privilege to resist complying with a subpoena to testify about the facts and circumstances relating to the receipt and disclosure of the classified information that constitutes NDI. Thus, a journalist who, without authorization, seeks, obtains, receives, or discloses classified information that may constitute NDI must weigh carefully not only whether her acts expose her to the risk of criminal liability under the Espionage Act, but also whether she is likely to be compelled to testify. In neither situation is the First Amendment a trump card or a "get out of jail free" card.[102]

[101] Two similar hypotheticals were raised in the discussion immediately following the lecture. Both involved a journalist colluding with a government insider and both point persuasively to the conclusion that the First Amendment is not a license to violate the Espionage Act. In the first hypothetical, the government insider, a D-Day planner, strongly objects to the date and plan chosen for the invasion of Normandy and fears that it will result in a bloodbath. Army leaders disagree and decline to alter the invasion plans. The government insider and a like-minded journalist decide that publishing the D-Day date and invasion location is the only way to prevent the bloodbath. In the second hypothetical, the government insider and like-minded journalist object to the country's plan to assassinate Osama bin Laden and when the government rejects their objection, they decide to publish the time and place of the planned assassination in order to frustrate the government's plan. For further discussion of journalists and the Espionage Act, see, e.g., Sarah Chayes, Journalists Trawling for Leaks Should Be Willing to Share the Risks, Wash. Post (May 31, 2013), http://articles.washingtonpost.com/2013-05-31/opinions/39653041_1_national-security-leaks-npr-reporter-classified-information (arguing that reporters should be "willing to risk repercussions for finding and airing [classified information]"); Emily Bazelon & Eric Posner, Secrets and Scoops, Slate (May 17, 2013, 1:52 P.M.), http://www.slate.com/articles/news_and_politics/im/2013/05/the_government_s_probe_of_the_ap_phone_records_scary_or_justified.html (debating the prosecution of journalists and government leakers).

[102] To be sure, although a journalist receiving such a subpoena cannot invoke a reporter's privilege, she can invoke her Fifth Amendment right to remain silent. The government would then have to consider whether to prosecute the journalist for an Espionage Act violation or instead, to immunize her and therefore compel her testimony on pain of incarceration. See, e.g., In re Grand Jury Subpoena, Judith Miller, 438 F.3d 1141, 1142 (D.C. Cir. 2006) (affirming district court's holding that journalists were in civil contempt of court for refusing to comply with subpoenas).

The *Sterling* panel's opinions on CIPA issues relate more directly to matters raised in the lecture. First, the district court agreed to permit the government to use a screen to conceal the covert agent witnesses' identity from the public seating section of the courtroom, much as the government was allowed to do in the *Lindh* suppression hearing.[103] This ruling was not appealed.[104] Second, Judge Gregory, writing for the majority as to the CIPA issues in *Sterling*, reversed in part and affirmed in part the district court order denying the government's motion to withhold from the jury and Sterling the true names and identities of several covert CIA agents whom the government intends to present at trial. Specifically, all three panel members agreed that the district court should be reversed as to revealing the true names to the jury, explaining that it could "discern no real benefit that would inure from providing the jury with the full, true names of the CIA operatives at issue."[105] Accordingly, because "the true names of the CIA operatives at issue will do nothing to enhance the jury's understanding of the facts and legal issues presented at trial," it "simply is not worth the risk to the lives of these operatives (and their families and associates) to disclose the operatives' true names to anyone who does not have a genuine need to know their identities."[106] Third, a majority of the panel affirmed the district court ruling requiring that the true names of the operatives be revealed to Sterling, explaining that "Sterling knows, or may know, some of the witnesses at issue, and depriving him of the ability to build his defense in this regard could impinge on his Confrontation Clause rights."[107] Chief Judge Traxler dissented on this point. He explained that because "there has been no demonstration that Sterling cannot effectively cross-examine the witnesses without this information," there is no justification for endangering "the personal safety of the witnesses and others associated with them, and jeopardiz[ing] the witnesses' effectiveness as agents and operatives."[108]

The panel's disagreement on this point in *Sterling* illustrates a central fact about national security cases: The involvement of classified information that constitutes NDI in national security cases often requires

[103] See *Sterling*, 2013 WL 3770692, at *26 & n.18.
[104] Id.
[105] Id. at *29; see also id. at *30 (Traxler, C.J., concurring in part and dissenting in part).
[106] Id. at *29 (majority opinion).
[107] Id. at *28.
[108] Id. at *30 (Traxler, C.J., concurring in part and dissenting in part).

courts to strike a delicate balance between the interests in protecting national secrets (including the identity of covert agents) and the rights afforded criminal defendants under the Fifth and Sixth Amendments. The need to strike this balance was important in *Lindh*, *Rosen*, and now *Sterling*, and will continue to be important in all future national security trials. Indeed, it is the need to balance these interests that must play an important role in the government's decision whether to try a national secusecurity case in a federal court or, if permitted, in a military tribunal.

***