

Notes

THE CLASSIFIED INFORMATION PROCEDURES ACT IN THE AGE OF TERRORISM: REMODELING CIPA IN AN OFFENSE-SPECIFIC MANNER

ARJUN CHANDRAN[†]

ABSTRACT

The Classified Information Procedures Act (CIPA) sets the balancing point between the government's interest in preventing disclosure of classified information with a criminal defendant's right to exculpatory material. Although CIPA was originally drafted with espionage cases in mind, the statute has become more commonly associated with terrorism prosecutions. This contextual shift has disrupted CIPA's interest-balancing formulation by altering the governmental interests at stake. CIPA's discovery burdens on the defendant are ordinarily constitutionally justified by the strong countervailing state interest in preserving vital national-security information. This concern is less salient with terrorism defendants, who are unlikely to possess state secrets. Accordingly, those defendants may require further reciprocity in discovery procedures to keep the statute within constitutional parameters. This Note examines the ill effects of CIPA's contextual shift and proposes a set of amendments to alleviate those concerns. Chiefly, this Note suggests an offense-specific CIPA, whereby the procedural mechanisms of the statute are tailored to the offense charged. The three core recommendations of this Note are (1) inclusion of defense counsel in the discovery process and clearer standards to govern discoverability; (2) a limited and qualified declassification requirement in select Foreign Intelligence Surveillance Act cases; and (3) bifurcation of admissibility hearings.

Copyright © 2015 Arjun Chandran.

[†] Duke University School of Law, J.D. expected 2015; Duke University, A.B. 2012. I am grateful to Professor Samuel Buell for his insights and guidance in writing this Note; to Supervisory Assistant Federal Public Defender Daniel Ecarius for his valuable mentorship, which cultivated my interest in this subject; and to my colleagues on the *Duke Law Journal* for their tireless efforts in editing this Note.

INTRODUCTION

The use of classified information in judicial proceedings requires striking a balance between the government's interest in preserving its state secrets and the criminal defendant's right to obtain information necessary to his defense. Over the last three decades, that balancing point has been set by the Classified Information Procedures Act (CIPA).¹ Despite a sharp contextual shift in the statute's use from espionage cases in the Cold War era to terrorism cases post-9/11,² CIPA has remained the standard for governing the introduction of classified information in criminal trials.

This Note examines whether an unamended CIPA is still an appropriate tool in light of this contextual shift, one marked by a climate of government secrecy altogether unfathomable by the framers of the statute in 1980. Though scholars have exhaustively detailed the statute's facial defects,³ the constitutional ramifications of the contextual shift to terrorism cases have been decidedly understudied. Existing scholarship has documented a transition from cases in which a government or military-insider defendant already possesses classified information, to cases in which an outsider defendant comes into possession of classified information only through the government's productions during discovery.⁴ Unfortunately, there is a dearth of literature on how the ill effects of this insider-to-outsider transition should be remedied.

CIPA currently calibrates the balancing point between the competing interests of the state and the defendant by requiring pretrial disclosures of the classified evidence the defense anticipates

1. Classified Information Procedures Act (CIPA), 18 U.S.C. app. III §§ 1–16 (2012).

2. See RICHARD B. ZABEL & JAMES J. BENJAMIN, JR., IN PURSUIT OF JUSTICE: PROSECUTING TERRORISM CASES IN THE FEDERAL COURTS 84–86 (2008), available at http://www.law.yale.edu/documents/pdf/Alumni_Affairs/USLS-pursuit-justice.pdf (documenting the shift toward CIPA's use in terrorism prosecutions).

3. See generally Joshua L. Dratel, *Section 4 of the Classified Information Procedures Act: The Growing Threat to the Adversary Process*, 53 WAYNE L. REV. 1041, 1041–42 (2007) (explaining that CIPA's allowance of ex parte submissions threatens the integrity of the adversarial process); Afsheen John Radsan, *Remodeling the Classified Information Procedures Act (CIPA)*, 32 CARDOZO L. REV. 437, 439 (2010) (asserting that CIPA's secretive procedures clash with norms of transparency in the American justice system); Melanie Reid, *Secrets Behind Secrets: Disclosure of Classified Information Before and During Trial and Why CIPA Should Be Revamped*, 35 SETON HALL LEGIS. J. 272, 274 (2011) (noting that CIPA has been not only misunderstood but also misapplied by federal courts).

4. Ellen Yaroshesky, *Secret Evidence is Slowly Eroding the Adversary System: CIPA and FISA in the Courts*, 34 HOFSTRA L. REV. 1063, 1067 (2005). For a discussion of the insider-outsider distinction, see *infra* Part III.B.

using and judicial determinations on the use, relevance, and admissibility of such evidence. Importantly, its disclosure requirements operate to prevent an artful defendant from threatening to reveal sensitive classified information as leverage to induce the government to drop criminal charges against him. The strong state interests in preserving secrets vital to national security can justify burdens on defendants that would otherwise be impermissibly nonreciprocal.⁵ But in “outsider” cases—those in which the defendant does not possess classified information—these state interests rapidly dissipate. Accordingly, the defendant is left with onerous, nonreciprocal discovery burdens without any countervailing state interest to justify them.

This Note proceeds in four parts. Part I provides a brief history of how courts dealt with classified information before CIPA and identifies the catalysts for its passage. Part II details the relevant provisions of the statute and describes early case law, which continues to inform how courts interpret CIPA. Part III documents the proliferation of terrorism prosecutions and document classification post-9/11 and discusses the under-appreciated constitutional concerns posed by the statute in the twenty-first century. Finally, Part IV proposes a refashioning of CIPA’s core procedures in an offense-specific fashion. If the outsider nature of terrorism defendants reduces governmental interests vis-à-vis espionage prosecutions, then CIPA should be revised to reformulate the procedural rights of the Executive and the criminal defendant to account for these different settings.

Though the primary purpose of this Note is to propose offense-based tailoring of CIPA provisions, it also attempts to set a starting point for future scholarship by drafting sample amendments that would alleviate CIPA’s constitutional defects in outsider cases, while preserving the statute’s vital functions. The first proposal involves inclusion of defense counsel in the discovery process and suggests clearer standards to govern discoverability. The second is a limited and qualified declassification requirement in select cases involving the Foreign Intelligence Surveillance Act (FISA). The final recommendation is the bifurcation of admissibility hearings to prevent CIPA from being used as an offensive weapon.

5. *See* *United States v. North*, 910 F.2d 843, 902 n.41 (D.C. Cir. 1990) (“Discovery proceedings under CIPA . . . may justify an exchange of information between the prosecution and defense that is not entirely reciprocal.”).

I. A BRIEF HISTORY: CIPA'S PROLOGUE AND INFANCY

A. *The History of Classified Information Use in Criminal Trials*

The notion that the Executive may withhold sensitive information concerning national security in a judicial proceeding long predates the passage of CIPA.⁶ In the seminal 1957 case of *Roviaro v. United States*,⁷ the Supreme Court established a test whereby the Executive's interest in withholding national-security information would be balanced against the defendant's right to a fair trial.⁸ Specifically, "where the disclosure of [classified evidence] . . . is relevant and helpful to the defense of an accused, or is essential to a fair determination of a cause, the [executive] privilege must give way."⁹ The Court nonetheless declined to establish a "fixed rule with respect to disclosure,"¹⁰ holding that "[w]hether a proper balance renders nondisclosure erroneous must depend on the particular circumstances of each case, taking into consideration the crime charged, the possible defenses, the possible significance of the informer's testimony, and other relevant factors."¹¹ Apart from these vague instructions, the Court gave little guidance to lower courts on how to balance the competing interests.¹² The unambiguous takeaway from *Roviaro*, however, was that the defendant's right to a fair trial cannot be overridden by executive privilege.¹³

6. See Sandra D. Jordan, *Classified Information and Conflicts in Independent Counsel Prosecutions: Balancing the Scales of Justice After Iran-Contra*, 91 COLUM. L. REV. 1651, 1657–58 (1991) ("The presidential power to classify information in the interests of national security . . . has been exercised as a matter of course during the country's history, without much notice from the legislative or judicial branches.").

7. *Roviaro v. United States*, 353 U.S. 53 (1957).

8. *Id.* at 60–61.

9. *Id.*

10. *Id.* at 62.

11. *Id.*

12. In *United States v. Smith*, 780 F.2d 1102 (4th Cir. 1985), the Fourth Circuit read *Roviaro* as calling "for balancing the public interest in protecting the information against the individual's right to prepare his defense," and observed that "[i]ts application results in a more strict rule of admissibility." *Id.* at 1105.

13. See, e.g., *United States v. Fernandez*, 913 F.2d 148, 154 (4th Cir. 1990) ("[T]he government's interest . . . cannot override the defendant's right to a fair trial."); *United States v. Pitt*, 382 F.2d 322, 325 (4th Cir. 1967) (quoting *Roviaro*, 353 U.S. at 628) (noting that executive privilege is "limited by the 'fundamental requirements of fairness'").

B. The Growing Threat of Graymail and the Impetus for CIPA

Whereas *Roviaro* regulated when the Executive could withhold classified information from the defendant, the government had no recourse if the defendant himself chose to disclose sensitive information from his own knowledge as a stratagem to secure his freedom. This problem, known as “graymail,” occurs when a potential criminal defendant threatens to expose sensitive classified information if he is prosecuted. This creates a “disclose or dismiss” dilemma,¹⁴ whereby “[t]he Government . . . must choose between going forward with the prosecution, thereby compromising the classified material, or safeguarding the material but dropping the prosecution.”¹⁵ Graymail thus creates an irreconcilable conflict between the government’s dual obligations to safeguard national-security secrets and prosecute violators of federal law.¹⁶ Concerned with this phenomenon, Congress passed CIPA in 1980.¹⁷

Unsurprisingly, CIPA’s most prominent cases in the first twenty years after its passage involved espionage.¹⁸ Even after the Cold War ended, CIPA was most famously used in the prosecutions of spies like Brian Regan, Aldrich Ames, and Robert Hanssen.¹⁹ Indeed, this was envisioned as the primary use of CIPA at the time of its passage.

14. S. REP. NO. 96-823, at 3 (1980), *reprinted in* 1980 U.S.C.C.A.N. 4294, 4297.

15. *Graymail Legis.: Hearings Before the Subcomm. on Legis. of the H. Permanent Select Comm. on Intelligence*, 96th Cong., 1st Sess. 1 (1979) [hereinafter *House Hearings*] (statement of Rep. Morgan Murphy, Chairman of the Subcommittee).

16. *Graymail: S. 1482: Hearings Before the S. Comm. on the Judiciary*, 96th Cong., 2d Sess. 13 (1980) [hereinafter *Senate Hearings*] (statement of Philip B. Heymann, Assistant Att’y Gen., Criminal Justice Division).

17. See Timothy J. Shea, *CIPA Under Siege: The Use and Abuse of Classified Information in Criminal Trials*, 27 AM. CRIM. L. REV. 657, 661 (1990). See generally *House Hearings*, *supra* note 15 (noting concerns about graymail when discussing the proposed legislation); *Senate Hearings*, *supra* note 16 (discussing the problems of graymail that prompted the proposed legislation). Chiefly, Congress wished to ensure “that classified information which bears no possible relationship to the issues in a criminal trial is not disclosed” and that *relevant* classified information is identified before trial “so that the Government can make an informed decision in determining whether or not the benefits of prosecution will outweigh the harm stemming from public disclosure of such information.” 126 CONG. REC. 26,503 (1980) (statement of Rep. Romano Mazzoli, floor manager of the bill for the House).

18. For examples, see generally *United States v. Miller*, 874 F.2d 1255 (9th Cir. 1989); *United States v. Zetl*, 835 F.2d 1059 (4th Cir. 1987); *United States v. Walker*, 796 F.2d 43 (4th Cir. 1986); *United States v. Smith*, 780 F.2d 1102 (4th Cir. 1985); *United States v. Lee*, 90 F. Supp. 2d 1324 (D.N.M. 2000); *United States v. Nicholson*, 955 F. Supp. 582 (E.D. Va. 1997); *United States v. Ntube*, No. 93-0322-2(HHG), 1996 WL 808068 (D.D.C. Dec. 9, 1996); *United States v. Lonetree*, 31 M.J. 849 (N-M.C.M.R. 1990).

19. Yaroshefsky, *supra* note 4, at 1068 n.22.

Congress was aware that one of the biggest problems with graymail was that it afforded spies de facto immunity from prosecution, because they tended to possess “military or technological secrets” that could be leveraged.²⁰ Fearful that the public would feel that “there [was] no effective check against improper conduct by members of our intelligence agencies,”²¹ Congress passed CIPA to “help ensure that the intelligence agencies are subject to the rule of law.”²² Although CIPA is a criminal-procedure statute that does not purport to alter the scheme of substantive rights afforded to criminal defendants,²³ its procedural mechanisms were formulated with espionage and the threat of graymail in mind. When prosecutors use CIPA in terrorism cases, outside its drafting context, the governmental interests against disclosure are altered,²⁴ and may or may not justify the level of deference to executive privilege warranted in espionage cases.

The significance of this evolution can be seen by contrasting cases that exemplify the two different eras. In 1983, CIPA was used in the trial of Air Force General Richard Collins to prevent him from revealing “activities of the U.S. government with respect to joint Intelligence/Military operations and the utilization of secret overseas bank accounts to finance said operations.”²⁵ In 2004, the same statute was used to withhold thousands of “non-pertinent” personal telephone conversations from the defendant, Sami Omar Al-Hussayen, a doctoral student at the University of Idaho²⁶ who was the target of extensive electronic surveillance conducted and authorized pursuant to FISA.²⁷ This Note is principally concerned with identifying the changes in the governmental interests accompanying

20. *House Hearings*, *supra* note 15, at 5 (statement of Rep. Morgan Murphy, Chairman of the Subcommittee).

21. *Id.*

22. S. REP. NO. 823, 96th Cong., 2d Sess. 3, *reprinted in* 1980 U.S.C.C.A.N. 4294, 4296 [hereinafter *Senate Report*].

23. 126 CONG. REC. 26,504 (1980) (statement of Rep. Don Edwards) (stating that CIPA is “a lawyer-like response to a series of delicate legal problems. It is primarily a procedural bill. It does not attempt to alter substantive rights”).

24. This difference is chiefly a result of the insider–outsider distinction. *See infra* Part III.B.

25. *United States v. Collins*, 20 F.2d 1195, 1197–98 (11th Cir. 1983).

26. Memorandum in Support of Motion to Declare CIPA Unconstitutional as Applied in this Case at 3–4, *United States v. Al-Hussayen*, No. CR03-048-C-EJL, 2004 U.S. Dist. LEXIS 29793 (D. Idaho Aug. 8, 2004).

27. Government’s Memorandum of Law in Opposition to Defendant’s Motion to Suppress FISA at 2, *Al-Hussayen*, U.S. Dist. LEXIS 29793. For further discussion of CIPA’s interplay with FISA, *see infra* Part II.C.

the shift from insider to outsider CIPA cases and reworking the interest-balancing formulation accordingly.

II. THE MECHANICS OF CIPA

A. Statutory Overview

CIPA “establishes procedures to protect classified information from public disclosure” in the course of a criminal action.²⁸ “Its animating purpose is ‘to harmonize a criminal defendant’s right to obtain and present exculpatory material’”²⁹ with the government’s countervailing interest in “withhold[ing] information from discovery when disclosure would be inimical to national security.”³⁰ In order to protect against harmful disclosures, CIPA allows pretrial determinations on the “use, relevance, or admissibility”³¹ of classified information that the defense “reasonably expects to disclose or cause the disclosure of”³² at trial.

Despite the presence of classified information, CIPA does not change the government’s discovery obligations under Rule 16 of the Federal Rules of Criminal Procedure.³³ If evidence meets the materiality standard of Rule 16(a)(1) and is otherwise discoverable, then “the government’s privilege must give way . . . to [the] criminal defendant’s right to present a meaningful defense.”³⁴ That is to say, “If the evidence is discoverable but the information is privileged, the court must . . . decide whether the information is helpful or material to the defense.”³⁵ Still, upon a sufficient showing, the court may

28. *United States v. Abu Ali*, 528 F.3d 210, 245–46 (4th Cir. 2008).

29. *In re Terrorist Bombings of U.S. Embassies in E. Afr.*, 552 F.3d 93, 115–16 (2d Cir. 2008) (quoting *United States v. Pappas*, 94 F.3d 795, 799 (2d Cir. 1996)).

30. *Id.* at 116 (quoting *United States v. Aref*, 533 F.3d 72, 79 (2d Cir. 2008)).

31. 18 U.S.C. app. III § 6(a) (2012).

32. 18 U.S.C. app. III § 5(a) (2012).

33. *See, e.g., United States v. Yunis (Yunis II)*, 867 F.2d 617, 621–22 (D.C. Cir. 1989) (“This Section creates no new rights of or limits on discovery Rather it contemplates an application of the general law of discovery in criminal cases to the classified information area with limitations imposed based on the sensitive nature of the classified information.”); *see generally* FED. R. CRIM. P. 16 (governing discovery and disclosure obligations in federal criminal proceedings).

34. *In re Terrorist Bombings*, 552 F.3d at 124 (citations and quotation marks omitted).

35. *Id.* A “district court must first decide” whether the evidence is ordinarily discoverable under the general law of discovery. *Id.* (quoting *Aref*, 533 F.3d at 78). “If so, the second step is . . . deciding whether the government has made a facially valid claim of privilege and whether the evidence in question should nevertheless be disclosed as material to the defense.” *United States v. Rezaq*, 156 F.R.D. 514, 516 n.3 (D.D.C. 1994) (citing *Yunis II*, 867 F.2d at 623; *United*

authorize the government to substitute specified articles of classified information with a summary of the information contained therein, or a statement admitting relevant facts.³⁶ This type of request may be made *ex parte*.³⁷ Courts have typically afforded the government a great deal of deference with these requests.³⁸

Before providing the defendant with all discoverable materials, the government may move for a protective order pursuant to Section 3 of CIPA to ensure that classified information furnished by the United States will not be disclosed.³⁹ These protective orders usually require defense counsel to obtain security clearance at the appropriate level of classification, sign a memorandum of understanding, agree to review or discuss classified evidence only in a secure area of review (known as a Secure Compartmented Information Facility, or “SCIF”),⁴⁰ and refrain from discussing the classified information with anyone not included in the order, *including the defendant himself*.⁴¹

If the defendant anticipates disclosing classified information at pretrial or trial proceedings, then he is governed by Sections 5 and 6

States v. Yunis (*Yunis III*), 924 F.2d 1086, 1095 (D.C. Cir. 1991)), *vacated on other grounds*, 899 F. Supp. 697 (D.D.C. 1995).

36. 18 U.S.C. app. III § 4 (2012).

37. *Id.*

38. See Saul M. Pilchen & Benjamin B. Klubes, *Using the Classified Information Procedures Act in Criminal Cases: A Primer for Defense Counsel*, 31 AM. CRIM. L. REV. 191, 198 (1994) (“A stark example of leeway granted to the government . . . can be found in *United States v. Yunis* . . . [where] the court held . . . that the defendant was not entitled to his own tape-recorded statements because they were not ‘helpful to the defense of [the] accused.’”) (footnote omitted) (quoting *Yunis II*, 867 F.2d at 623). This came despite the court recognizing that generally the production of a defendant’s own statements is “‘practically a matter of right even without a showing of materiality.’” *Yunis II*, 867 F.2d at 621–22 (quoting *United States v. Haldeman*, 559 F.2d 31, 74 n.80 (D.C. Cir. 1976) (en banc)).

39. 18 U.S.C. app. III § 3 (2012).

40. A SCIF is an enclosure restricted to noncleared personnel, where Sensitive Compartmented Information (SCI) is viewed. “Designed to withstand eavesdropping, phone tapping and computer hacking,” SCIFs “are protected areas where classified conversations can be held.” Rajini Vaidyanathan, *Barack Obama’s Top Secret Tent*, BBC NEWS (Mar. 22, 2011, 11:44 AM), <http://www.bbc.co.uk/news/world-us-canada-12810675>. SCIFs must be totally soundproof and contain an Intrusion Detection System; entry usually requires “a combination of pin numbers, access badges and biometric data.” *Id.*

41. See, e.g., Protective Order, *United States v. Khan*, No. 11-20331-CR-JORDAN(s), 2012 U.S. Dist. LEXIS 188320, at *14–*15 (S.D. Fla. Nov. 2, 2012) (forbidding the defendant from disclosing classified information). The government tends to suggest the same form language in most of its motions seeking protective orders pursuant to Section 3. Cf. Protective Order (DE 17), *United States v. Foggo*, No. 3:07-cr-00329-LAB (S.D. Cal. Mar. 5, 2007), available at <https://ecf.casd.uscourts.gov>.

of CIPA. Section 5 obligates the defendant to notify the United States and the court of any classified information that he “reasonably expects to disclose or to cause the disclosure of” at trial.⁴² This requirement extends not only to any documents expected to be entered into evidence, or to testimony proffered by the defendant, but also to any information that defense counsel might seek to elicit from witnesses during direct or cross-examination.⁴³ Failure to disclose such information may result in exclusion of that information at trial.⁴⁴ Moreover, the Section 5 notice must *specifically* set out the classified information the defendant will rely on; “[a] general statement of the areas the evidence will cover is insufficient.”⁴⁵

Upon receiving the defendant’s Section 5 notice, the United States may request a hearing for a determination on the “use, relevance, or admissibility” of the classified information listed in the defendant’s notice, pursuant to Section 6.⁴⁶ Such a hearing is held in camera at the request of the Attorney General.⁴⁷ CIPA “does not alter the existing standards for determining relevance or admissibility.”⁴⁸ Thus, courts do not consider whether information is classified when making the admissibility determination; classified information should still be admitted if it is otherwise allowed by the Federal Rules of Evidence.⁴⁹ The government may again move to

42. 18 U.S.C. app. III § 5(a).

43. See Jordan, *supra* note 6, at 1659 (“Section 5(a) is broad . . . ; it includes information that would be revealed in open court, such as testimony from witnesses or arguments of counsel.”).

44. 18 U.S.C. app. III § 5(b).

45. United States v. Smith, 780 F.2d 1102, 1105 (4th Cir. 1985). Similarly, the Eleventh Circuit has stated that it will “not countenance a Section 5(a) notice which allows a defendant to cloak his intentions and leave the government subject to surprise at what may be revealed in the defense.” United States v. Collins, 720 F.2d 1195, 1199–1200 (11th Cir. 1983). CIPA instead “requires that the defendant state, with particularity, which items of classified information . . . will be revealed . . . *Id.* at 1199.

46. 18 U.S.C. app. III § 6(a). If the government wishes to eliminate certain pieces of classified information pursuant to Section 6, it must provide the defendant with notice as to which specific parts of the Section 5(a) disclosure are at issue. *Collins*, 720 F.2d at 1200.

47. 18 U.S.C. app. III § 6(a).

48. 126 CONG. REC. 26,428 (1980). As discussed above, in practice, courts do sometimes impose a heightened standard of materiality in CIPA cases, though without explicit statutory justification. See *supra* note 38; see also United States v. Yunis (*Yunis II*), 867 F.2d 617, 623 (D.C. Cir. 1989) (holding that discovery of classified information requires a further showing that the information will be “helpful” to the defense).

49. United States v. Wilson, 586 F. Supp. 1011, 1013 (S.D.N.Y. 1983), *aff’d*, 750 F.2d 7 (2d Cir. 1984); see also *Collins*, 720 F.2d at 1199 (“[CIPA] does not suggest that simply because defense evidence may consist of classified information it shall be, ipso facto, excluded. Indeed,

substitute that evidence with a summary or an admission of facts.⁵⁰ The court may allow this substitution if it would be “consistent with preserving the accused’s right to make a full defense,” or, “if no alternative suffices, . . . dismiss the indictment or take other measures.”⁵¹ As to any classified information that the court deems admissible at trial, the court must order the United States to provide the defendant with the evidence the government intends to use to rebut his classified information, “unless the interests of fairness do not so require.”⁵²

B. *Judicial Review of CIPA*

The constitutionality of CIPA “has been tested repeatedly and uniformly upheld.”⁵³ In fact, no court has ever invalidated any portion of the statute.⁵⁴ Even so, CIPA continues to attract considerable constitutional scrutiny, as the challenges mounted by defendants have not subsided. Several of the earliest challenges to CIPA have set the tone for how courts interpret the statute today, even though the early courts viewed CIPA through an “insider” lens. This Section examines two Cold War–era opinions that fashioned much of the oft-cited language upholding the constitutionality of CIPA. It then demonstrates how applying those principles to outsider cases has created incongruous results.

1. *The Early Cases.* The highest-profile CIPA cases before the September 11 terrorist attacks were the trials of National Security Advisor John Poindexter and Lieutenant Colonel Oliver North for

CIPA appears premised upon the assumption that, if material to the defense and not otherwise avoidable, such information shall be admissible.”).

50. 18 U.S.C. app. III § 6(a); *see also* Pilchen & Klubes, *supra* note 38, at 206–07 (“If the court accepts the substitution, summary or admission, it in effect alters the documents . . . to follow a script authored by the prosecutor. For defense counsel and the accused, the prosecution’s redrafting of their evidence may be the most unusual and disturbing aspect of the process authorized by CIPA.”).

51. *Wilson*, 586 F. Supp. at 1013; *see also* 18 U.S.C. app. III § 6(c), (d) (providing for an alternative means of disclosure and the sealing of in camera hearings records).

52. 18 U.S.C. app. III § 6(f). “If the government does not comply with its obligations under section 6(f), the court may prohibit both its use of unrevealed classified information and its examination of witnesses with respect to that information.” *United States v. North*, 910 F.2d 843, 899 (D.C. Cir. 1990).

53. *United States v. Hashmi*, 621 F. Supp. 2d 76, 80 (S.D.N.Y. 2008).

54. *United States v. Drake*, 818 F. Supp. 2d 909, 913 n.1 (D. Md. 2011).

their roles in the Iran-Contra Affair.⁵⁵ Both individuals challenged the constitutionality of the statute.⁵⁶ North argued that CIPA's Section 5 notice requirements created unconstitutionally nonreciprocal discovery obligations by compelling him to furnish any classified testimony he anticipated eliciting from defense witnesses to the independent counsel without any reciprocal requirement as to the anticipated testimony of the independent counsel's witnesses.⁵⁷

To support his constitutional challenge, North, like many CIPA defendants after him, relied heavily on the Supreme Court's standard for discovery reciprocity set forth in *Wardius v. Oregon*.⁵⁸ In that case, the Court struck down an Oregon criminal-procedure statute requiring disclosure of alibi defenses with no reciprocal obligation on the state.⁵⁹ The Court declared itself "particularly suspicious" of nonreciprocal trial rules that interfere with a defendant's right to a fair trial.⁶⁰ It noted that "the State's inherent information-gathering advantages suggest that if there is to be any imbalance in discovery rights, it should work in the defendant's favor."⁶¹ The *North* court found the defendant's invocation of *Wardius* to be misplaced, because CIPA cases involve a strong governmental interest that may justify a nonreciprocal exchange of information between the prosecution and defense.⁶² The court suggested that unlike *Wardius*, where no

55. North was indicted on twelve counts relating to selling arms to Iran and providing assistance to the Contras, and was ultimately convicted on only three counts: aiding and abetting an endeavor to obstruct Congress in violation of 18 U.S.C. § 1505; destroying, altering, or removing official National Security Council documents in violation of 18 U.S.C. § 2071; and accepting an illegal gratuity in violation of 18 U.S.C. § 201(c)(1)(B). *North*, 910 F.2d at 851–52. Poindexter was charged with violations of 18 U.S.C. § 371 (conspiracy to make false statements and destroy documents), 18 U.S.C. § 1505 (obstructing and endeavoring to obstruct inquiries by the House of Representatives), and 18 U.S.C. § 1001 (making a false statement to Congress). *United States v. Poindexter*, 725 F. Supp. 13, 18, 24 (D.D.C. 1989).

56. *Poindexter*, 725 F. Supp. at 31; *North*, 910 F.2d at 843.

57. *North*, 901 F.2d at 901–02. North was primarily challenging the district court's implementation of CIPA—namely, its refusal to "order the United States to provide the defendant with the information it expects to use to rebut the classified information" pursuant to § 6(f) of CIPA. *North*, 910 F.2d at 899. The D.C. Circuit found this to be a harmless error, but also seemed dismissive of the notion that the § 6 burdens were nonreciprocal. *See id.* at 903 ("[CIPA] is consistent with the 'salutary' development of 'a system of liberal discovery which gives both parties the maximum possible amount of information . . . and thereby reduces the possibility of surprise at trial.'" (quoting *Wardius v. Oregon*, 412 U.S. 470, 473–74 (1973))).

58. *Wardius v. Oregon*, 412 U.S. 470 (1973).

59. *Id.* at 472.

60. *Id.* at 474 n.6.

61. *Id.* at 475 n.9.

62. *North*, 910 F.2d at 902 n.41 (citing *Wardius*, 412 U.S. at 475).

countervailing state interest existed, in CIPA cases “‘the State’s inherent information-gathering advantages’ are matched by the defendant’s opportunities for engaging in ‘greymail’ to derail legitimate prosecutions.”⁶³

Poindexter’s constitutional challenge to CIPA was more comprehensive. He argued, *inter alia*, that the Section 5 notice requirements violated his federal constitutional rights to remain silent, to testify in his own defense, to cross-examine witnesses against him, and to receive due process of law.⁶⁴ All of these claims were rejected.⁶⁵

Poindexter first construed *Brooks v. Tennessee*⁶⁶ to support the notion that CIPA impermissibly burdened his Fifth Amendment rights to remain silent and to testify in his own defense.⁶⁷ In *Brooks*, the Supreme Court held that a statute requiring a defendant to testify as the first defense witness or not at all was “an impermissible restriction on the defendant’s right against self-incrimination, ‘to remain silent unless he chooses to speak in the unfettered exercise of his own will, and to suffer no penalty . . . for such silence.’”⁶⁸ The statute “exact[ed] a price for [the defendant’s] silence by keeping him off the stand entirely unless he [chose] to testify first.”⁶⁹ Thus, the Court held that the challenged law “cut[] down on the privilege [to remain silent] by making its assertion costly.”⁷⁰ The *Poindexter* court declined to apply *Brooks*, distinguishing CIPA on the basis that the statute does not compel the defendant to reveal “when he will testify, or even whether he will testify.”⁷¹ Rather, all he must do under CIPA is identify the classified information on which he intends to rely.⁷²

63. *Id.* (citations omitted); *see also infra* Part III.B.

64. *United States v. Poindexter*, 725 F. Supp. 13, 31 (D.D.C. 1989).

65. *Id.*

66. *Brooks v. Tennessee*, 406 U.S. 605 (1972).

67. *Poindexter*, 725 F. Supp. at 33.

68. *Brooks*, 406 U.S. at 609 (quoting *Malloy v. Hogan*, 378 U.S. 1, 8 (1964)) (alteration in original).

69. *Id.* at 610.

70. *Id.* at 611 (quoting *Griffin v. California*, 380 U.S. 609, 614 (1965)) (alterations in original).

71. *Poindexter*, 725 F. Supp. at 33.

72. *Id.* The court also noted that the Federal Rules of Criminal Procedure sometimes require defendants to disclose elements of their defense in advance of trial. *Id.* “Examples of such requirements are FED. R. CRIM. P. 12.1 (alibi defense); FED. R. CRIM. P. 12.2 (insanity defense); FED. R. CRIM. P. 12.3 (public-authority defense); FED. R. CRIM. P. 16 (medical and scientific tests, tangible objects, and certain documents).” *Id.* “Provisions requiring the revelation of such defenses in advance of trial have consistently been held to be constitutional.”

The court likewise rejected Poindexter's contention that CIPA violated his Sixth Amendment right to confront the witnesses against him by forcing him to disclose to the prosecution both the classified information that he intended to elicit from prosecution witnesses on cross-examination and all the classified information contained in defense counsel's questions to those witnesses.⁷³ The problem with this argument (in the court's estimation) was that it assumed that defendants enjoy "an unqualified right to undiminished surprise with respect to . . . cross-examination, and that if there is any impairment of the element of surprise, however slight, cross-examination must be regarded as *per se* ineffective."⁷⁴ This assumption, the court warned, misapprehended the role of the Confrontation Clause.⁷⁵

Finally, as to Poindexter's claim that CIPA's disclosure requirements deprived him of due process by imposing a "one-sided burden," the court concluded that "CIPA burdens are not one-sided, but they are carefully balanced, and there is therefore no basis for a due process complaint."⁷⁶ Despite the entirely conclusory nature of the *Poindexter* court's statement that CIPA burdens are "carefully balanced," this language has been heavily cited in subsequent cases. For instance, in *United States v. Ivy*,⁷⁷ a defendant charged with violating the Arms Export Control Act challenged the constitutionality of the notice and hearing requirements of Sections 5 and 6 of CIPA as applied to him.⁷⁸ The Eastern District of Pennsylvania relied on *Poindexter* to deny this challenge in an opinion closely tracking *Poindexter*'s language and organizational structure.⁷⁹ Similarly, in *United States v. Lee*,⁸⁰ the defendant was a

Id. The *Poindexter* court's analysis is weakened somewhat by the fact that the Federal Rules of Criminal Procedure, unlike CIPA, safeguard a defendant's right to pretrial silence by declining to use exclusion of a defendant's testimony as a sanction. See FED. R. CRIM. P. 12.1(e) ("This rule shall not limit the right of the defendant to testify."); FED. R. CRIM. P. 12.3(c) ("This rule does not limit the defendant's right to testify."); FED. R. CRIM. P. 12.2(d) (clarifying that in the case of an undisclosed insanity defense, exclusion of evidence is expressly limited to testimony of expert witnesses).

73. *Poindexter*, 725 F. Supp. at 34 (citation omitted).

74. *Id.*

75. See *id.* ("The Confrontation Clause guarantees an *opportunity* for effective cross-examination, not cross-examination that is effective in whatever way, and to whatever extent, the defense might wish." (quoting *Delaware v. Van Arsdall*, 475 U.S. 673, 679 (1986))).

76. *Id.* at 35 (citation omitted).

77. *United States v. Ivy*, No. 91-00602-04, 1993 WL 316215 (E.D. Pa. Aug. 12, 1993).

78. *Id.* at *1.

79. See *id.* at *1-*7 (relying on *Poindexter* in evaluating Ivy's Fifth and Sixth Amendment claims).

scientist charged with transmitting American nuclear secrets to China. The District Court for the District of New Mexico dismissed his CIPA challenge by relying almost entirely on *Poindexter* and *Ivy*.⁸¹ As a result, a loosely supported conclusion by one district court that CIPA burdens are “carefully balanced”⁸² has snowballed into a voluminous and well-developed body of case law.

2. *The Problematic Application of Poindexter to the Terrorism Context.* Despite the fact that *Poindexter* was decided in 1989 and written while contemplating discovery between the government and a highly sophisticated senior intelligence officer, courts have applied its reasoning to terrorism cases without hesitation. In *United States v. Bin Laden*,⁸³ the Southern District of New York invoked *Poindexter* nearly a dozen times in denying CIPA challenges by three terrorism defendants.⁸⁴ The court found *Poindexter* applicable despite recognizing that the two cases involved disanalogous defendants—John Poindexter was national security advisor, and the classified evidence in that case was equally known to both sides.⁸⁵ Curiously, the *Bin Laden* court even noted that CIPA’s legislative history suggests that it was intended primarily for cases in which the defendant *already* possessed classified information.⁸⁶ Nonetheless, the court did not consider whether shifting contexts might affect the balance of discovery burdens.⁸⁷ Instead, the court concluded that although the facts of *Poindexter* were “significantly different,” the same general

80. *United States v. Lee*, 90 F. Supp. 2d 1324 (D.N.M. 2000).

81. *See id.* at 1327–29 (citing heavily to *Poindexter* and *Ivy* in determining that Sections 5 and 6 of CIPA were not unconstitutional as applied).

82. *United States v. Poindexter*, 725 F. Supp. 13, 35 (D.D.C. 1989).

83. *United States v. Bin Laden*, No. S(7) 98 CR. 1023 LBS, 2001 WL 66393 (S.D.N.Y. Jan. 25, 2001).

84. *Id.* at *1–2, *5–6, *8.

85. *Id.* at *6 n.5. Terrorism defendants, on the other hand, are normally not privy to classified information and cannot access certain evidence against them except through the government.

86. *Id.* at *2.

87. Indeed, the court’s recognition that “the situation presented here is different from the usual CIPA case”—that terrorism defendants do not already possess classified information—was *not* a recognition that terrorism defendants may be uniquely affected by CIPA’s statutory requirements. *See id.* Instead, this issue was raised because “[t]he Government claim[ed] that this difference—the fact that the Defendants have had ‘no prior access to the classified information’—necessitates that the Court continue to prohibit the disclosure of the classified information to the Defendants.” *Id.*

principles applied.⁸⁸ On appeal, the Second Circuit affirmed the district court's decision to deny this as-applied challenge to CIPA.⁸⁹

Perhaps the most notable terrorism case involving CIPA is *United States v. Moussaoui*.⁹⁰ Zacarias Moussaoui, an al-Qaeda member charged with conspiracy to commit international terrorism, was arrested before the 9/11 attacks, but was sentenced afterward, thus “straddl[ing] two eras in American counterterrorism.”⁹¹ Moussaoui's legal challenge to CIPA was unique in that it did not dispute the notice and hearing requirements of Sections 5 and 6, but instead challenged prosecutors' ability to provide written summaries as substitutes for the testimony of potential defense witnesses. Because approximately 75 percent of the indictment concerned the events of September 11th, Moussaoui needed the testimony of several detainees to exonerate himself.⁹² The government offered substitutions for witness testimony pursuant to CIPA, arguing that a strong national-security interest foreclosed granting Moussaoui direct access to detainees.⁹³ The district court rejected the proposed substitution, finding the government's written summaries unreliable and flawed in numerous respects.⁹⁴ The court further found that the defense had made a sufficient showing that the detainees in question could offer testimony that would undermine the government's contention that Moussaoui had participated in 9/11.⁹⁵ Because the United States “deprived Moussaoui of any opportunity to present critical testimony from the detainees at issue in defense of his life,” the court eliminated the death penalty as a possible sentence.⁹⁶ It also prohibited the prosecution from arguing that Moussaoui had any knowledge of or involvement in the 9/11 attacks.⁹⁷

88. *Id.* at *6 n.5.

89. *In re Terrorist Bombings of U.S. Embassies in E. Afr.*, 552 F.3d 93, 156 (2d Cir. 2008).

90. *United States v. Moussaoui*, 382 F.3d 453 (4th Cir. 2004).

91. Radsan, *supra* note 3, at 439.

92. *United States v. Moussaoui*, 282 F. Supp. 2d 480, 482–83 (E.D. Va. 2003), *aff'd in part, vacated in part, remanded*, 365 F.3d 292 (4th Cir. 2004), *opinion amended on reh'g*, 382 F.3d 453 (4th Cir. 2004), *aff'd in part, vacated in part, remanded*, 382 F.3d 453 (4th Cir. 2004).

93. *Moussaoui*, 382 F.3d at 458 n.5.

94. *Id.* at 459.

95. *Moussaoui*, 282 F. Supp. 2d at 486.

96. *Id.* at 487.

97. *Id.* These sanctions were necessary because the government made clear that it would not produce witnesses for deposition despite the district court's finding that testimony from such witnesses could be material to Moussaoui's defense. *Moussaoui*, 382 F.3d at 476. “Although dismissal is the presumptive sanction contemplated by CIPA when a defendant is prevented

On appeal, the Fourth Circuit vacated the lower court's ruling in part, acknowledging that Moussaoui had a Sixth Amendment right to cross-examine the detainees, but rejecting the argument that written substitutions would be "inherently inadequate."⁹⁸ The court remanded for a reformulation of the substitutions in an acceptable manner, instructing that the "compiling of substitutions be an interactive process among the parties and the district court," that the substitutions use the exact language of the government's written summaries, and that the government refrain from creating substitutions "larded with inculpatory information under the guise of [the rule of] completeness."⁹⁹ The court further ordered that substitutions be admitted only by Moussaoui, and that the trial court retain full discretion to determine admissibility.¹⁰⁰

The Fourth Circuit's decision in *Moussaoui*—that CIPA's procedures for written substitutions of witness testimony can adequately preserve a defendant's Sixth Amendment rights—has come under criticism.¹⁰¹ Notably, implicit in the Fourth Circuit's decision is the assumption that "the import of [the Sixth Amendment cross-examination] right" lies in "the *content* of the evidence," which disregards "the importance of the form of presentation."¹⁰² It is difficult to imagine how a written summary could achieve the same benefits as the live presence of a witness, which allows a jury to directly hear cross-examination and "take measure of the demeanor and appearance of the witness."¹⁰³ Nonetheless, as of yet, no court has rejected *Moussaoui*'s Sixth Amendment holding.

C. CIPA's Interplay with FISA

CIPA is very frequently invoked in cases involving the Foreign Intelligence Surveillance Act, because FISA-generated materials are

from disclosing classified information found to be material and favorable," *Moussaoui*, 282 F. Supp. 2d at 482–83, the district court believed "that a more measured approach [was] required." *Moussaoui*, 382 F.3d at 476.

98. *Moussaoui*, 382 F.3d at 478.

99. *Id.* at 479–81.

100. *Id.*

101. See, e.g., Brian McEvoy, Note, *Classified Evidence and the Confrontation Clause: Correcting a Misapplication of the Classified Information Procedures Act*, 23 B.U. INT'L L.J. 395, 414–20 (2005).

102. *Id.* at 414 (emphasis added).

103. *Id.* at 417.

initially classified.¹⁰⁴ Indeed, FISA is used in 61 percent of national-security or terrorism-associated prosecutions involving CIPA.¹⁰⁵ As a result, to properly analyze CIPA, it is important to gain a basic understanding of FISA and its implications.¹⁰⁶

FISA¹⁰⁷ was enacted in 1978 to establish procedures that the government must follow when conducting electronic surveillance for foreign-intelligence purposes within the United States.¹⁰⁸ To authorize such surveillance, FISA established the Foreign Intelligence Surveillance Court (FISC).¹⁰⁹ A FISC judge may approve the use of electronic surveillance to obtain foreign intelligence if there is probable cause to believe that the proposed target of electronic surveillance is a “foreign power or an agent of a foreign power.”¹¹⁰ The Foreign Intelligence Surveillance Court of Review (FISCR) has the authority to review the denial of any application under FISA.¹¹¹ Such denials, though, are exceedingly rare—for the first twenty-four years of the court’s existence, no application was ever denied, and the first ever review (in 2002) was of an application that was merely modified.¹¹² Although recently a few applications have been denied or withdrawn every year, the approval rate has not even come close to dipping below 99 percent in any year.¹¹³ In practice, then, the FISC serves as little more than a rubber stamp for government surveillance.¹¹⁴

104. CTR. ON LAW & SEC., N.Y. UNIV. SCH. OF LAW, TERRORIST TRIAL REPORT CARD: SEPTEMBER 11, 2001-SEPTEMBER 11, 2009, at 27 (2010) [hereinafter *2009 Terrorist Trial Report Card*], available at http://www.lawandsecurity.org/Portals/0/documents/02_TTRCFinalJan142.pdf.

105. *See id.* (percentage calculated from underlying data).

106. *See generally* Joshua L. Dratel, *Ethical Issues in Defending a Terrorism Case: How Secrecy and Security Impair the Defense of a Terrorism Case*, 2 CARDOZO PUB. L. POL’Y & ETHICS J. 81 (2003) (providing background on CIPA’s interplay with FISA).

107. 50 U.S.C. § 1881a (2012).

108. Keith G. Logan, *Foreign Intelligence Surveillance Act*, in 1 BATTLEGROUND CRIMINAL JUSTICE 287 (Gregg Barak ed., 2007).

109. 50 U.S.C. § 1881a.

110. 50 U.S.C. § 1805(a)(3); *In re Sealed Case*, 310 F.3d 717, 722 (Foreign Int. Surv. Ct. Rev. 2002). The term “foreign power” includes, *inter alia*, “a group engaged in international terrorism or activities in preparation therefor.” 50 U.S.C. § 1801(a)(4).

111. 50 U.S.C. § 1803(b).

112. *See In re Sealed Case*, 310 F.3d at 719 (noting that this was the first appeal since the passage of FISA).

113. *See* Logan, *supra* note 108, at 292. The approval rate hit an all-time low of 99.7 percent in 2003. *Id.*

114. *See* *Clapper v. Amnesty Int’l USA*, 133 S. Ct. 1138, 1159 (2013) (Breyer, J., dissenting) (“[T]o exercise this capacity [to surveil] the Government must have intelligence court

The government's applications submitted to the FISC are classified, as are the overwhelming majority of the court's orders.¹¹⁵ As a result, when the government prosecutes a suspected terrorist after conducting electronic surveillance, all FISA intercepts—which comprise the majority of evidence in the case—will be classified. Thus, CIPA and its procedures are implicated in such prosecutions.¹¹⁶

III. CIPA AND TERRORISM: A NEW CONSTITUTIONAL CONCERN

The events of September 11, 2001 had a profound effect on federal prosecutorial priorities. Indeed, in the decade following 9/11, the Department of Justice indicted more than one thousand defendants in terrorism prosecutions.¹¹⁷ This trend has shown no signs of subsiding, as the number of jihadist-related terrorism prosecutions doubled in 2009 and 2010.¹¹⁸ Significantly, 23 percent of terrorism prosecutions since 9/11 have involved CIPA.¹¹⁹ This Section explores the constitutional concerns raised by CIPA when it is used in the terrorism context, and how this shift has fundamentally altered the balance of interests originally thought to justify the statute's more restrictive provisions. This Part first documents how the problem of overclassification, coupled with the type of classified information in CIPA cases, makes the statute's application in the terrorism context far more problematic than in the typical espionage case. It then details how the governmental interests weighing against defendants' procedural rights have waned significantly as the government has

authorization. But the Government rarely files requests that fail to meet the statutory criteria.”).

115. See *In re* Motion For Release of Court Records, No. Misc. 07-01 at *6 (FISA Ct. Dec. 7, 2011), available at https://www.aclu.org/sites/default/files/pdfs/safefree/fisc_order_2007_1211.pdf (holding that there is no public right of access to FISC records).

116. See, e.g., Motion for Order Declaring the Classified Information Procedures Act Unconstitutional (DE 111) at 3, *United States v. Qazi*, No. 12-6098, (S.D. Fla. July 8, 2013), available at <https://ecf.flsd.uscourts.gov> (explaining how the use of FISA prompted classification of discovery materials and the application of CIPA).

117. See CTR. ON LAW & SEC., N.Y. UNIV. SCH. OF LAW, TERRORIST TRIAL REPORT CARD: SEPTEMBER 11, 2001-SEPTEMBER 11, 2011, at 7 n.2 (2011) [hereinafter *2011 Terrorist Trial Report Card*], available at <http://www.lawandsecurity.org/Portals/0/Documents/TTRC%20Ten%20Year%20Issue.pdf>. This number includes 578 defendants who were “formally or informally associated with an Islamist terror group—whether one with a global jihadist ideology (i.e. Al Qaeda), or a local Islamist movement (i.e. Hamas).” *Id.* at 7 n.1. The remaining five-hundred-plus terrorism prosecutions involve terror cases without an identifiable link to jihadist crimes. *Id.* at 7 n.2.

118. *Id.* at 2.

119. *Id.* at 13.

prosecuted fewer insiders and more outsiders in CIPA cases. As a result, CIPA may now be unconstitutional as applied in terrorism prosecutions, particularly due to problems of nonreciprocal discovery obligations and ineffective assistance of counsel.

A. *The Proliferation of the Executive Classification Privilege and the Role of Classified Information in Terrorism Trials*

A phenomenon that has made CIPA's use more problematic in the last decade (especially in relation to terrorism cases) is the explosion of document-classification decisions.¹²⁰ The number of classified documents doubled in the decade from 1997–2007, with 14.2 million documents classified in 2005 alone.¹²¹ “That’s 39,000 a day, or 1,600 every hour of the night and day.”¹²²

The questionable nature of these classification decisions is well documented.¹²³ When members of the public petition agencies to review documents for declassification (through a process known as mandatory declassification review), those documents are declassified 92 percent of the time.¹²⁴ Former National Security Council Executive Secretary Rodney McDaniel estimated that only 10 percent of classification decisions were actually made for “legitimate protection of secrets.”¹²⁵ Nonetheless, four out of five documents classified in 2005 were designated “Secret” or “Top Secret.”¹²⁶ Information is classified at this level when its disclosure could reasonably be expected to threaten national security.¹²⁷ The absurdity of some classification decisions is illustrated by a memo from a member of the

120. For background on overclassification, see generally TED GUP, *NATION OF SECRETS: THE THREAT TO DEMOCRACY AND THE AMERICAN WAY OF LIFE* 98–130 (2007); Alex Rossmiller, *Adjudicating Classified Information*, 85 ST. JOHN'S L. REV. 1275, 1293–97 (2011); William G. Weaver & Robert M. Pallito, *State Secrets and Executive Power*, 120 POL. SCI. Q. 85 (2005).

121. GUP, *supra* note 120, at 8.

122. *Id.*

123. Weaver & Pallito, *supra* note 120, at 87 (“Virtually all observers acknowledge that overclassification is a significant problem . . .”).

124. See INFO. SEC. OVERSIGHT OFFICE, 2010 REPORT TO THE PRESIDENT 20 (2011) (“As a result of initial MDR processing, only 285,418 pages (8 percent) remained classified in their entirety after an initial MDR review.”).

125. COMM'N ON PROTECTING AND REDUCING GOV'T SECRECY, REPORT OF THE COMMISSION ON PROTECTING AND REDUCING GOVERNMENT SECRECY, S. Doc. No. 105-2, at 36 (1997).

126. GUP, *supra* note 120, at 8.

127. *Id.*

Joint Chiefs of Staff claiming that too many documents were being classified, which was in turn classified itself.¹²⁸

In CIPA cases, evidence is often classified because it is derived from FISA surveillance,¹²⁹ meaning that access to evidence is restricted because of how the government acquired it. As one defendant argued in the Southern District of Florida,

Many sections of the [Government's] proposed order are written so broadly as to potentially encompass Mr. Khan's own words either telephonically or in written form . . . Paragraph 4(B) of the proposed protective order . . . defines what is "classified information." It includes documents that were "*once in the possession of a private party, which has been derived from a United States Government classified document*, information, or material, regardless of whether such document, information, or material has itself subsequently been classified by the Government pursuant to Executive Order 12958 or its predecessor orders as "CONFIDENTIAL" or "SECRET."¹³⁰

Thus, the classified information at issue in CIPA hearings may be derived from the defendant's own speech, which the defendant consequently cannot use as evidence without the United States' permission.¹³¹ This leads to the strange result, as detailed above, that a defendant's own phone calls, emails, internet searches, or social-media messages may be subject to CIPA's Section 5 notice

128. H.R. REP. NO. 92-1633, pt. 1, at 20 (1973). Other instances include the classification of a 2006 cable from a U.S. diplomat describing a wedding he attended in Dagestan:

The paragraph describing a typical Dagestani wedding was classified as 'Confidential,' meaning that its release '*reasonably could be expected to cause damage to the national security*.' The paragraph included the following classified observations: 'Dagestani weddings . . . take place in discrete parts over three days. On the first day the groom's family and the bride's family simultaneously hold separate receptions. . . . The next day, the groom's parents hold another reception, this time for the bride's family and friends, who can 'inspect' the family they have given their daughter to. On the third day, the bride's family holds a reception for the groom's parents and family.'

Elizabeth Goitein & David M. Shapiro, Brennan Ctr. for Justice, Reducing Overclassification Through Accountability 6 (2011) (emphasis added), *available at* <http://www.brennancenter.org/publication/reducing-overclassification-through-accountability>.

129. *See supra* Part II.C.

130. Defendant Hafiz Muhammad Sher Ali Khan's Response to Government's Motion for Protective Order on CIPA Materials at 3 (DE 101), *United States v. Khan* (S.D. Fla. Aug. 30, 2011) (No. 11-20331) (emphasis added), *available at* <https://ecf.flsd.uscourts.gov>.

131. *Id.* at 2.

requirement because they were obtained or derived from FISA surveillance.¹³²

CIPA may be just a procedural statute, but the informational asymmetry it creates—magnified by the nature and volume of classified information in terrorism cases—confers a rather significant advantage upon prosecutors. So although CIPA may very well be neutral on paper, it could certainly “be used instrumentally in an advocacy context”¹³³ to stack the deck against a defendant.

B. The Balance of Interests in Terrorism Prosecutions

CIPA’s constitutionality has long been settled.¹³⁴ Nevertheless, as discussed above, the climate of overclassification¹³⁵ and the nature of evidence in terrorism prosecutions have substantially increased the burden CIPA imposes on outsider defendants. CIPA has been used in more than 140 terrorism cases since 9/11.¹³⁶ Accordingly, an examination of the constitutional ramifications of this contextual shift is necessary. This Section expounds on the nature of CIPA’s contextual shift and the diminution of the governmental interests that

132. An example of this problem is illustrated by the predicament of defense counsel in *United States v. Khan*: “Based upon the indictment the bulk of the ‘classified’ information will be Mr. Khan’s own words as he speaks on the phone overseas . . . [and] could include acquaintances of Mr. Khan or methods of communication such as email, text, social media, or faxes.” Motion to Strike Use of CIPA as Unconstitutional at 6, *United States v. Khan* (S.D. Fla. Aug. 30, 2011) (No. 11-20331). In *United States v. Al-Hussayen*, No. CR03-048-C-EJL, 2004 U.S. Dist. LEXIS 29793 (D. Idaho Apr. 6, 2004), the classified information at issue spanned eighty-nine CDs in Arabic, consisting of Al-Hussayen’s own emails and telephone conversations. In *United States v. Al-Arian*, 267 F. Supp. 2d 1258, 1260 (M.D. Fla. 2003), the government refused to declassify twenty-one thousand hours of the defendant’s own communications. For more background on the government’s tactical classification of FISA intercepts, see Joshua L. Dratel, *Symposium: Secret Evidence and the Courts in the Age of National Security: Sword or Shield? The Government’s Selective Use of its Declassification Authority for Tactical Advantage in Criminal Prosecutions*, 5 CARDOZO PUB. L. POL’Y & ETHICS J. 171, 175 (2006).

133. Pilchen & Klubes, *supra* note 38, at 194.

134. See *United States v. Poindexter*, 725 F. Supp. 13, 32 (D.D.C. 1989) (“Every court that has passed on the constitutionality of CIPA has upheld it.”).

135. The overclassification problem worsened in the wake of 9/11. According to the 2007 testimony of Mark Agrast, later Deputy Assistant Attorney General and current executive director of the American Society of International Law, “there were nearly three times as many classification actions in 2004 as in the last year of the Clinton presidency,” and “while Clinton declassified nearly a billion pages of historical material, the pace has slowed to a trickle in the last six years.” *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. 94 (2007) (testimony of Mark D. Agrast, Senior Fellow, Ctr. for Am. Progress).

136. 2009 *Terrorist Trial Report Card*, *supra* note 104, at 27.

previously justified more onerous burdens on defendants. This Section also presents two ways in which outsider prosecutions implicating CIPA may run afoul of the Constitution. Part III.B.1 argues that CIPA could violate outsider defendants' due-process rights by imposing nonreciprocal discovery burdens in the absence of a sufficiently strong governmental interest. Part III.B.2 contends that CIPA could similarly erode an outsider defendant's right to the effective assistance of counsel.

The crux of the contextual shift is that CIPA has transitioned from typically insider cases to outsider ones.¹³⁷ In insider cases, the defendants (government officials or intelligence operatives) "previously had access to the classified information and the access to the classified information was for work-related conduct."¹³⁸ On the other hand, in outsider cases—typically relating to terrorism or international drug conspiracies—the defendants "never had and never will have access to the material."¹³⁹ In this latter category of cases, the defendants are not capable of "graymailing," as they "cannot reveal classified information other than that provided in discovery."¹⁴⁰ Indeed, the type of evidence at issue in CIPA cases today rarely concerns the vital state secrets that graymailers threatened to expose in CIPA's infancy.

The most significant constitutional implication of this transition from insider to outsider cases is that it fundamentally alters the governmental interests that weigh against criminal defendants' rights. This shift bolsters the recurring argument made by defendants that CIPA violates their right to due process by imposing nonreciprocal discovery obligations. As the D.C. Circuit explained in *United States v. North*,¹⁴¹ "CIPA was specifically designed to minimize the need to forego prosecution[s] . . . in order to avoid compromising national security information," and this strong state interest may justify

137. Yaroshefsky, *supra* note 4, at 1067.

138. *Id.* "In such cases, the government typically produces all the classified information to security-cleared defense counsel and the defendant, *who himself has security clearance* for access to the classified documents, reviews the evidence with his lawyer." *Id.* at 1067–68 (emphasis added). Accordingly, CIPA balances the competing interests effectively in insider cases by affording the defendant "basic Fifth and Sixth Amendment rights, while preserving the government's national security concerns." *Id.* at 1068.

139. *Id.*

140. *Id.*

141. *United States v. North*, 910 F.2d 843 (D.C. Cir. 1990).

nonreciprocal discovery obligations.¹⁴² This concern, if not entirely ameliorated in terrorism prosecutions, is hardly as compelling as it once was. It is a rare terrorism defendant who possesses sensitive national-security information.

As for classified information that the government possesses, it is important to remember that the purpose of CIPA was *not* to allow the government to persist in prosecutions when it is disinclined to disclose exculpatory information that threatens national security. Instead, Congress wished to ensure that classified information “*which bears no possible relationship to the issues in a criminal trial is not disclosed,*” and that relevant classified information is identified before revelation so that the “Government *can make an informed decision*” on whether prosecuting is worth the risk of public disclosure.¹⁴³

In terrorism cases, because only the government possesses the classified information from the start, it may reach “an informed decision” on the benefits of prosecution before disclosing sensitive information to the defendant. If the government wanted to avail itself of other protections afforded by CIPA (such as the ability to request a substitution of a classified document with a summary), it could certainly do so without requiring the defendant to provide a roadmap of the defense under Section 5. If the government itself possessed discoverable exculpatory information, the disclosure of which could threaten national security, it is hard to imagine that it would need the *defendant* to identify that issue. Such a scenario could be easily resolved before the defense is even privy to such information, through an *ex parte* Section 4 hearing to “delete specified items of classified information from documents to be made available to the defendant through discovery under the Federal Rules of Criminal Procedure.”¹⁴⁴ If the trial court ruled that such information *was* discoverable after a Section 4 hearing, the government would not need the defendant to disclose his defense before it sought to substitute that information with a written summary.

In *Wardius v. Oregon*, the Supreme Court noted that “the State’s inherent information-gathering advantages suggest that if there is to be any imbalance in discovery rights, it should work in the

142. *Id.* at 902 n.41 (quotations omitted).

143. 126 CONG. REC. 26,503 (1980) (statement of Rep. Romano Mazzoli, floor manager of the bill for the House) (emphasis added).

144. 18 U.S.C. app. III § 4 (2012).

defendant's favor."¹⁴⁵ Responding to the applicability of *Wardius*, the *North* court observed that "the State's inherent information gathering advantages are matched by the defendant's opportunities for engaging in 'greymail' to derail legitimate prosecutions."¹⁴⁶ This sensible reasoning, which assured the rejection of first-generation CIPA challenges, has little relevance to today's outsider cases. Even in the very rare instances when discovery provides a terrorism defendant with graymail material, the government cannot exclude relevant defense information anyway.¹⁴⁷ Thus, the prospect of graymail could hardly be deemed a defense advantage sufficient to justify nonreciprocal discovery burdens as *North* suggests—it is a consequence of the Federal Rules of Criminal Procedure, which apply in every federal criminal action.¹⁴⁸

Further, given that a defendant can use only that classified information that is relevant and helpful to his defense, using such information hardly constitutes "engaging in 'greymail' to derail legitimate prosecutions."¹⁴⁹ When the government gives a defendant a classified document that the Federal Rules entitle him to deploy in furtherance of his defense, it is of little consequence that the government would prefer it remain undisclosed to the public. CIPA was never intended to prevent disclosure when the information is necessary to the defense. Certainly, this scenario is incomparable to insider cases, in which intelligence officers or government employees actively threaten to expose immaterial state secrets from their own knowledge.

CIPA was *not* designed to relieve the government from deciding whether to prosecute or avoid disclosure; on the contrary, it was designed to facilitate that decision by ensuring open information.¹⁵⁰

145. *Wardius v. Oregon*, 412 U.S. 470, 475 n.9 (1973).

146. *North*, 910 F.2d at 902 n.41 (quotation omitted).

147. Because CIPA does not change the standards for admissibility or discoverability, the government cannot withhold exculpatory information merely because it would threaten national security. *See, e.g.*, *United States v. Yunis (Yunis II)*, 867 F.2d 617, 621–22 (D.C. Cir. 1989) ("This Section creates no new rights of or limits on discovery of a specific area of classified information."); 126 CONG. REC. H9308 (1980) (statement of Rep. Romano Mazzoli, floor manager of the bill for the House) (explaining that CIPA "does not alter the existing standards for determining relevance or admissibility").

148. FED. R. CRIM. P. 16 (governing discovery and disclosure obligations in criminal proceedings).

149. *North*, 910 F.2d at 902 n.41.

150. *See House Hearings, supra* note 15, at 2 (stating that the proposed legislation was "designed to eliminate the guesswork, surprise and fear" from deciding whether to prosecute).

When the government already possesses the information, the defendant's Section 5 notice should have no bearing on the government's "informed decision" to prosecute. The government is already as "informed" as it will be after such notice.

1. *Nonreciprocal Discovery Obligations.* As detailed extensively above, the countervailing governmental interests that exist in espionage cases are rarely present in terrorism prosecutions.¹⁵¹ Thus, if the discovery burdens imposed by CIPA are not reciprocal, the statute may be susceptible to as-applied constitutional challenges in the prosecution of outsiders. Indeed, the Supreme Court is "particularly suspicious" of "trial rules which provide nonreciprocal benefits to the [government] when the lack of reciprocity interferes with the defendant's ability to secure a fair trial."¹⁵²

The *Poindexter* court declared that CIPA burdens are "not one-sided," but are instead "carefully balanced."¹⁵³ This is because under CIPA, when a defendant provides Section 5 notice of the classified information he intends to disclose or cause disclosure of at trial, the trial court must order the prosecution to provide the defendant with the information it expects to use to rebut his classified information.¹⁵⁴ Indeed, "It is crystal clear, then, that disclosure provisions of CIPA would be unconstitutional if the reciprocity section were not part of the Act."¹⁵⁵

Still, defendants have argued that CIPA's reciprocity provisions are constitutionally inadequate. As National Security Agency (NSA) whistleblower Thomas Drake argued in his trial, the notice requirements of Sections 5 and 6 violate the Due Process Clause of the Fifth Amendment by "imposing ill-defined, one-sided notice and hearing obligations on the defense that do nothing to enhance the accuracy of the fact-finding process."¹⁵⁶ Drake further argued that the reciprocity provision is functionally nonreciprocal for two reasons.

151. Other countervailing governmental interests that may be implicated in these cases are discussed at the end of this Subsection.

152. *Wardius v. Oregon*, 412 U.S. 470, 474 n.6 (1973).

153. *United States v. Poindexter*, 725 F. Supp. 13, 35 (D.D.C. 1989).

154. 18 U.S.C. app. III § 6(f) (2012).

155. *United States v. North*, 910 F.2d 843, 936 (D.C. Cir. 1990) (Wald, C.J., dissenting).

156. Motion for a Declaration that Sections 5 and 6 of the Classified Information Procedures Act Are Unconstitutional at 14, *United States v. Drake*, 818 F. Supp. 2d 909 (D. Md. 2011) (No. 1:10-cr-0181-RDB) [hereinafter *CIPA Motion*].

First, the “government controls the scope of a defendant’s notice obligation under CIPA through its power to decide what information will be classified.”¹⁵⁷ Because neither defendants nor courts can challenge such classifications,¹⁵⁸ the government may effectively exercise “significant control over the extent to which the defense will be compelled to disclose and explain its case” through its classification decisions.¹⁵⁹ “The more information that the government classifies, the greater the defendant’s notice-and-hearing obligations under CIPA.”¹⁶⁰

Second, Drake pointed out that the decision to convene a Section 6(a) pretrial hearing on the use, relevance, or admissibility of classified information is entirely within the prosecution’s discretion. Moreover, Section 6(f)’s reciprocity provision is limited by the fact that the government may identify the specific classified information at issue in a Section 6 hearing.¹⁶¹ Drake explained:

*If the prosecution, in its sole discretion, chooses to request a hearing as to some or all of the classified information listed in the defendant’s § 5(a) notice, and if at the hearing (following the defendant’s explanation) the court determines that some portion of the listed information is relevant and admissible at trial, then as to that information only “the court shall . . . order the United States to provide the defendant with the information it expects to use to rebut the classified information.”*¹⁶²

Thus, Drake argued, the prosecution may reap the benefits of a defendant’s Section 5 notice, “hearing many details of his case” and excluding parts of that disclosure from the Section 6 hearing, thereby limiting the government’s reciprocal discovery obligations.¹⁶³ As another defendant similarly argued, CIPA imposes a one-sided

157. *Id.*

158. *United States v. Smith*, 750 F.2d 1215, 1217 (4th Cir. 1984) (“[D]efendants cannot challenge this classification. A court cannot question it.”), *rev’d on other grounds*, 780 F.2d 1102 (4th Cir. 1985).

159. *CIPA Motion*, *supra* note 156, at 15–16.

160. *Id.*; *see also* *Dratel*, *supra* note 132, at 173 (“Unfettered government discretion . . . permits the government to use its unreviewable classification authority as an offensive weapon, effectively placing voluminous amounts of critical evidence off limits to the defense.”); *United States v. George*, No. 91-0521, 1992 U.S. Dist. LEXIS 9632, at *2 (D.D.C. June 24, 1992) (“[T]he CIPA process is strangely one-sided; the government may declassify any information it wishes, for whatever reason, if it suits the needs of the prosecution.”).

161. 18 U.S.C. app. III § 6(b)(1) (2012).

162. *CIPA Motion*, *supra* note 156, at 15.

163. *Id.* at 16.

burden on the defendant because notwithstanding the reciprocity requirement, “the amount (if any) of disclosed rebuttal information is entirely within the control of his adversary.”¹⁶⁴

Curiously, neither the government in its Response, nor the district court in its Order, addressed either of Drake’s arguments in responding to his reciprocity challenge.¹⁶⁵ Perhaps the most noticeable defect of the “reciprocal” burdens of CIPA in outsider cases is that the government already possesses the classified information that would be presented in a defendant’s Section 5 notice. Because FISA is used in nearly 60 percent of terrorism-associated prosecutions involving CIPA,¹⁶⁶ the classified documents that a defendant will have access to at trial are usually his own communications contained in FISA intercepts. The government will have reviewed this information long before the defendant ever has access to it, but a defendant must still “specifically set out the classified information [he] believes he will rely upon in his defense,”¹⁶⁷ and counsel must explain her theories of the anticipated use and relevance of that information.¹⁶⁸ Thus, CIPA effectively allows the government to elicit defense counsel’s theory of the case under the pretense of preventing the “government [from being] subject to surprise at what may be revealed in the defense,”¹⁶⁹

164. Motion for Order Declaring the Classified Information Procedures Act Unconstitutional (DE 111) at 7, *United States v. Qazi*, No. 12-6098 (S.D. Fla. July 8, 2013).

165. See *United States’ Response to Defendant’s Motion for a Declaration that Sections 5 and 6 of CIPA are Unconstitutional as Applied at 1*, *United States v. Drake*, 818 F. Supp. 2d 909 (D. Md. 2011) (No. 1:10-cr-00181-RDB); *Drake*, 818 F. Supp. 2d at 914–15. Instead, the court simply used generic language that seemed to respond more to arguments raised by the defendants in *United States v. Ivy*, No. Crim. A. 91-00602-04, 1993 WL 316215, at *2 (E.D. Pa. Aug. 12, 1993), and *United States v. Wilson*, 721 F.2d 967, 976 (4th Cir. 1983), than by Thomas Drake. Noting that *Wardius* condemned only those procedures wherein the overall balance of discovery burdens tipped against the defendant, the court concluded that CIPA’s burdens were “carefully balanced,” reasoning that “[CIPA] authorizes this Court to impose upon the Government a continuing duty to disclose rebuttal evidence or have such evidence excluded . . . [T]he Government must also comply with the Federal Rules of Criminal Procedure and *Brady v. Maryland*.” *Drake*, 818 F. Supp. 2d at 915 (citations omitted). The court failed to acknowledge Drake’s arguments that CIPA’s burdens are nonreciprocal because the government controls the defendant’s notice requirements through its power to classify, and because it can manipulate its reciprocal discovery obligations through its unbridled discretion in requesting a Section 6 hearing. See *id.* at 914–15.

166. Percentage calculated from data compiled in *2009 Terrorist Trial Report Card*, *supra* note 104.

167. *United States v. Smith*, 780 F.2d 1102, 1105 (4th Cir. 1985).

168. 18 U.S.C. app. III § 6(a) (2012).

169. *United States v. Collins*, 720 F.2d 1195, 1199 (11th Cir. 1983).

even though in most cases the defendant could not possibly reveal any classified information that would “surprise” the government.

Contrary to what the *Poindexter* court assumed,¹⁷⁰ the argument that defense counsel should not have to provide a roadmap of the defense is decidedly *not* based on the premise that the defense enjoys a procedural right to surprise the prosecution. Rather, the constitutional prohibition against this kind of disclosure stems both from the defendant’s right to pretrial silence,¹⁷¹ and even more so from the due-process prohibition against nonreciprocal discovery burdens. Section 6(f)’s reciprocity clause is unbalanced from the start, since the government has no obligation to furnish the defense with information regarding the “use, relevance, or admissibility” of rebuttal material, as the defense must do for the government under Section 6(a).¹⁷² Indeed, it appears that the government can satisfy its reciprocity obligations with a mere document dump, whereas the defendant must make an exhaustive disclosure “with particularity.”¹⁷³ Such skewed burdens cannot be reconciled with the *Wardius* Court’s instruction that any imbalance in discovery rights should “work in the defendant’s favor.”¹⁷⁴

It is also worth reiterating that this analysis is only compelling within the sphere of terrorism and other outsider prosecutions. In standard insider cases, the government’s interest in not being graymailed has been held to outweigh the harm caused by unbalanced discovery burdens. *Wardius* was, after all, decided in the absence of any showing of strong state interests.¹⁷⁵ Unless some other compelling state interest were at play, *Wardius* would render nonreciprocal discovery burdens unconstitutional as applied to outsider defendants. As the Supreme Court has noted, “it is obvious and unarguable that no governmental interest is more compelling than the security of the

170. See *United States v. Poindexter*, 725 F. Supp. 13, 34 (D.D.C. 1989) (“This argument assumes that defendant has an unqualified right to undiminished surprise with respect to his cross-examination.”).

171. See *supra* Part II.B.; see also *supra* note 72 and accompanying text.

172. See 18 U.S.C. app. III § 6(f) (requiring the United States to disclose the “information it expects to use to rebut the classified information”).

173. *Collins*, 720 F.2d at 1199.

174. *Wardius v. Oregon*, 412 U.S. 470, 475 n.9 (1973). The common response to invocations of *Wardius* is that the case was decided in a context with an “absence of a strong showing of state interests.” *Id.* at 475. But as this Subsection argues, the state interests particular to CIPA cases are eroded (if not entirely eliminated) in terrorism prosecutions.

175. *Id.* at 475.

Nation.”¹⁷⁶ Undoubtedly, in the realm of counterterrorism and national security, some state secrets could cause irreparable damage if disclosed. Moreover, certain defendants might seek to aid a larger jihadist conspiracy by attempting to relay to other conspirators useful classified information produced to them in discovery. Nonetheless, for two reasons, these state interests will rarely be compelling.

First, these concerns apply to very few defendants. Although they may be meaningful for the Zacarias Moussaouis of the world, they are of little relevance to self-radicalized individuals and the two-thirds of all terrorism defendants who have either no link to jihadist crimes or no identifiable affiliation with a terrorist organization.¹⁷⁷ Only around 9 percent of all terrorism defendants have a formal or informal association with al-Qaeda,¹⁷⁸ and even this number is inflated by increasing use of the charge of material support for terrorism.¹⁷⁹

Second, it is very unlikely that a FISA intercept in a civilian terrorism prosecution would contain perilous state secrets. Data collected from surveillance of a defendant is unlikely to contain anything but information about the defendant himself.¹⁸⁰ Disclosure of the defendant’s own speech would almost certainly not threaten national security, since the communications were not classified when made, and had they been recorded by the defendant rather than the government, the defendant could introduce them at trial and reveal them to the public at his pleasure.¹⁸¹ When vital national-security information *is* implicated, or when defendants are particularly likely to disclose classified information, a strong governmental interest in protecting national security—often present in *first-generation* CIPA cases—may justify CIPA’s potential discovery imbalance.

176. Haig v. Agee, 453 U.S. 280, 307 (1981).

177. See 2011 Terrorist Trial Report Card, *supra* note 117 (percentage calculated using underlying data). Of the roughly 1078 terrorism prosecutions in the decade after 9/11, nearly five hundred involved individuals without a link to jihadist crimes, but instead other activity “such as violence by far right wing paramilitary terror groups in South America or the United States.” *Id.* at 7 n.2. A further 231 defendants classified as jihadists had no identifiable link to a terrorist organization. *Id.* at 14.

178. See *id.* at 14 (percentage calculated from underlying data).

179. See *id.* at 16 (“The idea that terror organization affiliation is on the rise is buttressed, for example, by the increase in material support charges, in which 85% are conclusively associated with a terrorist group.”); see also 18 U.S.C. § 2339A, 2339B (2012) (defining the offenses of providing material support to terrorism and to designated foreign terrorist organizations).

180. See *supra* note 132 and accompanying text.

181. Dratel, *supra* note 132, at 180.

2. *Ineffective Assistance of Counsel.* The contextual shift in CIPA cases has also threatened defendants' right to the effective assistance of counsel. When evidence has been generated through FISA surveillance, discovery will be particularly voluminous. The classified evidence will often consist of months of electronic surveillance data, including telephone conversations, emails, social-media or fax exchanges, and Internet browsing histories. One case even involved *seven years* of FISA intercepts.¹⁸²

A larger problem is that the content of these intercepts is quite often (if not usually) in a foreign language, such as Urdu or Arabic.¹⁸³ In *United States v. Al-Hussayen*,¹⁸⁴ for example, the classified discovery included more than twenty thousand communications, including an additional seventy-five CDs of "classified raw internet data" and ninety-seven CDs of classified telephone intercepts, "predominantly if not exclusively in Arabic."¹⁸⁵ Defense counsel did not speak Arabic, and there were no qualified Arabic translators with security clearance in Southern Idaho.¹⁸⁶ The volume and language of the classified evidence rendered it "impossible for the defense to review the materials in time to make effective use of them at trial."¹⁸⁷ Al-Hussayen thus argued that the government had "used its unreviewable classification authority as an offensive weapon, effectively placing critical voluminous evidence off-limits to [his] defense."¹⁸⁸ This tactic, he claimed, amplified "the general inequity created by CIPA in cases in which the defendant does not have knowledge of the classified information."¹⁸⁹

Even beyond these problems, there are scenarios in which the defendant's assistance is essential. In the Embassy Bombings case, defendant El-Hage's attorneys argued that certain classified material "must be discussed with Mr. El-Hage prior to his testimony if his right

182. *United States v. Sattar*, No. 02 CR. 395 (JGK), 2003 U.S. Dist. LEXIS 16164, at *27 (S.D.N.Y. Sept. 13, 2003).

183. *See* Dratel, *supra* note 132, at 175–77 (compiling cases).

184. *United States v. Al-Hussayen*, No. CR03-048-C-EJL, 2004 U.S. Dist. LEXIS 29793 (D. Idaho Apr. 7, 2004).

185. Memorandum in Support of Motion To Declare CIPA Unconstitutional as Applied in This Case at 3–4, *Al-Hussayen*, No. CR03-048-C-EJL, 2004 U.S. Dist. LEXIS 29793.

186. *Id.* at 4.

187. *Id.*

188. *Id.* at 7.

189. *Id.*

to counsel . . . is to have any meaning.”¹⁹⁰ Counsel further contended that because they did not know which government witnesses would testify at trial, El-Hage’s assistance was needed to determine what portions of the classified discovery materials were relevant to his defense.¹⁹¹

The Sixth Amendment right to counsel requires more than the presence of an attorney “alongside the accused”—it also comprehends the “effective assistance of counsel.”¹⁹² This guarantee is violated by a government action that “interferes in certain ways with the ability of counsel to make independent decisions about how to conduct the defense.”¹⁹³ If, as in the case of Al-Hussayen, CIPA is used to prevent the defendant from viewing classified information relevant to his defense, or to tactically delay declassification until it is impossible to effectively review the evidence in time, the Sixth Amendment’s guarantee is interfered with.¹⁹⁴ This problem will plague nearly every CIPA and FISA case in which the outsider defendant does not possess the classified information from the start. This issue exists even in the absence of prosecutorial abuse, as the sheer volume of classified evidence and the effort required to translate it can pose nearly insurmountable tactical obstacles to the defense.

In insider cases, CIPA is rightly invoked to prevent national-security gamesmanship by the defendant. But in outsider cases, CIPA can completely undermine defense counsel’s ability to identify exculpatory evidence and enlist the client in his own defense. This problem, and many others posed by CIPA, can be readily solved by tailoring the statute’s procedural mechanisms to the specific offenses that are charged.

190. *In re Terrorist Bombings of U.S. Embassies in E. Afr.*, 552 F.3d 93, 123 (2d Cir. 2008) (citation omitted).

191. *Id.* at 123–24.

192. *Strickland v. Washington*, 466 U.S. 668, 685–86 (1984) (quotations omitted).

193. *Id.* at 686.

194. In contrast to ordinary ineffective-assistance claims, in which a convicted defendant identifies something his counsel could have done better with the available information, defendants in CIPA cases are instead challenging a systematic “state interference with the ability of counsel to render effective assistance to the accused” proscribed by *Strickland*. *Id.* at 683.

IV. A PROPOSAL FOR REFORM: AN OFFENSE-SPECIFIC APPROACH

Without CIPA, the government would be left without any procedural mechanism to control the dissemination of national-security information in criminal proceedings. For this reason, CIPA serves a vital function in many cases. Correcting constitutional defects in the statute should therefore be accomplished through amendment, not repeal. Because it is specifically the contextual shift from insider to outsider cases that has engendered constitutional concerns, this Note proposes that CIPA be reworked in an offense-specific manner to account for varying governmental interests and differently situated criminal defendants. This would allow CIPA to remain substantially unchanged in its initially contemplated contexts, which have been universally upheld. A new set of procedures should be fashioned for cases in which the specter of graymail is absent. The ensuing Sections suggest new sample language intended to correct contextual disparities in enforcement, while preserving the statute's recognized virtues.

My proposed revision to CIPA would codify the contextual variations in CIPA's use, and, more specifically, would prescribe new standards for discoverability, a limited and qualified declassification requirement, and a bifurcated method of conducting admissibility hearings.

A. *Codifying the Insider–Outsider Distinction*

I propose a statutory recognition of the insider–outsider distinction,¹⁹⁵ allowing CIPA to adapt dynamically to varying contexts. First, Section 1 of the statute should be amended as “Definitions and Procedural Application,” with the following new subsection:

In cases in which the indictment alleges violation(s) of 18 U.S.C. §§ 792–98, §§ 951–52, § 957, §§ 1385–86, §§ 2381–84,¹⁹⁶ or in the

195. These terms were initially coined by Professor Ellen Yaroshefsky when she observed that terrorism cases may exacerbate problems with secret evidence in the courts. Yaroshefsky, *supra* note 4, at 1067–68. Because her article focused on the deleterious effects of secret evidence generally, she did not expound on the change in context or suggest how it might be resolved. *See id.* (describing the nature of the distinction).

196. Owing to the author's limited foresight, this is not, and is not intended to be, an exhaustive list, but rather a sample of offenses for which there is a reasonable likelihood that the defendant will possess sensitive national-security information, thereby triggering a strong state interest justifying more restrictive measures. Any statutory amendment should thus include any other offenses that meet this criterion. The sample offenses listed here are the federal statutes proscribing espionage, aiding a foreign government, selling state secrets, acting

prosecution of any government official or member of the armed forces for actions committed in their official capacity, §§ 4–6 of this Act shall govern the disclosure of classified information. The United States may, in the alternative, invoke §§ 4–6 of this Act by submitting to the court an affidavit of the Attorney General certifying that the defendant is in possession of classified information, the disclosure of which would cause identifiable damage to the national security of the United States.

In all cases in which the procedures of Sections 4–6 are not invoked pursuant to the above provision, newly added sections of CIPA should govern the disclosure of classified information. The proposed Section 1 applies CIPA’s existing procedures to prosecutions involving espionage, treason, and other typically “insider” cases. To alleviate the constitutional concerns arising from CIPA’s contextual shift to “outsider” prosecutions, a variety of adjustments must be made to the Section 4–6 equivalents for those cases.¹⁹⁷

B. Discovery of Classified Information by Defendants

Section 4 of CIPA currently permits courts to authorize the United States to delete or substitute specific pieces of classified information from the discovery provided to the defendant through an ex parte request by the government.¹⁹⁸ The court will determine whether documents are discoverable on the basis of their materiality and relevance to the defense.¹⁹⁹ If documents are deemed to be discoverable, then the court can either order disclosure or permit a substitution.²⁰⁰

Forbidding defense counsel from participating in determinations of materiality and relevance is indefensible in an adversarial criminal-justice system—no one but defense counsel, who has conferred with her client and developed a legal strategy, could possibly know what is

as an agent of a foreign government without permission, publishing diplomatic codes, possessing property in aid of a foreign government, using the Army or Air Force as a *posse comitatus*, stealing Department of Defense locks or keys, and committing treason, misprision of treason, rebellion or insurrection, or seditious conspiracy.

197. These cases will likely predominantly consist of terrorism and international drug-conspiracy prosecutions. See Yaroshefsky, *supra* note 4, at 1067–68.

198. 18 U.S.C. app. III § 4 (2012).

199. See, e.g., *United States v. Clegg*, 740 F.2d 16, 18 (9th Cir. 1984) (ordering the government to disclose information where materials were “relevant to the development of a possible defense”).

200. Yaroshefsky, *supra* note 4, at 1069.

material and relevant to the defense. The judge and prosecutor are not zealous advocates of the defendant. Surely, then, they should not be asked to predict the defense's theory of the case and fairly represent the defendant's interests. As one court observed, such a system "force[s] this court into the very awkward position of making [the] defendant's case and then deciding his claim."²⁰¹ The Supreme Court has similarly remarked that "[i]n our adversary system, it is enough for judges to judge. The determination of what may be useful to the defense can properly and effectively be made only by an advocate."²⁰² Accordingly, Section 4 should be rewritten as follows (with proposed additions marked in italics):

The court, upon a sufficient showing of *irrelevance and immateriality*, may authorize the United States to delete specified items of classified information from documents to be made available to the defendant through discovery under the Federal Rules of Criminal Procedure, *or upon a sufficient showing of identifiable damage to the national security of the United States*, to substitute a summary of the information for such classified documents, or to substitute a statement admitting relevant facts that the classified information would tend to prove, *when such substitution would not be reasonably likely to prejudice the defendant*. The court may permit the United States to make a request for such authorization in the form of a written statement to be inspected by the court *and by defense counsel possessing security clearance at a sufficient level to view the classified information at issue. If the court grants such authorization, it shall, upon motion of the United States, order defense counsel to protect against disclosure of undiscoverable classified information to the defendant or any other individual.*

My proposed Section 4 introduces three significant changes. First, it alters the *ex parte* nature of Section 4 hearings, allowing cleared defense counsel to object to the government's requests for substitutions and deletions, and thereby argue for the discoverability of evidence. Second, it establishes two discrete standards for making Section 4 determinations: irrelevance and immateriality (for deletions) and identifiable damage to the national security of the United States (for substitutions). These new standards would provide much-needed clarity for judges deciding whether to admit classified

201. *United States v. Rezaq*, 156 F.R.D. 514, 527 (D.D.C. 1994), *opinion vacated in part on reconsideration*, 899 F. Supp. 697 (D.D.C. 1995).

202. *Dennis v. United States*, 384 U.S. 855, 875 (1966).

evidence, and bring the statute more in line with the *Roviaro* Court's instruction that the executive privilege must be subordinated to the defendant's right to a fair trial.²⁰³ Clarifying that deletion of evidence is permissible only when it bears no relevance to the case should also prevent courts from deferring too strongly to the government and imposing heightened materiality standards without statutory authorization to do so.²⁰⁴

Finally, this proposal would allow the court to issue a protective order barring defense counsel from disclosing to the defendant any classified information that the court excludes as a result of its Section 4 determination. This safeguard would preclude artful defense attorneys from using the Section 4 hearing to pinpoint sensitive information without having to navigate voluminous recordings, in order to facilitate graymail.

Because the problem of defense counsel's exclusion from Section 4 hearings is not intrinsic to outsider cases (though it is certainly more pervasive in that context), these changes must be made to *both* the insider and outsider sections of an offense-based CIPA.

C. *The Section 5 Notice and FISA: A Qualified Declassification Requirement*

Section 5 of CIPA sets forth the notice requirements of the statute.²⁰⁵ Subsection (a) mandates that defendants must provide the government with advance notice of any classified information that the defense "reasonably expects to disclose or to cause the disclosure of . . . in any manner in connection with [the] trial."²⁰⁶ The defendant is also barred from disclosing any classified information until the statutorily required notice has been given and the United States has been allowed a reasonable time to seek a determination on admissibility and appeal any such determination.²⁰⁷ These requirements may well impose nonreciprocal (and therefore unconstitutional) discovery burdens.²⁰⁸ I propose that Section 5(a) be supplemented by the following new language:

203. *See Roviaro v. United States*, 353 U.S. 53, 60–61 (1957) ("Of course where enforcement of a nondisclosure policy deprives an accused of a fair trial it must either be relaxed or the prosecution must be foregone.").

204. *See supra* notes 37, 47 and accompanying text.

205. 18 U.S.C. app. III § 5 (2012); *see supra* Part II.A.

206. 18 U.S.C. app. III § 5(a).

207. *Id.*

208. *See supra* Part III.B.1.

(a)(1) Before the filing of notice by the defendant pursuant to Section 5, the Government shall declassify all qualifying classified documents or materials. For purposes of this section, a qualifying document is one that meets all three of the following criteria:

(A) The information is limited to the personal communications of the defendant, including his or her own telephone, Internet, and written communications, or other electronic or Internet records, telephone or cellular-device records, or physical materials belonging to the defendant, notwithstanding seizure by the Government;

(B) The contents of such documents or communications are not classified independent of their presence within a government intercept or seizure conducted pursuant to the Foreign Intelligence Surveillance Act (FISA), or other statute authorizing classification based on method of acquisition; AND

(C) The classified information was made available to the defendant by the United States through discovery under the Federal Rules of Criminal Procedure.

These amendments would resolve a recurring problem in terrorism prosecutions, in which defendants are prevented from disclosing their own emails, conversations, or Google searches, merely because of the method through which the government acquired them.²⁰⁹ Taken together, these amendments would alleviate the Section 5 notice burden by requiring the government to declassify the defendant's personal communications if they were deemed discoverable and do not contain content that was classified when the defendant uttered or produced it. In other words, the amendments mandate declassification of information that was classified *solely* because of method of acquisition, not content.

This provision would remedy many of Section 5's constitutional problems without impairing any compelling governmental interests. If a document is discoverable, it is not excludable anyway, so declassification merely eases the review process for counsel by eliminating the need to travel to a SCIF to view any FISA-intercepted communications, and entirely refrain from discussing them outside that area.²¹⁰ Moreover, since the classification authority rests with the government, the only documents that would be declassified would be

209. *See supra* Part III.A.

210. *See supra* note 40 and accompanying text; Part II.A.

ones that the United States, in its unfettered discretion, does not deem classifiable but for the method through which they were acquired. Thus, the amendments would not threaten to expose state secrets.

Because classification is an executive function, this proposal could not be enforced by a court *ordering* the government to declassify. Instead, failure to declassify would be met with sanctions (dismissal of a charge, or other sanctions the district court deems appropriate). Sanctions are already imposed under CIPA when the government declines to turn over documents deemed discoverable,²¹¹ and could work equally well in this context. The revised Section 5(a) should be added only to the new outsider sections because in insider prosecutions involving espionage, intelligence officers, or government officials, a defendant's own communications may very well contain classified information, and so a content review of all communications would be prohibitively onerous for the prosecution and only minimally advantageous for the defendant.²¹²

Prosecutors are likely to object to this proposal because it requires the state to undertake a time-consuming pretrial process of declassification before discovery. This is a valid concern, but prosecutors would be far less burdened by the proposal than defense counsel would be in having to travel to a SCIF and navigate thousands of hours of recordings to find relevant evidence. This is because the state will likely know beforehand whether discovery materials contain sensitive information. Prosecutors would also likely argue that even the defendant's innocuous personal communications ought to remain classified if disclosure would reveal American surveillance protocols. This argument justifies the classification of FISA warrants generally, but becomes less persuasive once the government has already disclosed to the defendant that he has been electronically surveilled under the authority of FISA.

211. 18 U.S.C. app. III § 6(e) (2012); *see also* United States v. Wilson, 586 F. Supp. 1011, 1013 (S.D.N.Y. 1983) (noting that CIPA “does not alter the existing standards for determining relevance or admissibility”).

212. For instance, if FISA surveillance had been conducted on an individual charged under 18 U.S.C. § 798 with transmitting classified documents to a foreign government, the defendant's intercepted electronic documents would presumably contain the very classified information that gave rise to the charge. In contrast, the personal communications of terrorism defendants rarely, if ever, contain information that would be classified because of its content; instead, they usually contain incriminatory statements or Internet searches evincing a desire to commit or conspire to commit an act of terror. This would make it much easier for the government to identify communications classifiable on the basis of content, if they even existed at all.

D. The Section 6 Hearing and Bifurcation

Section 6 allows the government to move for a hearing on the use, relevance, or admissibility of classified information contained in the defendant's Section 5 notice.²¹³ As many defendants have argued, this effectively requires the defense to hand the government a roadmap of its case by explaining counsel's theories on the use and relevance of defense evidence. Further, Section 6 imposes greater discovery burdens on defendants than on the government.²¹⁴ Whereas compelling state interests justify these lopsided procedures for insider CIPA cases, no such justification exists in the vast majority of terrorism prosecutions. Thus, Section 6(a) should be rewritten as follows to account for outsider cases (proposed changes are marked in italics):

Within the time specified by the court for the filing of a motion under this section, *and upon request of the United States, the court shall* conduct a *series of* hearings to make all determinations concerning the use, relevance, or admissibility of classified information that would otherwise be made during the trial or pretrial proceeding. *Before making its determination of admissibility, the court shall order defense counsel to make an in camera and ex parte showing of the use, admissibility, and relevance of such information. The court shall then conduct an in camera review of the United States' reasons counseling against disclosure. As to each item of classified information, the court shall set forth in writing the basis for its determination.*

The sample language above also omits the provision of Section 6(a) that currently allows for an in camera hearing upon certification by the Attorney General that "a public proceeding may result in the disclosure of classified information."²¹⁵ This provision is obviated by the proposed amendment's requirement that all proceedings be held in camera. The most significant proposed change is the bifurcation of the hearing stage. Counsel for the United States would be excluded from the initial hearing, and as such, would not be privy to defense counsel's theories on the use and relevance of classified information (though the United States would be allowed to make a separate in camera showing of the state interests weighing against disclosure).

213. 18 U.S.C. app. III § 6.

214. *See supra* Part III.B.1.

215. 18 U.S.C. app. III § 6(a).

Excluding the United States from such hearings is not unprecedented.²¹⁶ In *United States v. Bin Laden*, the court rejected the government's argument that an *ex parte* showing by the defendant would "clearly frustrate CIPA's purpose in identifying for the Government the national security 'cost' of going forward with particular charges against particular defendants."²¹⁷ The district court, acknowledging that CIPA's framers "expected the trial judge to fashion creative and fair solutions for classified information problems,"²¹⁸ held five *in camera* CIPA hearings.²¹⁹ First, defendant El-Hage's attorneys, in the presence of the government, described the classified information expected to be disclosed. The court then excused defense counsel in order to hear the government's reasons for refusing to declassify. Finally, the court recalled El-Hage's attorneys, "inquiring, in the absence of government counsel, into the use that El-Hage's counsel planned to make of the classified information at issue."²²⁰ This solution, which succeeded in preventing prejudice to either side in *Bin Laden*, should be statutorily mandated in CIPA.

Excluding the government's attorneys from a hearing on the use and relevance of evidence to the defense case is not as problematic as excluding defense counsel from a Section 4 hearing. In the latter situation, the court makes a determination on the relevance and materiality of evidence for the defense, but with no input from defense counsel. This is particularly troubling because only defense counsel could possibly know the defense's theory of the case, and thus, the relevance and materiality of evidence. In a Section 6 hearing, however, exclusion of the United States would not prejudice

216. See *United States v. Poindexter*, 725 F. Supp. 13, 29 (D.D.C. 1989) (permitting an *ex parte* submission so that defendant would not have to disclose his trial strategy to the government). In *United States v. North*, 708 F. Supp. 389 (D.D.C. 1983), the district court allowed an *ex parte* and *in camera* hearing on discovery for Oliver North. *Id.* at 391. "[T]he court heard North and his counsel at an *ex parte, in camera* hearing where aspects of North's defense were revealed. As a result of that proceeding, without giving Independent Counsel even an opportunity to be heard, the Court ordered extensive discovery on July 8, 1988." *Id.* Though this was not a hearing on materiality, the court's *in camera* review of defense counsel's reasons for pursuing pieces of evidence is analogous to a materiality showing, in which counsel would have to disclose his theory of relevance and use.

217. *United States v. Bin Laden*, No. S(7) 98 CR. 1023 LBS, 2001 WL 66393, at *6 (S.D.N.Y. Jan. 25, 2001).

218. *Id.* (quoting *United States v. Poindexter*, 698 F. Supp. 316, 320 (D.D.C. 1989)).

219. *In re Terrorist Bombings of U.S. Embassies in E. Afr.*, 552 F.3d 93, 118–19 (2d Cir. 2008).

220. *Id.* at 119.

either side, as the presence of the government's attorney is not necessary to determine the materiality of evidence to the defense. Under a bifurcated system, the government would still be given the Section 5 notice of classified information that the defendant intends to disclose, but would not know how defense counsel intended to use it.

Of course, if Section 5 of CIPA is amended as suggested in the previous section, Section 6 hearings will become somewhat rare in outsider cases, since personal communications will have been declassified. As a result, these hearings will only be necessary when the evidence at issue does not concern personal communications, such as Zacarias Moussaoui's request to depose detainees. For the same reasons as with the Section 5 amendments, these changes must be only in the new sections dealing with outsider cases. Because the *content* of the classified information in insider cases is far more likely to be sensitive, the threat of exposing the government to "surprise at what may be revealed in the defense"²²¹ is much greater in prosecutions of government officials and intelligence officers. As previously discussed, the argument against forcing defense counsel to make extensive disclosures is based on the qualified²²² rights to pretrial silence and reciprocal discovery burdens. These are overcome in insider cases, where the strong interest against inadvertent disclosure of vital state secrets outweighs the defendant's right to reciprocal burdens.

CONCLUSION

More than half a century ago, the Supreme Court declared that when disclosure of classified information is necessary for a fair trial of the accused, "the [executive] privilege must give way."²²³ The Court declined to establish clear rules for courts to use in this difficult interest-balancing equation. As originally conceived, CIPA served a vital gap-filling function by establishing fixed procedures for the admission of classified information in criminal trials. But a recent contextual shift in the types of cases involving CIPA has resulted in increasing deference to the Executive at the expense of the "fair

221. *United States v. Collins*, 720 F.2d 1195, 1200 (11th Cir. 1983).

222. *See, e.g., Wardius v. Oregon*, 412 U.S. 470, 475 (1973) (stating that the right to reciprocal discovery burdens exists only "in the absence of a strong showing of state interests to the contrary").

223. *Roviaro v. United States*, 353 U.S. 53, 61 (1957).

determination of a cause.”²²⁴ As a result, CIPA—an otherwise facially constitutional statute—has become unconstitutional as applied in many cases. As the *Rovario* Court remarked, “Whether a proper balance renders nondisclosure erroneous *must depend on the particular circumstances of each case, taking into consideration the crime charged, the possible defenses, . . . and other relevant factors.*”²²⁵ As currently written, CIPA applies identically to all circumstances and federal crimes.

By amending CIPA in an offense-specific manner and tailoring CIPA’s procedures to the criminal defendant in question, the statute’s important goal of providing a sensible interest-balancing mechanism can be preserved. A dynamic and adaptable CIPA would also bring the statute in line with the Court’s instructions on offense-tailored interest balancing. To these ends, this Note has proposed sample amendments designed to achieve an offense-based CIPA, including (1) a more inclusive discovery process and clearer standards to govern discoverability; (2) a limited and qualified declassification system in select cases involving FISA; and (3) a new bifurcated procedure for Section 6 hearings on admissibility.

In an era of unprecedented government secrecy, it is more important than ever to preserve the integrity of our courts. CIPA was designed for this very purpose, but if it is not brought into the twenty-first century, it will undermine that integrity and subvert the procedural safeguards that have long been hallmarks of our Constitution.

224. *Id.*

225. *Id.* at 62 (emphasis added).