ADDRESSING THE BALANCE: RESTRUCTING CIPA AND FISA TO MEET THE NEEDS OF JUSTICE AND THE CRIMINAL JUSTICE SYSTEM

*Wesley S. McCann**

ABSTRACT

Balancing the needs of defendants and the needs of the state in criminal prosecutions is a difficult task. This same issue is aggravated in prosecutions involving national security or terrorism. The Classified Information Procedures Act ("CIPA")[1] and Foreign Intelligence Surveillance Act ("FISA")[2] govern the admissibility and use of classified information in criminal trials and obtainment of classified communications, respectively.[3] Each presents its own challenges to the adjudicative process for both sides.[4] As such, both play an important role in our national security, yet their application to criminal prosecutions can involve the circumvention of civil liberties or due process rights.[5] However, both Acts can also burden the government when using intelligence information in criminal cases.[6] This article examines both CIPA and FISA within the context of terrorism and national security-related prosecutions. This article also examines the extent to which each Act can be reformed to meet the needs of both sides during the criminal process by presenting what other scholars have recommended along with the major revisions posited here.

* Wesley S. McCann, Ph.D., Criminology and Criminal Justice, Washington State University.

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

[2] Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801–1885c.

[3] 18 U.S.C. app. §§ 4, 6, 8, 10; 50 U.S.C. §§ 1804(a), 1806(d)–(f).

[4] *See* Arjun Chandran, Note, *The Classified Information Procedures Act in the Age of Terrorism: Remodeling CIPA in an Offense-Specific Manner*, 64 DUKE L.J. 1411, 1412–13, 1427–28, 1437–38 (2015).

[5] *See id.* at 1412–13; 1428; 1437–38.

[6] *See id.* at 1427, 1428.

I. INTRODUCTION

The criminal adjudicative process consists of numerous provisions that protect the defendant from the overarching power of the State.[7] Within the penumbra of provisions that defendants have access to are the rights to a speedy trial and an impartial jury, to confront witnesses, have counsel,[8] and the right against self-incrimination.[9] Terrorism-related trials are slightly different from conventional criminal cases.[10] These trials are furthermore affected by CIPA, whereby both the government and the defendant have to abide by specific guidelines as to how to both preserve the integrity of the defendant's due process rights and maintain national security interests.[11] Thus, the invocation of CIPA in terrorism-related cases seemingly creates a balancing test between defendants' Fifth and Sixth Amendment rights and the security of the state.[12]

The use of CIPA during the adjudicative process prevents defendants from "graymail[ing]" the government into reducing or dropping the charges against them in order to preclude them from disclosing secretive or sensitive information.[13] These situations usually arose, however, from those involved in the Intelligence Community ("IC") presenting or threatening to present information that they had access to via their capacity within the IC.[14] Nonetheless, the government has the authority to prevent such information from ever being used in court proceedings.[15] Yet some argue that this infringes on a defendant's Fifth and Sixth Amendment rights, while leaving the door open to certain government abuses of authority.[16] Similarly, FISA poses other issues concerning the collection and dissemination of intelligence for prosecutorial purposes.[17]

---

[7] U.S. CONST. amend. V, VI.

[8] U.S. CONST. amend. VI.

[9] U.S. CONST. amend. V.

[10] *See* Michal Buchhandler-Raphael, *What's Terrorism Got to Do with It? The Perils of Prosecutorial Misuse of Terrorism Offenses*, 39 FLA. ST. U.L. REV. 807, 839 (2012).

[11] *See* Chandran, *supra* note 4, at 1412–13.

[12] *See id.*

[13] *See id.* at 1415.

[14] *See* Christopher W. Behan, *Guantanamo Bay: What Next?: Military Commissions and the Conundrum of Classified Evidence: A Semi-Panglossian Solution*, 37 S. ILL. U. L. J. 643, 654 (2013).

[15] *See id.* at 657–58.

[16] *See* Rabea Chaudhry, Comment, *Effective Advocacy in a Time of Terror: Redefining the Legal Representation of a Suspected Terrorist Facing Secret Evidence*, 8 UCLA J. ISLAMIC & NEAR E. L. 101, 123–24 (2009).

[17] *See* Chandran, *supra* note 4, at 1437–38.

In Part II, this article examines both CIPA and FISA historically. This section also examines the procedural mechanisms that guide both CIPA and FISA and how they comport and differ with conventional criminal procedure. Part II will also discuss materiality standards, and what constitutes evidence and information that is "material" to a defendant in all criminal cases. Part III provides a case example and analysis of the tenuous application of FISA and CIPA in *United States v. Abu-Jihaad*.[18] This section does not contend that either the district or circuit courts were wrong, but rather, merely contends that there is difficulty inherent in applying both FISA and CIPA to terrorism prosecutions.

Part IV discusses the current literature on CIPA and FISA reform and what should be done with each Act moving forward. This part considers various recommendations offered by others and adopts in part some of these recommendations while proffering its own specifics. Specially, this article advocates for the restructuring of the purpose of FISA, as well as its provisions, in order to make it more amenable to criminal prosecutions, while also making declassification procedures under it more robust and efficient. Furthermore, this part also argues that CIPA needs to be altered to allow for the participation of defense counsel in *ex parte* proceedings to strengthen the adversarial process. Last, this part argues that there needs to be more independent and external oversight and transparency concerning the use and issues related to the application of FISA in terrorism and national security-related prosecutions. Part V briefly concludes and summarizes the arguments of the article.

II. THE STATE OF THE ADVERSARIAL SYSTEM

A. Overview of CIPA and FISA

There is great debate about whether our current counter-terrorism policies are effective, or whether they are actually causing more harm than good.[19] However, many of these arguments specifically concern policies that prevent the criminal act of

[18] United States v. Abu-Jihaad, 630 F.3d 102 (2d Cir. 2010).

[19] *See* Gary LaFree & Gary Ackerman, *The Empirical Study of Terrorism: Social and Legal Research*, 5 ANNU. REV. SOC. SCI. 347, 361 (2009); Clark McCauley, *Psychology Issues in Terrorism and the Response to Terrorism*, *in* PSYCHOLOGY OF TERRORISM 13 (Bruce Bongar et al. eds., 2007).

terrorism, not policies relating to due process rights of terrorists.[20] This is even more evident in the fact that much of the post-9/11 legislation has attempted to significantly curb terrorists' legal rights.[21] Thus, the question remains: do the policies control crime, or do they control specific populations of people? In any case, scholars have meticulously analyzed the legal arguments of whether terrorists held at extraterritorial facilities should even be tried in Article III courts—yet the Supreme Court has had the final say as to how this right is interpreted.[22] Moving forward, many scholars have begun to analyze both contemporary surveillance powers in United States law enforcement and national security efforts,[23] and the ability of the courts to combat terrorism[24]:

> Several factors distinguish the war against al Qaeda from a large-scale criminal investigation or a broad, persistent social problem. First, al Qaeda represents a foreign threat that originates outside the United States. Al Qaeda's foreign element makes it different from homegrown terrorism, such as Timothy McVeigh's 1995 bombing of the Alfred Murrah Federal Building in Oklahoma City, which is an appropriate subject for the criminal justice system. Second, al Qaeda is unlike a crime organization in that it seeks purely political ends, rather than purely financial gain. Al Qaeda attacked the United States because it wants the United States to withdraw its military and political presence from the Middle East. Al Qaeda may seek financial gain to fund its terrorist operations to achieve that goal, but financial advancement is not its purpose. Third, al Qaeda has proven that it is

---

[20] *See* Carl Tobias, *Terrorism and the Constitution: Civil Liberties in a New America: Punishment and the War on Terrorism*, 6 U. PA. J. CONST. L. 1116, 1116–17 (2004).

[21] *See, e.g.*, National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, 125 Stat. 1298; Military Commissions Act of 2006, Pub. L. No. 109-366, 120 Stat. 2600; Authorization for Use of Military Force Act, Pub. L. No. 107-40, § 2(a), 115 Stat. 224 (2001); *see generally* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 [hereinafter USA PATRIOT Act of 2001].

[22] *See* Tobias, *supra* note 20, at 1126–28; *see, e.g.*, Boumediene v. Bush, 553 U.S. 723, 732, 766, 771 (2008) (deciding whether terrorists being held at Guantanamo Bay, Cuba, were capable of seeking relief in Article III courts, citing *Hamdi v. Rumsfeld* as controlling law); Hamdan v. Rumsfeld, 548 U.S. 557, 569, 677–78 (2006); Hamdi v. Rumsfeld, 542 U.S. 507, 510, 525 (2004).

[23] *See* Jeffrey S. Brand, *Eavesdropping on Our Founding Fathers: How a Return to the Republic's Core Democratic Values Can Help Us Resolve the Surveillance Crisis*, 6 HARV. NAT'L SEC. J. 1, 22–23 (2015); Afsheen John Radsan, *Remodeling the Classified Information Procedures Act (CIPA)*, 32 CARDOZO L. REV. 437, 461–62 (2010).

[24] *See* Tobias, *supra* note 20, at 1117; John Yoo, *Courts at War*, 91 CORNELL L. REV. 573, 575 (2006).

> capable of inflicting a degree of violence and destruction that crosses the line separating crime and war. Although the precise location of this line may not be certain, it seems clear that with approximately three thousand deaths and billions of dollars in damage, the September 11 attacks crossed this line.[25]

What has been a continual struggle for our country is the balance between security and liberty.[26] The question that continually resurfaces is: "to what end is our conduct necessary?" While it can be argued that our punishment of suspected and confirmed terrorists is in need of systematic review,[27] the adjudication process is also in need of review.[28] At its core, CIPA is meant to procedurally regulate the admission of sensitive information in criminal courts.[29] Parallel to CIPA is FISA.[30] FISA was designed to procedurally delineate how foreign intelligence and counter-intelligence could be conducted by agencies,[31] as prior jurisprudence and legislation had avoided the topic of how *foreign* intelligence gathering could be conducted.[32] However, some claim that FISA was flawed because of its assumption that Fourth Amendment protections would be subject to national interest.[33] Nonetheless, there are inherent obstacles in showing how the amended FISA[34] purports to injure individuals via their communications.[35] *Clapper v. Amnesty International USA*[36] demonstrates how difficult it is for plaintiffs to establish not only the nature of the injury[37] and that it be "impending," but also the connection of the injury to FISA;[38] hence why the Court ruled in this case that the plaintiffs lacked

---

[25] Yoo, *supra* note 24, at 578–79.

[26] *See* Tobias, *supra* note 20, at 1117.

[27] *See id.* at 1149 ("In sum, basic aspects of the war on terrorism, namely detentions and military tribunals, comprise unique and disputed punishment systems. The regimes' adverse impacts, especially vis-a-vis civil liberties, outstrip the techniques' benefits, particularly those that involve security.").

[28] *See id.* at 1147–48.

[29] *See* Radsan, *supra* note 23, at 451.

[30] *See* Chandran, *supra* note 4, at 1426–28.

[31] *See* Brand, *supra* note 23, at 8–9.

[32] *See id.* at 8 (discussing how Title III, *Katz v. United States* (389 U.S. 347 (1967)), and *United States v. United States District Court* (407 U.S. 297 (1972)), intentionally failed to dictate how foreign intelligence gathering should be conducted, and instead, focused on how domestic intelligence gathering should be conducted for purposes of national security).

[33] *See id.* at 8, 24.

[34] Foreign Intelligence Surveillance Act, 50 U.S.C. § 1881a (2012).

[35] *See id.* § 1881a(d)(1).

[36] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).

[37] *See id.* at 1147–48 (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)).

[38] *Clapper*, 133 S. Ct. at 1142–43 (quoting *Whitmore*, 495 U.S. at 158).

Article III standing.[39] While this mainly concerns the use of foreign surveillance of non-U.S. citizens that are "reasonably" located outside of the United States,[40] it also exemplifies how the legal lexicons that are used to protect national security are ostensibly and purposely broad.[41] Also, the Foreign Intelligence Surveillance Court ("FISC") has held that there is no public right to FISC records, under either common law or the First Amendment.[42]

These concerns also coincide with the issue of courts overseeing the administration of justice via the structures meant to protect against the penetration of the intelligence community into the criminal justice system.[43] For one, there is the argument that there needs to be a wall between the intelligence community and law enforcement in an effort to prevent collusion between the two that would undermine the legitimacy of the criminal justice system.[44] However, law enforcement has already been engaging in intelligence gathering and surveillance through investigating organized crime, narcoterrorism, and drug operations.[45] Thus, FISA may actually further the penetration of intelligence gathering and the intelligence community into ordinary law enforcement in a manner that reflects, rather than amends, contemporary policing. How does this translate to the court system? Are courts meant to provide a meaningful check on these intelligence and data collection devices, or should their job be the conventional application of the law? If one were to look at the FISC, there would seem to be an abhorrent lack of judicial oversight of FISA warrants, in that close to 99.7% of all applications submitted by the Department of Justice ("DOJ") for surveillance purposes are approved.[46] Nonetheless, this process could be rigorous than is evident, but given that lack of transparency, it is easy to see this process as trivial. Overall, district courts in general may be providing a more adequate check

[39] *Clapper*, 133 S. Ct. at 1155.

[40] *Id.* at 1142 (citing 50 U.S.C. § 1881a(b)(2)).

[41] *See Clapper*, 133 S. Ct. at 1142.

[42] *See In re* Motion for Release of Court Records, No. Misc. 07-01 (FISA Ct. Dec. 11, 2007), https://www.eff.org/files/filenode/07403TFH/20071214doj-notice-relevant-authority-fisc-opinion.pdf (holding that there is no public right of access to FISC records).

[43] *See* RICHARD A. BEST JR., CONG. RESEARCH SERV., RL33873, SHARING LAW ENFORCEMENT AND INTELLIGENCE INFORMATION: THE CONGRESSIONAL ROLE 3 (2007).

[44] *See* DAVID H. BAYLEY & ROBERT M. PERITO, THE POLICE IN WAR: FIGHTING INSURGENCY, TERRORISM, AND VIOLENT CRIME 78 (2010).

[45] *See id.* at 75, 78.

[46] *See generally* Erika Eichelberger, *FISA Court Has Rejected .03 Percent of all Government Surveillance Requests*, MOTHER JONES (June 10, 2013), http://www.motherjones.com/mojo/2013/06/fisa-court-nsa-spying-opinion-reject-request (contending that out of approximately 33,900 FISA applications, only 11 resulted in denials).

on the procedures and application of both CIPA and FISA, as they are responsible for examining the lawfulness of the surveillance, and the conformity of the surveillance to the authorization.[47] Again, however, district courts are tasked with balancing the ever-present dichotomy within the criminal justice system: balancing social order and security with individual liberty.[48]

This is a complex issue, since courts already provide checks on law enforcement through the administration of criminal procedure laws, as well as hearing violations of due process claims.[49] However, what seems to be missing from most of the cases involving either FISA or CIPA is the idea that judges are also supposed to question the legitimacy of the rule of law that has been arguably expanded under the executive branch to further the aims of counter-terrorism and global surveillance.[50] There is a mounting argument that "if suspected terrorists are to be tried in federal court, the CIPA statute and other trial practices must be updated to sustain and to encourage greater collaboration between American intelligence agencies and law enforcement."[51] However, both FISA and CIPA's use in the adjudication of terrorists replaces its former use, which was to prosecute espionage cases.[52] Also, following 9/11, Congress amended FISA's requirement so that the pursuit of foreign intelligence be a "significant purpose," instead of the previous "primary purpose," in obtaining a warrant.[53] This could be viewed as altering the requirements needed to establish probable cause,[54] which is paramount to obtaining a warrant in any criminal

[47] *See, e.g.*, Foreign Intelligence Surveillance Act, 50 U.S.C. § 1806(f) (2012).

[48] *See* Marguerite Rigoglioso, *Civil Liberties in the Era of Surveillance*, STAN. L. (Nov. 13, 2014), https://law.stanford.edu/stanford-lawyer/articles/civil-liberties-and-law-in-the-era-of-surveillance/.

[49] *See* Robert P. Capistrano, *Federal Practice Manual for Legal Aid Attorneys: 5.1.B Express Causes of Action, Section 1983, Due Process Claims and Procedural Issues*, SHRIVER CTR. (2013), http://federalpracticemanual.org/chapter5/section1b.

[50] *See* Royce Lamberth, Former Presiding Judge of the U.S. Foreign Intelligence Surveillance Court, The Role of the Judiciary in the War on Terrorism, Address Before the University of Texas Law Alumni Association (April 13, 2002), http://www.pbs.org/wgbh/pages/frontline/shows/sleeper/tools/lamberth.html.

[51] *See* Radsan, *supra* note 23, at 438.

[52] *See* RICHARD B. ZABEL & JAMES J. BENJAMIN JR., IN PURSUIT OF JUSTICE: PROSECUTING TERRORISM CASES IN THE FEDERAL COURTS 87 (2008) (describing the shift in CIPA's purpose); William C. Banks, *The Death of FISA*, 91 MINN. L. REV. 1209, 1271 (2007) (describing the shift in FISA's purpose).

[53] USA PATRIOT Act of 2001, Pub. L. No. 107–56, 115 Stat. 272 (codified as amended in 50 U.S.C. §§ 1804, 1823 (2012)).

[54] *See, e.g.*, United States v. Abu-Jihaad, 630 F.3d 102, 119, 120, 127 (2d Cir. 2010); United States v. Duggan, 743 F.2d 59, 77 (2d Cir. 1984).

investigation.[55]

Former Attorney General Ashcroft, along with the FBI, has already tried to further *minimize* this wall between intelligence gathering and law enforcement.[56] Nonetheless, the FISC was dissuaded by the arguments brought forth to minimize the procedures separating the dissemination of information between law enforcement and intelligence officials.[57] More specifically, the court ruled that:

> In order to preserve both the appearance and the fact that FISA surveillances and searches were not being used *sub rosa* for criminal investigations, the Court routinely approved the use of information screening "walls" proposed by the government in its applications. Under the normal "wall" procedures, where there were separate intelligence and criminal *investigations*, or a single counter-espionage investigation with overlapping intelligence and criminal *interests*, FBI criminal investigators and Department prosecutors were not allowed to review all of the raw FISA intercepts or seized materials lest they become [de facto] partners in the FISA surveillances and searches. Instead, a screening mechanism, or person, usually the chief legal counsel in an FBI field office, or an assistant U.S. attorney not involved in the overlapping criminal investigation, would review all of the raw intercepts and seized materials and pass on only that information which might be relevant evidence. In unusual cases such as where attorney-client intercepts occurred, Justice Department lawyers in OIPR acted as the "wall." In significant cases, involving major complex investigations such as the bombings of the U.S. Embassies in Africa, and the millennium investigations, where criminal investigations of FISA targets were being conducted concurrently, and prosecution was likely, this Court became the "wall" so that FISA information could not be disseminated to criminal prosecutors without the Court's approval. In some cases where this Court was the "wall," the procedures seemed to have functioned as provided in the Court's orders; however, in an alarming

[55] FED. R. CRIM. P. 41(d)(1).

[56] Carol M. Bast & Cynthia A. Brown, *A Contagion on Fear: Post-9/11 Alarm Expands Executive Branch Authority and Sanctions Prosecutorial Exploitation of America's Privacy*, 13 CARDOZO PUB. L. POL'Y & ETHICS J. 361, 378–79 (2015).

[57] *Id.* at 379–80.

number of instances, there have been troubling results.[58]

Furthermore, the court essentially rejected Ashcroft's design to reduce the amount of "wall" between these two sides in an effort to make counter-terrorism cleaner due to the notion that his idea ostensibly "substitute[d] FISA for Title III electronic surveillances and Rule 41 searches."[59] Moreover:

> The 2002 minimization procedures give the Department's criminal prosecutors every legal advantage conceived by Congress to be used by U.S. intelligence agencies to collect foreign intelligence information, including:
>
> - A foreign intelligence standard instead of a criminal standard of probable cause;
> - Use of the most advanced and highly intrusive techniques for intelligence gathering; and
> - Surveillances and searches for extensive periods of time.[60]

This ruling was short-lived as the Foreign Intelligence Security Court of Review ("FISCR") reversed the decision, maintaining that "FISA . . . does not oblige the government to demonstrate to the FISA court that its primary purpose in conducting electronic surveillance is *not* criminal prosecution[.]"[61] Furthermore, the court maintained that the minimization procedures were not in direct conflict with the Fourth Amendment.[62] Moreover, despite the notion that law enforcement may use an "ends justifying the means" argument to apply warrantless searches under the special exceptions rule to the Fourth Amendment,[63] the court noted that this issue deals more with the programmatic purpose of an organization and less about the subjective intent of the actor.[64]

---

[58] *In re* All Matters Submitted to Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 620 (FISA Ct. 2002).

[59] *See* Bast & Brown, *supra* note 56, at 379.

[60] *See In re All Matters Submitted to Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d at 624.

[61] *See In re* Sealed Case No. 02-001, 310 F.3d 717, 736 (FISA Ct. Rev. 2002).

[62] *See id.* at 743, 746 ("[B]y focusing on the subjective motivation of those who initiate investigations, the *Truong* standard, as administered by the FISA court, could be thought to discourage desirable initiatives. []It is also at odds with the Supreme Court's Fourth Amendment jurisprudence which regards the subjective motivation of an officer conducting a search or seizure as irrelevant[.] . . . [W]e think the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close." (citations omitted)).

[63] *See In re Sealed Case No. 02-001*, 310 F.3d at 745 (citing Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995)).

[64] *See In re Sealed Case No. 02-001*, 310 F.3d at 745 ("[B]y 'purpose' the Court makes clear it was referring not to a subjective intent, which is not relevant in ordinary Fourth

There is the argument, however, that the court in this case "endorsed the [PATRIOT] Act amendments to FISA even in light of the amendments lowering the standard to something below probable cause."[65]

However, the court seems to hint at the notion that Fourth Amendment jurisprudence is established regarding the use of warrantless searches in typical law enforcement, but not with regards to electronic surveillance warrants for the purposes of foreign intelligence.[66] Furthermore, the court also acknowledged that most foreign intelligence gathering is in some part a "criminal investigation."[67] This presents the issue then of convenience rather than how each might semantically be different. Given the ruling of the court in this particular case, and the overall effect of the PATRIOT Act[68] and its subsequent amendments,[69] it would seem that obtaining a FISA warrant in criminal investigations would be significantly easier than obtaining a traditional warrant from a criminal court judge.[70] Nevertheless, the court argued heavily for FISA's ability to somewhat meet the burden of contemporary Fourth Amendment jurisprudence, regardless of minor differences between FISA and Title III requirements.[71]

The court, however, argued that criminal law and foreign intelligence procedure and jurisprudence are quite different, despite

---

Amendment probable cause analysis, but rather to a programmatic purpose.").

[65] *See* Bast & Brown, *supra* note 56, at 380.

[66] *See In re Sealed Case No. 02-001*, 310 F.3d at 744 (quoting United States v. United States Dist. Court, 407 U.S. 297, 321–22 (1972)).

[67] *See In re Sealed Case No. 02-001*, 310 F.3d at 743 (quoting United States v. Truong Dinh Hung, 629 F.2d 908, 915 (4th Cir. 1980)).

[68] *See In re Sealed Case No. 02-001*, 310 F.3d at 721.

[69] *See id.*

[70] *See* Bast & Brown, *supra* note 56, at 380–81. In addition:

> Obtaining a FISA court order may become the preferred method of conducting surveillance in criminal investigations, as the law enforcement officer seeking judicial approval need not comply with the higher standard of the Fourth Amendment. Employing FISA as the easier method for obtaining surveillance authority may result in an increase in surveillance applications under FISA, which is what has happened. Prior to the [PATRIOT] Act (years 1979 through 2001) FISC granted 14,036 surveillance orders, without rejecting any surveillance applications; thus, the court granted an average of 610 annually. After the [PATRIOT] Act through 2012, FISC granted 19,906 surveillance orders and rejected eleven surveillance applications; thus, the court granted an average of 1,809 annually, amounting to a nearly 300 percent growth over the first twenty-three years.

Id.

[71] *See In re Sealed Case No. 02-001*, 310 F.3d at 741, 742 (arguing that per significant Fourth Amendment jurisprudence regarding the Warrant Clause, the actions of obtaining a FISA warrant are not only similar to Title III requests, despite certain inherent differences, but they also resemble the same judicial scrutiny inherent in obtaining conventional warrants from criminal court judges).

their discernable overlap.[72] More specifically, the court contended that the purpose of each is entirely different, claiming that:

> The main purpose of ordinary criminal law is twofold: to punish the wrongdoer and to deter other persons in society from embarking on the same course. The government's concern with respect to foreign intelligence crimes, on the other hand, is overwhelmingly to stop or frustrate the immediate criminal activity. As we discussed in the first section of this opinion, the criminal process is often used as part of an integrated effort to counter the malign efforts of a foreign power. Punishment of the terrorist or espionage agent is really a secondary objective; indeed, punishment of a terrorist is often a moot point.[73]

What the court does understand here is how the etiology of crime itself says something about the etiology of terrorism, although terrorism is in fact a crime.[74] However, what the court fails to understand is the importance of criminal law in doing more than punishing and deterring,[75] but rather, strengthening the rule of law by creating transparency and ensuring accountability of actors to the system and to society.[76] While FISA and Title III for that matter may not be inherently dissimilar from conventional criminal procedure and criminal law in scope,[77] the court argues in sum that criminal law is holistically reactive, while FISA is ostensibly proactive and in need of support for special exception.[78] Given the actuarial frame of mind that the criminal justice system (and polity) had entered into *prior to* 9/11,[79] it seems that both the criminal justice system as a whole and foreign intelligence "gatherers" are not as "at odds" as the court purports.[80] Put another way, the criminal justice system has become highly entrenched in the notion

---

[72] *See id.* at 744.

[73] *See id.* at 744–45.

[74] *See id.* at 744.

[75] *See id.* at 744–45.

[76] *See* Paul D. Carrington, *Justice on Appeal in Criminal Cases: A Twentieth-Century Perspective*, 93 MARQ. L. REV. 459, 474 (2009).

[77] *See In re Sealed Case No. 02-001*, 310 F.3d at 741–42.

[78] *See id.* at 744–45 (citing Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995)).

[79] *See* JONATHAN SIMON, GOVERNING THROUGH CRIME: HOW THE WAR ON CRIME TRANSFORMED AMERICAN DEMOCRACY AND CREATED A CULTURE OF FEAR 4 (2007); MARILYN PETERSON, BUREAU OF JUSTICE ASSISTANCE, OFFICE OF JUSTICE PROGRAMS, U.S. DEP'T OF JUSTICE, INTELLIGENCE-LED POLICING: THE NEW INTELLIGENCE ARCHITECTURE 5 (2005), https://www.ncjrs.gov/pdffiles1/bja/210681.pdf.

[80] *See* United States v. Abu-Jihaad, 630 F.3d 102, 122 (2d Cir. 2010) (quoting United States v. United States Dist. Court, 407 U.S. 297, 322 (1972)).

of national security since 9/11,[81] but more so due to the amalgamation of the military industrial complex, polity, and corporate interests,[82] rather than the existential threat that is further aggravated by this "wall" that exists.[83]

B. Materiality, Disclosure, and Limitations on the Defense in Criminal Cases

Given the discussion on the restrictions imposed by CIPA and FISA on a defendant's ability to respond to the government's case,[84] it seems that a more narrow focus on the process of disclosure of relevant evidence is required.[85] In all criminal cases, the defendant enjoys the right to hear all allegations and requisite evidence against them pursuant to the Sixth Amendment.[86] In *Jencks v. United States*,[87] the U.S. Supreme Court overturned the conviction of Clinton Jencks because the State failed to overturn evidence that was material to the defense.[88] The Court held that:

> It is unquestionably true that the protection of vital national interests may militate against public disclosure of documents in the Government's possession. This has been recognized in decisions of this Court in civil causes where the Court has considered the statutory authority conferred upon the departments of Government to adopt regulations "not inconsistent with law, for . . . use . . . of the records, papers . . . appertaining" to his department. The Attorney General has adopted regulations pursuant to this authority declaring all Justice Department records confidential and that no disclosure, including disclosure in response to subpoena, may be made without his permission.
>
> But this Court has noticed, in *United States v. Reynolds*, . . . the holdings of the Court of Appeals for the Second Circuit that, in criminal causes ". . . the Government can invoke its evidentiary privileges only at the price of letting

---

[81] *See* Mathew C. Waxman, *Police and National Security: American Local Law Enforcement and Counterterrorism after 9/11*, 3 J. NAT'L SEC. L. & POL'Y 377 (2009).

[82] *See* PETER B. KRASKA, MILITARIZING THE AMERICAN CRIMINAL JUSTICE SYSTEM: THE CHANGING ROLES OF THE ARMED FORCES AND THE POLICE 3 (2001).

[83] *See* RICHARD A. BEST JR., SHARING LAW ENFORCEMENT AND INTELLIGENCE INFORMATION: THE CONGRESSIONAL ROLE 1 (2007), https://fas.org/sgp/crs/intel/RL33873.pdf.

[84] *See* Chandran, *supra* note 4, at 1411.

[85] *See id.*

[86] *See* Greene v. McElroy, 360 U.S. 474, 496–97 (1959).

[87] Jencks v. United States, 353 U.S. 657 (1957).

[88] *See id.* at 672 (citing Roviaro v. United States, 353 U.S. 53, 60–61 (1957)).

> the defendant go free. The rationale of the criminal cases is that, since the Government which prosecutes an accused also has the duty to see that justice is done, it is unconscionable to allow it to undertake prosecution and then invoke its governmental privileges to deprive the accused of anything which might be material to his defense. . . ."[89]

The Court in *Roviaro v. United States* similarly held that the government must at times disclose informant information in order to protect the access to a fair trial for the defendant.[90] Following these two cases was the Jencks Act,[91] which regulates how inculpatory evidence should be disclosed to the defendant following direct testimony during trial.[92] After the presentation of testimony, the defendant must request the statements[93] that the government has.[94] The Jencks Act contends: "If the entire contents of any such statement relate to the subject matter of the testimony of the witness, the court shall order it to be delivered directly to the defendant for his examination and use."[95]

The Supreme Court has also ruled that withholding exculpatory evidence "violates due process where the evidence is material either to guilt or to punishment, irrespective of the good faith or bad faith of the prosecution."[96] *Giglio v. United States*[97] further extends the reach of *Brady v. Maryland*[98] by holding that the prosecution must disclose to the defense (and jury) when witnesses have accepted an agreement with the State,[99] since such information is considered material, and failing to provide said information is a violation of due process.[100] Nonetheless, while *Brady* material is required to be

---

[89] *See Jencks*, 353 U.S. at 670–71.

[90] *Roviaro*, 353 U.S. at 60–61.

[91] *See* Jencks Act, 18 U.S.C. § 3500 (2012); Memorandum from David W. Ogden, Deputy Attorney Gen., to Prosecutors, Dep't of Justice (Jan. 4, 2010), https://www.justice.gov/dag/memorandum-department-prosecutors.

[92] *See* 18 U.S.C. § 3500(b).

[93] *See id.* § 3500(b), (e) ("The term 'statement,' as used in subsections (b), (c), and (d) of this section in relation to any witness called by the United States, means—(1) a written statement made by said witness and signed or otherwise adopted or approved by him; (2) a stenographic, mechanical, electrical, or other recording, or a transcription thereof, which is a substantially verbatim recital of an oral statement made by said witness and recorded contemporaneously with the making of such oral statement; or (3) a statement, however taken or recorded, or a transcription thereof, if any, made by said witness to a grand jury.").

[94] *See id.* § 3500(b).

[95] *See id.*

[96] *See* Brady v. Maryland, 373 U.S. 83, 87 (1963).

[97] *See* Giglio v. United States, 405 U.S. 150 (1972).

[98] *See Brady*, 373 U.S. at 87.

[99] *See Giglio*, 405 U.S. at 154–55.

[100] *See id.*

produced by the prosecution,[101] Jencks Act material needs to be requested by the defense at the right time,[102] and is not subject to the rules of discovery.[103] Building on the precedent set forth in *Giglio*, the Supreme Court maintained that both exculpatory evidence and impeachment evidence are covered under *Brady*;[104] however, it ruled that materiality is determined if the nondisclosure of said evidence shows that there is a "reasonable probability" that, had the evidence been disclosed, there would have been a result[105] ostensibly relying on the language set forth in *Strickland*[106] concerning the "reasonable probability" standard.[107] *Kyles v. Whitley*[108] later contended that materiality need not be determined by the outcome of the nondisclosure, but whether or not in its absence, the defense received a fair trial.[109]

Rule 16 of the Federal Rules of Criminal Procedure[110] outlines the process of discovery during trial[111] and which forms of information

---

[101] *See* United States v. Hanna, 55 F.3d 1456, 1459 (9th Cir. 1995) (citing *Brady*, 373 U.S. at 87–88).

[102] *Hanna*, 55 F.3d at 1459 ("*The burden rests upon the defendant* to invoke the statute at the appropriate time. . . . 'No ritual of words' is required, but the defendant must plainly tender to the Court the question of the producibility of the document *at a time when it is possible for the Court to order it produced*, or to make an appropriate inquiry. If he fails to do so he may not assert, on appeal, that failure to order production or to undertake further inquiry was error. . . . The responsibility for fairly directing the attention of the Court to the precise demand submitted for the Court's determination is appropriately placed upon the Defendant, who seeks the statute's benefits." (quoting United States v. Burke, 506 F.2d 1165, 1168 (9th Cir. 1974))). In addition, "[t]he district court may not require the government to produce Jencks Act material relating to one of its witnesses until after the witness has testified." United States v. Lewis, 35 F.3d 148, 151 (4th Cir. 1994).

[103] *See* Jencks Act, 18 U.S.C. § 3550(a) (2012) ("In any criminal prosecution brought by the United States, no statement or report in the possession of the United States which was made by a Government witness or prospective Government witness (other than the defendant) shall be the subject of subpoena, discovery, or inspection until said witness has testified on direct examination in the trial of the case.").

[104] *See* United States v. Bagley, 473 U.S. 667, 676 (1985) (citing *Giglio*, 405 U.S. at 153–54; *Brady* 373 U.S. at 87; Naupue v. Illinois, 360 U.S. 264, 269 (1959)).

[105] *See Bagley*, 473 U.S. at 682.

[106] *See id*. (citing Strickland v. Washington, 466 U.S. 668, 694 (1985)).

[107] *See Strickland*, 466 U.S. at 694.

[108] Kyles v. Whitley, 514 U.S. 419 (1995).

[109] *See id.* at 434 ("The question is not whether the defendant would more likely than not have received a different verdict with the evidence, but whether in its absence he received a fair trial, understood as a trial resulting in a verdict worthy of confidence."); Sonja N.Y. Kawasaki, *Uncle Ted Teaches a Lesson: The Fairness in Disclosure of Evidence Act Challenges a Flawed Exculpatory Evidence Disclosure System*, 39 U. DAYTON L. REV. 413, 416–17 (2015); Kirsten M. Schimpff, *Rule 3.8, the Jencks Act, and How the ABA Created a Conflict Between Ethics and the Law on Prosecutorial Disclosure*, 61 AM. U. L. REV. 1729, 1731, 1732–33, 1734 (2012) (discussing *Kyles*, *Bagley*, *Giglio*, *Brady*, and prosecutorial obligations).

[110] FED. R. CIV. P. 16.

[111] *See, e.g.*, FED. R. CIV. P. 16(a)(1)(A).

the prosecution is required to present to the defense,[112] taking into account the differences with Jencks Act material as well.[113] Similarly, and almost identical to the Jencks Act, Rule 26.2 of the Federal Rules of Criminal Procedure[114] also states the process of obtaining witness statements material to the defense.[115] Concomitantly, attorneys are guided by the American Bar Association ("ABA") Model Rules of Professional Conduct,[116] which outline professional standards that attorneys are meant to abide by—especially prosecutors—in providing material to the defense.[117] That being said, many have advocated with little success for amendments to the aforementioned Rules of Criminal Procedure to place time-restricted obligations on the prosecution concerning disclosure.[118] In general, little has been accomplished in changing prosecutorial disclosure mechanisms or expanding *Brady* in terms of criminal procedure and ethics as of late.[119] Furthermore, the constitutionality of CIPA in general has been challenged and upheld on numerous occasions.[120]

"For terrorism and other cases, CIPA is a place where the secrecy necessary to protect sources and methods collides with the transparency at the core of American justice."[121] Courts have also noted that the contextual shift from focusing on espionage cases to focusing on terrorism cases has significantly altered the character of discovery in terrorism trials.[122] For example, in *In re Terrorist*

---

[112] *See, e.g.*, FED. R. CIV. P. 16(a)(1)(B).

[113] *See, e.g.*, FED. R. CIV. P. 16(a)(2).

[114] FED. R. CIV. P. 26.2.

[115] *See* FED. R. CIV. P. 26.2(a)–(c); *see also* Jencks Act, 18 U.S.C. § 3550(a) (2012).

[116] *See Model Rules of Professional Conduct*, AM. BAR ASS'N, http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct.html (last visited Feb. 13, 2017).

[117] *See* MODEL RULES OF PROF'L CONDUCT r. 3.8(d) (AM. BAR ASS'N 1983).

[118] *See* Schimpff, *supra* note 109, at 1754 ("[P]roponents of broader and earlier disclosure have been unable to secure an amendment to Rule 16 that would guarantee full pretrial disclosure of all exculpatory and impeachment information regardless of its source (i.e., regardless of whether it may be contained in a Jencks Act witness statement, as is often the case), and are unlikely to reach this outcome in the foreseeable future.").

[119] *See, e.g., id.* at 1758 (discussing how attempts at altering the Jencks Act, the ABA Model Rules, specifically Rule 3.8, and the Federal Rules of Criminal Procedure have failed over the past decade or so).

[120] *See, e.g.*, United States v. Wilson, 721 F.2d 967, 976 (4th Cir. 1983); United States v. Drake, 818 F. Supp. 2d 909, 913 (D. Md. 2011); United States v. Hashmi, 621 F. Supp. 2d 76, 80 (S.D.N.Y. 2008); United States v. Yunis, 924 F.2d 1086, 1094–95 (D.C. Cir. 1991).

[121] Radsan, *supra* note 23, at 439.

[122] *See* Chandran, *supra* note 4, at 1412, 1416. The author argues that there is a need for:

> [A]n offense-specific CIPA, whereby the procedural mechanisms of the statute are tailored to the offense charged. The three core recommendations . . . are (1) inclusion of defense counsel in the discovery process and clearer standards to govern discoverability;

Bombings,[123] the court held that:

> [T]he district court must first decide whether the classified information the [g]overnment possesses is discoverable. If it is, the district court must then determine whether the state-secrets privilege applies because . . . there is a reasonable danger that compulsion of the evidence will expose matters which, in the interest of national security, should not be divulged. . . . If the evidence is discoverable but the information is privileged, the court must next decide whether the information is helpful or material to the defense, i.e., useful to counter the government's case or to bolster a defense . . . .[124]

Thus, if the materiality standard[125] is met, the government may withhold any information it requires.[126] However, others claim that regardless of how "confidential" the evidence may be, it should still be admissible during discovery under the Federal Rules of

---

(2) a limited and qualified declassification requirement in select Foreign Intelligence Surveillance Act cases; and (3) bifurcation of admissibility hearings.

Id. at 1411.

[123] *In re* Terrorist Bombings of U.S. Embassies in E. Afr. v. Odeh, 552 F.3d 93 (2d Cir. 2008).

[124] *Id.* at 124 (quoting United States v. Aref, 533 F.3d 72, 80 (2d Cir. 2008)).

[125] The materiality standard cited in numerous CIPA cases revolves around the precedent set forth in *United States v. Stevens*. *See, e.g.*, *Odeh*, 552 F.3d at 125 (citing United States v. Stevens, 985 F.2d 1175, 1180 (2d Cir. 1993)). Specifically:

> To the extent pertinent to the telephone records, Rule 16(a)(1) provides that upon a defendant's request, the government must permit the defendant to inspect and copy papers and documents in its possession, custody, or control, "which are material to the preparation of the defendant's defense or are intended for use by the government as evidence in chief at the trial."

Stevens, 985 F.2d at 1179–80 (quoting FED. R. CRIM. P. 16(a)(1)(C)). *Stevens* also established that:

> Evidence that the government does not intend to use in its case in chief is material if it could be used to counter the government's case or to bolster a defense; information not meeting either of those criteria is not to be deemed material within the meaning of the Rule merely because the government may be able to use it to rebut a defense position. Nor is it to be deemed material merely because it would have dissuaded the defendant from proffering easily impeached testimony. An appellate court, in assessing the materiality of withheld information, considers not only the logical relationship between the information and the issues in the case, but also the importance of the information in light of the evidence as a whole. To warrant a new trial, "[t]here must be some indication that the pretrial disclosure of the disputed evidence would have enabled the defendant significantly to alter the quantum of proof in his favor."

Stevens, 985 F.2d at 1180 (citations omitted).

[126] *See Odeh*, 552 F.3d at 124 (citing *Aref,* 533 F.3d at 80). "To be helpful or material to the defense, evidence need not rise to the level that would trigger the Government's obligation under *Brady* . . . to disclose exculpatory information." *Aref,* 533 F.3d at 80 (citing Brady v. Maryland, 373 U.S. 83, 87 (1963)).

Evidence.[127] Nonetheless, "national security" was operationalized quite broadly within the scope of CIPA.[128] This makes the task of balancing the defendant's rights over the state's almost insurmountable. Despite judges acknowledging the inherent paradox of not being able to show what information may be *material* without having viewed its nature,[129] the disclosure of classified information under CIPA is still subject to a higher standard of materiality.[130] Overall, § 5 and § 6 of CIPA govern the introduction and use of classified evidence by the defendant.[131] However, some evidence suggests that irrespective of the hurdles of proving materiality, CIPA itself protects against certain abuses:

> Section 5(a) of CIPA requires the defendant to notify the court and the prosecutor about any classified information he reasonably expects to disclose at trial. Under § 6(a), the United States may then request a hearing for the court to determine the "use, relevance, or admissibility of classified information that would otherwise be made during the trial or pretrial proceeding." If the court authorizes disclosure of the information under § 6(a), the United States may move that the court order either a substitute statement admitting relevant facts . . . or a substitute summary of specific classified information . . . . Section 6(c)(1) states that the court "shall grant such a motion . . . if it finds that the statement or summary will provide the defendant with substantially the same ability to make his defense as would disclosure of the specific classified information." If the court denies the substitution motion under § 6(c)(1), the Attorney General is authorized to submit an affidavit to the court barring disclosure of the classified information . . . in which case the court must fashion an appropriate remedy, ranging from dismissal of the indictment to preclusion of

---

[127] *See* Ellen Yaroshefsky, *Lawyers' Ethics in an Adversary System: Secret Evidence is Slowly Eroding the Adversary System: CIPA and FISA in the Courts*, 34 HOFSTRA L. REV. 1063, 1069 n.26 (2006) ("CIPA concerns both discovery of classified information and its admissibility at trial. There is abundant case law that the classified nature of the evidence should not affect the determination of its disclosure and admissibility, thus the traditional materiality and relevance discovery standard . . . should be applicable.").

[128] *See* Classified Information Procedures Act, 18 U.S.C. app. § 1(b) (2012). "'National security,' as used in this Act, means the national defense and foreign relations of the United States." *Id.*

[129] *See* United States v. Yunis, 867 F.2d 617, 624 (D.C. Cir. 1989).

[130] *See id.*

[131] *See* 18 U.S.C. app. §§ 5, 6.

testimony . . . .[132]

Section 5 requires that the defendant be explicit in his or her designation of the classified information that will be used at trial.[133] Furthermore, failing to disclose such information would result in it being excluded from trial altogether.[134] Section 6 governs the response to the initial disclosure by enabling the government to interdict, alter, or allow the use of such information.[135] In doing so, the government is allowed to submit a motion for a determination hearing concerning the "use, relevance, or admissibility" of the information.[136] Subsequently, any hearing regarding the admission of classified information at trial or in pretrial proceedings will be held *in camera* once it is certified by the Attorney General that classified information will be disclosed during such proceedings.[137] However, prior to the hearing, the government is tasked with providing notice to the defendant of the issues surrounding the use of classified information in a specific manner, if the defendant already knows such information.[138] When such information has not been made available to the defendant, the government can describe such information in "generic" fashion or in a manner that the court approves.[139] Nonetheless, the court, at the request of the defendant, can order the government to provide more information or specificity concerning the issues at hand if it is needed to provide the defendant with fair notice.[140]

If the court does approve this requested disclosure of classified information, the government may then attempt to have the court order the substitution of said information in the form of a statement demonstrating relevant facts[141] or a summary of the information instead.[142] Again, a hearing *in camera* at the request of the government may require the court to support such attempts if the government demonstrates that substitution still enables the defendant to make his or her defense in the same capacity.[143] Each

[132] United States v. Fernandez, 913 F.2d 148, 151 (4th Cir. 1990) (quoting 18 U.S.C. app. § 6(e)(2)).
[133] 18 U.S.C. app. § 5(a).
[134] *Id.* § 5(b).
[135] *See id.* §§ 6(c), (d), (f).
[136] *Id.* § 6(a).
[137] *Id.*
[138] *Id.* § 6(b)(1).
[139] *Id.*
[140] *Id.* § 6(b)(2).
[141] *Id.* § 6(c)(1)(A).
[142] *Id.* § 6(c)(1)(B).
[143] *Id.* § 6(c)(1).

of the recorded hearings—if it is determined that classified information cannot be disclosed during any of the proceedings—is sealed and retained in the event that the defendant appeals.[144] This provides a small measure of hope for defendants appealing on the grounds that the information they intended to use was material to their defense and such a substitution was inappropriate, even if the government claimed that the classified information implicated national security.[145]

In the event that the court bars the disclosure of classified information, the defendant is ordered to not disclose any such information at any time.[146] Interestingly enough, CIPA § 6(e)(2) states:

> Whenever a defendant is prevented by an order under paragraph (1) from disclosing or causing the disclosure of classified information, the court shall dismiss the indictment or information; except that, when the court determines that the interests of justice would not be served by dismissal of the indictment or information, the court shall order such other action, in lieu of dismissing the indictment or information, as the court determines is appropriate. Such action may include, but need not be limited to—
>
> (A) [D]ismissing specified counts of the indictment or information;
>
> (B) [F]inding against the United States on any issue as to which the excluded classified information relates; or
>
> (C) [S]triking or precluding all or part of the testimony of a witness.[147]

However, prior to the invocation of either § 5 or § 6, the government may draw on § 4,[148] which allows the government to delete classified information in an *ex parte*, *in camera* hearing prior to discovery.[149] Whereas the former two sections deal directly with the processes surrounding pretrial and trial activities—specifically

---

[144] *Id.* § 6(d).

[145] *See id.* §§ 6(c)(1), (2) ("[T]he United States may, in connection with a motion under paragraph (1), submit to the court an affidavit of the Attorney General certifying that disclosure of classified information would cause identifiable damage to the national security of the United States and explaining the basis for the classification of such information. If so requested by the United States, the court shall examine such affidavit *in camera* and *ex parte*.").

[146] *See id.* § 6(e)(1).

[147] *Id.* § 6(e)(2).

[148] *Id.* § 4.

[149] *See id.*

concerning the introduction and rebuttal of classified information[150]—§ 4 allows the government to go to the court *prior* to discovery to get rid of evidence that may be material to the defendant.[151] Furthermore, the court can allow the government to substitute the information with a statement of relevant facts or a summary of the classified information instead;[152] very similar to the procedures under § 5 and § 6, except that they involve both parties.[153] This is related to and in compliance with Rule 16(d)(1) of the Federal Rules of Criminal Procedure,[154] which allows for the government to determine the admissibility of evidence.[155] It has been put forward that "Congress specifically stated that CIPA was meant only as a procedural tool 'that will permit the trial judge to rule on questions of admissibility involving classified information before [the] introduction of . . . evidence in open court.'"[156] Nonetheless, Congress has provided little guidance to judges as to the manner in which classified information should be deleted, substituted, or presented in its entirety.[157] However, similar to the ruling in *Roviaro*, the U.S. Court of Appeals for the Ninth Circuit has held that judges can utilize a balancing test to decide admissibility of evidence when national security is at stake.[158] While not explicitly mentioned, this seemingly comports with the intentions of CIPA.[159]

---

[150] *See id.* §§ 5, 6.

[151] *Id.* § 4.

[152] *Id.*

[153] *Id.* ("The court, upon a sufficient showing, 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, 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. 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 alone. If the court enters an order granting relief following such an *ex parte* showing, the entire text of the statement of the United States shall be sealed and preserved in the records of the court to be made available to the appellate court in the event of an appeal.").

[154] FED. R. CRIM. P. 16(d)(1).

[155] *See* FED. R. CRIM. P. 16(d)(1), (2).

[156] 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); *see* H.R. CONF. REP. NO. 96-1436, at 12 (1980), *reprinted in* 1980 U.S.C.C.A.N. 4307, 4310 (explaining that the conference substitute is not intended to change the existing standards for determining relevance and admissibility); H.R. REP. NO. 96-831, pt. 1, at 11 (1980) ("The bill does not alter the existing rules or standards for making the substantive determination of whether the particular information is admissible in a criminal trial.").

[157] Reid, *supra* note 156, at 280–81.

[158] *See, e.g.,* United States v. Sarkissian, 841 F.2d 959, 965 (9th Cir. 1988); *see also* Roviaro v. United States, 353 U.S. 53, 62 (1957).

[159] *See* S. REP. NO. 96-823, at 1 (1980), *reprinted in* 1980 U.S.C.C.A.N. 4294, 4329–30; *but*

It seems like the "interests of justice" are always at stake in the post-9/11 world, which is contextually different from the era when "graymailing" would have precluded the prosecution from moving forward due to this language.[160] Nonetheless, one could make the argument that admissibility and materiality are unblemished by CIPA in practice and on paper.[161] On another note, one could see how the complex interplay with FISA could complicate the matter as well.[162]

It remains unclear as to how damning CIPA may actually be in precluding defendants from accessing exculpatory or even material information.[163] However, some go so far as to state that when information and evidence is submitted *ex parte*, or when redacted or summarized documents are used, there is a loss of context that is essential to the defendant's case.[164] Since "national security" can legitimately mean almost anything within the auspices of CIPA, a defendant's procedural rights may fall by the wayside like so many other civil liberties have in times of national emergency.[165] However, many of the cases involving CIPA may not have anything to do with the gravity of national security claims—as was evident in times of war—but instead are used as loopholes by prosecutors to withhold information from the defense.[166] However, the State has the dual responsibility of providing security to its citizens and upholding the very liberties it is attempting to usurp when CIPA is invoked.[167] The Court has recognized this paradox prior to both CIPA and FISA:

see id. at 4303 ("[T]he court should not balance the national security interests of the government against the rights of the defendant to obtain the information.").

[160] *See* Justin Florence & Matthew Gerke, *National Security Issues in Civil Litigation: A Blueprint for Reform* 5, 8 (Series on Counterterrorism & Am. Statutory Law, Working Paper, 2008).

[161] *See* United States v. Wilson, 586 F. Supp. 1011, 1013 (S.D.N.Y. 1983) ("Under CIPA, in making its rulings on admissibility, the Court is to disregard the fact that certain material may be classified."); United States v. Collins, 720 F.2d 1195, 1199 (11th Cir. 1983) ("CIPA appears premised upon the assumption that, if material to the defense and not otherwise avoidable, such information shall be admissible.").

[162] *See* Yaroshefsky, *supra* note 127, at 1085–86.

[163] *See* Rosa Brooks, *The Trickle-Down War*, 32 YALE L. & POL'Y REV. 583, 594 (2014).

[164] *See id.*

[165] *See* Yaroshefsky, *supra* note 127, at 1068. There is a long history of the government claiming that its actions were warranted by matters of national security or due to exigent circumstances. *See, e.g.*, Korematsu v. United States, 323 U.S. 214, 219–20 (1944); Yasui v. United States, 320 U.S. 115, 117 (1943); Hirabayashi v. United States, 320 U.S. 81, 100–01 (1943).

[166] *See* Yaroshefsky, *supra* note 127, at 1072, 1073.

[167] *See id.* at 1066, 1068; *see also* United States v. Reynolds, 345 U.S. 1, 12 (1953).

> [S]ince the Government which prosecutes an accused also has the duty to see that justice is done, it is unconscionable to allow it to undertake prosecution and then invoke its governmental privileges to deprive the accused of anything which might be material to his defense. Such rationale has no application in a civil forum where the Government is not the moving party, but is a defendant only on terms to which it has consented.[168]

Nonetheless, the inability for defense counsel to receive classified information precludes his or her involvement in CIPA- or FISA-related cases.[169] The DOJ has required defense attorneys to receive a security clearance prior to being retained as counsel in cases involving either CIPA or FISA mechanisms.[170] Specifically concerning terrorism cases, CIPA and FISA are both used in a significant amount of contemporary terrorism-related cases.[171] In fact, from 2001 through 2009, about twenty-two percent of all terrorism-related cases involved either CIPA or FISA.[172] Furthermore, in terrorism prosecutions where either CIPA or FISA was present, there was approximately an eighty-nine percent conviction rate of at least one charge.[173] While these numbers may be somewhat underwhelming, terrorism and national security-related cases went to trial approximately ten times more often than conventional crimes, as of 2011.[174] This makes the influence (and in many cases, confluence) of CIPA and FISA on terrorism-related cases all the more important. Also, both CIPA and FISA govern the use and/or collection of classified information during both the prosecution and investigation stages.[175] Consider the following:

> While use of CIPA is the most direct indication of the presence of classified information in a case, reference to the Foreign Intelligence Surveillance Act ("FISA") means that

---

[168] *Reynolds*, 345 U.S. at 12.

[169] *See id.*; Yaroshefsky, *supra* note 127, at 1070–71.

[170] *See* Yaroshefsky, *supra* note 127, at 1070.

[171] *See* CTR. ON LAW & SEC., N.Y.U. SCH. OF LAW, TERRORIST TRIAL REPORT CARD: SEPTEMBER 11, 2001–SEPTEMBER 11, 2011, at 13 (2011), http://www.lawandsecurity.org/Portals/0/Documents/TTRC%20Ten%20Year%20Issue.pdf [hereinafter 2011 TERRORIST TRIAL REPORT CARD].

[172] *See* CTR. ON LAW & SEC., N.Y.U. SCH. OF LAW, TERRORIST TRIAL REPORT CARD: SEPTEMBER 11, 2001–SEPTEMBER 11, 2009, at 27 (2010), http://www.lawandsecurity.org/Portals/0/documents/02_TTRCFinalJan142.pdf [hereinafter 2009 TERRORIST TRIAL REPORT CARD].

[173] *See id.*

[174] *See* 2011 TERRORIST TRIAL REPORT CARD, *supra* note 171, at 11.

[175] *See* 2009 TERRORIST TRIAL REPORT CARD, *supra* note 172, at 27.

> classified information was involved in the investigation. Conversations intercepted via FISA electronic surveillance and materials seized in FISA-authorized "sneak and peek" searches are initially (and sometimes remain) classified. Consequently, both CIPA and FISA indicate the presence of classified information at some point in the investigation or prosecution. . . . CIPA and FISA appear to run in pairs, presumably because FISA-generated materials are initially (and can remain) classified information, and as such are potentially the subject of CIPA procedures. The over-lap is significant although not complete, as prosecutors generally declassify FISA-generated materials (recordings and seized records) before producing them to the defense as part of pretrial discovery. Thus, FISA may be implicated without the need for CIPA proceedings. Conversely, a case may involve classified information that is not the product of FISA surveillance or searches. In those instances, CIPA will be invoked but not FISA.[176]

Thus, classified information, regardless of its origin, is highly tempered by both of these legislative mechanisms.[177] While this is not inherently a bad thing, as the prosecution and investigation of terrorism is understandably complex, it does raise some questions concerning how the prosecution is supposed to disclose these forms of classified information to the defendant during the adjudicative process.[178] This is also complicated by the fact that all classified information collected under FISA will automatically invoke CIPA if the prosecution decides to use the information to substantiate the charges,[179] or chooses to prosecute the defendant under other statutes, which do not implicate either FISA or CIPA.[180]

Some argue that the contextual shift that was evidenced in CIPA-related prosecutions, coupled with the mass over-classification of documents following 9/11, has resulted in an unequal playing field for defendants seeking access to material evidence.[181] More specifically, cases involving CIPA have transitioned from insider to outsider cases, since defendants who were formerly government

---

[176] *Id.*

[177] *See id.*

[178] *See id.* at 24.

[179] *See id.* at 26, 30 (illustrating that prosecutors should be careful when basing their cases on classified information, lest the defendant be necessarily permitted to review it).

[180] *See id.* (concerning prosecution strategies under FISA and/or CIPA).

[181] *See, e.g.*, Chandran, *supra* note 4, at 1431–32.

officials once had access to classified information whereas "outsider" defendants, including terrorists, did not.[182] This holds true even if the information the defendants seek is their own communications.[183]

Given that CIPA provides some reciprocity for defendants, in that they are entitled to the information that the government intends to use to rebut their classified information,[184] it is subject to abuse.[185] Concomitantly, the more information the government classifies, the more heinous the "notice-and-hearing obligations" for defendants become, as they must challenge the government's classification more and more.[186] The prosecution also benefits from the nonreciprocal nature of CIPA in that § 5 notices and the § 6 hearing allow the government to hear the details of the case and yet omit sections of that disclosure from the hearing.[187] In essence, the government gets to decide what rebuttal evidence will be provided based on what evidence will be admissible in court during a § 6 hearing, as opposed to providing all relevant information to the defense.[188] In combination with the rebuttal obligation that defendants are subject to under § 6, it does seem that the discovery process overall in cases involving CIPA is "unbalanced."[189]

Nonetheless, the process itself can place such a burden on defendants, substantially impacting their right to effective assistance of counsel by either the sheer amount of information that is released under FISA investigations and surveillance,[190] or by the

---

[182] *See id.* at 1432.

[183] *See id.* at 1437.

[184] *See* Classified Information Procedures Act, 18 U.S.C. app. § 6(f) (2012) ("Whenever the court determines pursuant to subsection (a) that classified information may be disclosed in connection with a trial or pretrial proceeding, the court shall, unless the interests of fairness do not so require, order the United States to provide the defendant with the information it expects to use to rebut the classified information. The court may place the United States under a continuing duty to disclose such rebuttal information. If the United States fails to comply with its obligation under this subsection, the court may exclude any evidence not made the subject of a required disclosure and may prohibit the examination by the United States of any witness with respect to such information.").

[185] *See* 2009 TERRORIST TRIAL REPORT CARD*, supra* note 172, at 24.

[186] Chandran, *supra* note 4, at 1436.

[187] *See id.*

[188] *See id.* at 1438.

[189] *See id.* ("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 [§] 6(a). Indeed, it appears that the government can satisfy its reciprocity obligations with a mere document dump, whereas the defendant must make an exhaustive disclosure. . . .").

[190] *See id.* at 1440.

fact that the government is able to maneuver around § 5 and § 6 of CIPA in an effort to use the information presented under § 5 motions to discern its response.[191] Furthermore, the government can use classification schemes to mask evidence that may be relevant to the defense.[192] Since FISA intercepts are classified,[193] the government can use its position to slowly declassify materials relevant to the defense.[194] Put another way, if the government chooses not to listen to, view, or in many terrorism cases, translate, intercepts, then the burden to find *Brady* material, and exculpatory evidence, is placed on the defendant.[195] Thus, many defendants seek evidence that concerns their own communications, but which is nevertheless still subject to government classification.[196]

III. TERRORISM CASE STUDY INVOLVING BOTH CIPA AND FISA

Briefly examining a terrorism-related case involving both CIPA and FISA claims or challenges will be useful in demonstrating the various issues inherent in their application and interpretation. While numerous scholars advocate for a plethora of changes to CIPA and FISA individually, looking at cases where both are applied and/or scrutinized will yield more insight into the interrelatedness of the Acts themselves, and also why they need revision within the context of terrorism cases. These revisions and recommendations will be offered in Part III. Nonetheless, an examination of *United States v. Abu-Jihaad* will provide a good baseline to examine the various components that can be altered to benefit the effectiveness of prosecuting terrorists, and the various complexity that is inherent in routine cases involving CIPA and FISA. This is not to say that this case deals with issues of clearly erroneous decisionmaking or fact finding. Rather, this analysis will give more insight into how terrorist prosecutions differ from conventional criminal cases, and despite those differences, the government can still act within the bounds of substantive and procedural rationality.

---

191 *See id.* at 1437–38.

192 *See id.* at 1436.

193 *See* 2009 TERRORIST TRIAL REPORT CARD, *supra* note 172, at 27.

194 *See, e.g.*, Chandran, *supra* note 4, at 1441.

195 *See* Joshua L. Dratel, *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, 178 (2006).

196 *See* Chandran, *supra* note 4, at 1437.

A. The Case of United States v. Abu-Jihaad

United States v. Abu-Jihaad is about a U.S. Navy signalman who was found guilty by a jury in the U.S. District Court for the District of Connecticut of having communicated national defense information.[197] The court found that the signalman had provided the movements of the U.S. Navy who were set to be deployed to the Persian Gulf in spring 2001.[198] The signalman was also found to have explained the various capabilities of each of the ships set to deploy, the formation they would be traveling in, and also their missions and vulnerabilities.[199] All of the aforementioned information was allegedly transmitted to Azzam Publications,[200] which professes jihadist and anti-American views and glorifies martyrdom.[201] This was a violation of the U.S. Code,[202] and Abu-Jihaad was given a ten-year prison sentence, accordingly.[203]

This case involves both FISA and CIPA challenges in that the defendant argued that the:

> (1) [I]nculpatory evidence obtained pursuant to the Foreign Intelligence Surveillance Act ("FISA"), should have been suppressed because (a) that statute is unconstitutional and (b) in any event, was not complied with in this case; (2) erroneous evidentiary rulings deprived him of a fair trial; (3) the trial evidence was insufficient to support conviction; and (4) the district court abused its discretion in entering protective orders pursuant to the Classified Information Procedures Act ("CIPA").[204]

IV. FISA CHALLENGES

The appellate court found that these claims had no merit and affirmed the judgment of the district court.[205] In demonstrating Abu-Jihaad's guilt, the government relied on FISA intercepts, which the defendant argued should have been suppressed due to FISA being unconstitutional.[206] Nonetheless, the court demonstrated that

---

197 United States v. Abu-Jihaad, 630 F.3d 102, 108, 111 (2d Cir. 2010).
198 *See id.* at 108, 110.
199 *See id.* at 111.
200 *See id.* at 109.
201 *See id.*
202 *See* 18 U.S.C. § 793(d) (2012).
203 *Abu-Jihaad*, 630 F.3d at 117.
204 *Id.* at 108.
205 *Id.*
206 *See id.* at 117 (arguing that FISA is a violation of the Fourth Amendment and that the

counter to Abu-Jihaad's argument that a "primary purpose" was required for the purposes of making FISA warrants constitutional, the "significant purpose" used to demonstrate probable cause following Congress' amendment to FISA via the PATRIOT Act was indeed constitutional.[207] In reviewing a warrant application, the FISC is tasked with:

> (1) . . . [Finding] probable cause to believe that the target of the requested surveillance is an agent of a foreign power; (2) to find that the application is complete and in proper form; and (3) when the target is a United States person, to find that the certifications are not "clearly erroneous."[208]

While probable cause is slightly different in the context of obtaining a warrant for electronic surveillance,[209] the language that authorizes the interception of wires and communications under the Omnibus Crime Control Act[210] enumerates what probable cause means within those contexts.[211] This comports with FISA's requirement that the government demonstrate in the warrant application via probable cause that the intelligence is intended for the surveillance of a "foreign power or an agent of a foreign power."[212] Nonetheless, the court in *Abu-Jihaad* concluded that this difference in "purpose" did not amount to a gross constitutional violation as the basic requirements of obtaining a warrant under the Fourth Amendment were satisfied, and that other courts had also ruled in favor of FISA's constitutionality.[213] The court specifically stated:

---

statute's basic requirements were not even met in this case).

[207] *Id.* at 119–20.

[208] United States v. Duggan, 743 F.2d 59, 77 (2d Cir. 1984).

[209] *See id.* at 72–73.

[210] Omnibus Crime Control and Safe Streets Act, 18 U.S.C. § 2510 (2012).

[211] Specifically:

> (3) Upon such application the judge may enter an *ex parte* order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction), if the judge determines on the basis of the facts submitted by the applicant that—(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in [§] 2516 of this chapter; (b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception . . . .

Id. § 2518(3)(a)–(b).

[212] Foreign Intelligence Surveillance Act, 50 U.S.C. § 1805(a)(2).

[213] *See* United States v. Abu-Jihaad, 630 F.3d 102, 120 (2d Cir. 2010); *see, e.g.*, United States v. Ning Wen, 477 F.3d 896, 898 (7th Cir. 2007); United States v. Damrah, 412 F.3d 618, 625 (6th Cir. 2005).

> [T]he Fourth Amendment warrant requirement demands a showing of probable cause reasonable to the purpose being pursued. Thus, identification of purpose is necessary to assess the reasonableness of the probable cause standards at issue. Where multiple purposes are significant to an investigation, however, the Fourth Amendment does not require the government to identify a primary purpose or limit its ability to secure a warrant to satisfaction of the standards for that purpose. Rather, the government may secure a warrant under the probable cause standards applicable to any purpose that it pursues in good faith.[214]

Furthermore, the court said that the main concern that Abu-Jihaad raised regarding the need for a "primary purpose" was premised on restricting the executive branch's ability to conduct warrantless searches for the purpose of gathering foreign intelligence, which was different than in his case.[215] Moreover, the court found that when prior courts had interpreted "primary purpose" to be required, they were adhering to congressional intent, not a constitutional mandate.[216] The court also argued that conventional warrants for preventing criminal activity were qualitatively different than warrants obtained for the purposes of security intelligence, which often involved significantly different modes of communication.[217] However, this was despite the fact that Congress had encouraged cooperation amongst both law enforcement authorities and intelligence agencies.[218]

Abu-Jihaad's primary issue with the shift in language was that it could potentially enable the government to use FISA warrants for criminal investigations that required probable cause to be demonstrated pursuant to Title III.[219] Since national security investigations that rely on foreign intelligence usually involve more than one purpose,[220] the court ruled that a "significant purpose" still precluded this risk.[221] More specifically, the court clarified that:

---

[214] *Abu-Jihaad*, 630 F.3d at 120.

[215] *See id.* at 121.

[216] *See id.* at 124 (citing United States v. United States Dist. Court, 407 U.S. 297, 322 (1972)).

[217] *See Abu-Jihaad*, 630 F.3d at 121–22.

[218] *See generally* Foreign Intelligence Surveillance Act, 50 U.S.C. § 1806(k)(1) (2012) (discussing coordination of efforts between federal officers and both federal and state law enforcement to protect against actual or potential attack, sabotage, or other instances).

[219] *See Abu-Jihaad*, 630 F.3d at 127.

[220] *See id.*

[221] *See id.*

> For Fourth Amendment purposes, the critical question is not whether the executive can certify that obtaining foreign intelligence information is its 'primary' purpose, but whether it can certify that it is a bona fide purpose of the surveillance. Thus, where the executive in good faith pursues both intelligence and law enforcement purposes, it may apply for surveillance authority under either FISA or Title III, provided it satisfies the particular warrant standards of the statute invoked. A Fourth Amendment concern would arise only if the executive, without a bona fide purpose to obtain foreign intelligence information, tried to secure a warrant under the standards identified in FISA as reasonable for that purpose.[222]

In recognizing not only that FISA comports with the Fourth Amendment in criminal prosecutions, the court also implied that many times, foreign intelligence has some criminal law-related purpose.[223] However, this ostensibly conflates routine law enforcement with intelligence gathering, irrespective of their differing or overlapping purposes.[224] Related to this discussion is the ruling by the FISCR in *In re Sealed Case*, which contended that for the purposes of national security, involving law enforcement agencies—and by extension, the criminal justice system—was a good idea, and tested the assumption that:

> [T]he government seeks foreign intelligence information (counterintelligence) for its own sake—to expand its pool of knowledge—because there is no discussion of how the government would use that information outside criminal prosecutions. That is not to say that the government could have no other use for that information. The government's overriding concern is to stop or frustrate the agent's or the foreign power's activity by any means, but if one considers the actual ways in which the government would foil espionage or terrorism it becomes apparent that criminal prosecution analytically cannot be placed easily in a separate response category.[225]

This is an excellent point. Within the context of national security, both the IC and American criminal justice system are essential in

---

[222] *Id.* at 127–28.
[223] *See id.*
[224] *See id.* at 128.
[225] *In re* Sealed Case No. 02-001, 310 F.3d 717, 727 (FISA Ct. Rev. 2002).

providing that security.[226] While they may be on different sides of the "wall," so to speak, each acts with differing, but sometimes overlapping, purposes.[227] Looking at conventional criminal activity, it can be conceded that the use of FISA would be problematic, though not viable, since there is no "bona fide" purpose to obtain foreign intelligence.[228] Terrorism blurs that dividing line.[229] The court in *In re Sealed Case* argued that while this dichotomy between law enforcement and intelligence can become intertwined, the use of FISA—pursuant to its congressional design—cannot be used for the primary purpose of prosecuting crimes, even foreign intelligence crimes.[230] The court held that the "addition of the word 'significant' to [§] 1804(a)(7)(B) imposed a requirement that the government have a *measurable* foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes."[231] More importantly, the court also wrote that:

> [W]hen [the government] commences an electronic surveillance of a foreign agent, typically it will not have decided whether to prosecute the agent (whatever may be the subjective intent of the investigators or lawyers who initiate an investigation). So long as the government entertains a realistic option of dealing with the agent other than through criminal prosecution, it satisfies the significant purpose test.
>
> The important point is—and here we agree with the government—the [PATRIOT] Act amendment, by using the word 'significant,' eliminated any justification for the FISA court to balance the relative weight the government places on criminal prosecution as compared to other counterintelligence responses. If the certification of the

[226] *See, e.g.*, PETERSON, *supra* note 79, at 11–12 (discussing the importance of involving local officers in intelligence-based policing in national security).

[227] *See generally In re Sealed Case No. 02-001*, 310 F.3d at 721 (discussing the barrier between law enforcement and intelligence officials, sometimes referred to as a "wall"); John E. Branch III, *Statutory Misinterpretation: The Foreign Intelligence Court of Review's Interpretation of the "Significant Purpose" Requirement of the Foreign Intelligence Surveillance Act*, 81 N.C. L. REV. 2075, 2080 n.23 (2003) (discussing changes to FISA, made after September 11, following allegations of a "wall" between the Justice Department and criminal investigators).

[228] *See In re Sealed Case No. 02-001*, 310 F.3d at 734–35.

[229] *See id.* at 727 (discussing how foreign intelligence information can be used by both the government and for criminal prosecution, and thus, should not be separated into different categories).

[230] *See id.* at 735.

[231] *Id.* (emphasis added).

> application's purpose articulates a broader objective than criminal prosecution—such as stopping an ongoing conspiracy—and includes other potential non-prosecutorial responses, the government meets the statutory test.[232]

However, it can be argued that the new language of "measurable purpose" held by the FISCR in *In re Sealed Case* actually makes the showing of probable cause almost obsolete.[233] Thus, while the FISCR has the ability to inquire further as to the government's actual intent in obtaining foreign surveillance,[234] the government can skirt the issue by contending that the significant purpose of its operations are to obtain foreign intelligence, and then decide later to prosecute.[235] It is similar to developing probable cause to support a claim that something has occurred on the criminal level, deciding to investigate, and then prosecuting *only* after sufficient evidence has been obtained.[236] One could make the argument that there is nothing wrong with FISA being used for these purposes; especially considering how weak the dichotomy may actually be. If criminal activity were to be discovered in the course of the intelligence gathering, the agency could then seek to prosecute those crimes or disseminate that information to the proper authorities.[237] This issue was brought forward to the United States District Court for the District of Oregon in the case of *Mayfield v. United States*.[238] It

---

[232] *Id.*

[233] *See* Branch, *supra* note 227, at 2093–94 ("The Court of Review, however, went too far in its interpretation of FISA when it lowered the standard for obtaining a FISA search or surveillance order from a significant purpose to a measurable purpose. This new standard effectively allows a search or surveillance if the government asserts almost any foreign intelligence purpose for its investigation. The appropriate interpretation of the 'significant purpose' requirement in FISA lies in between the two courts' decisions. While it is sometimes necessary to disseminate information properly acquired through FISA searches and surveillances to criminal investigators, a watchful FISC is necessary to prevent abuse of the expansive surveillance powers granted under FISA.").

[234] *See id.* at 2093.

[235] *See id.* at 2085.

[236] *See Investigation*, U.S. DEP'T JUST.: OFF. U.S. ATT'YS, https://www.justice.gov/usao/justice-101/investigation (last visited Sept. 30, 2017).

[237] Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801(h)(3) (2012) ("'Minimization procedures'. . . allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes[.]").

[238] *See* Mayfield v. United States, 504 F. Supp. 2d 1023, 1032–33 (D. Or. 2007) ("[I]n criminal investigations, the government can now avoid the Fourth Amendment's probable cause requirement when conducting surveillance or searches . . . merely by asserting a desire to also gather foreign intelligence information from the person whom the government intends to criminally prosecute. The government is now authorized to conduct physical searches and electronic surveillance upon criminal suspects without first proving to an objective and neutral magistrate that probable cause exists to believe that a crime has been committed.

could be argued that this is why the court in *Abu-Jihaad* argued that under FISA, the obtainment of a warrant for the 'significant purpose' of gathering foreign intelligence was also valid under the Fourth Amendment, as it still allows for criminal prosecution so long as foreign intelligence is the 'significant purpose' as well.[239] Thus, there are a few dimensions of FISA that may need clarification or consolidation.

V. CIPA CHALLENGES

The defendant in *Abu-Jihaad* argued that the district court erred in granting the government's protective orders under § 4, and also by "considering *ex parte* whether the classified materials—submitted and reviewed *in camera*—were discoverable."[240] More specifically, the defendant argued that the appellate court should have reviewed the sealed materials in light of the district court's decision. In denying the challenges by the defendant to obtain the excluded materials,[241] the district court utilized the "relevant and helpful" standard set forth by *Yunis*.[242] This test determines the applicability of the "state secrets privilege" if the information is in fact discoverable under *Brady*.[243] The test applies when "there is 'a reasonable danger that compulsion of the evidence will expose . . . matters which, in the interest of national security, should not be divulged,' and (2) the privilege is 'lodged by the head of the department which has control over the matter, after actual personal

The government need only represent that the targeted individual was an agent of a foreign power . . . and that 'a significant purpose' of the surveillance and search is to collect foreign intelligence.").

[239] United States v. Abu-Jihaad, 630 F.3d 102, 128 (2d Cir. 2010) ("FISA's 'significant purpose' requirement, so construed, is sufficient to ensure that the executive may only use FISA to obtain a warrant when it is in good faith pursuing foreign intelligence gathering, the purpose for which that statute's warrant standards apply. The fact that the government may also be pursuing other purposes, including gathering evidence for criminal prosecution, compels no different conclusion.").

[240] *Id.* at 139.

[241] *See* United States v. Abu-Jihaad, No. 3:07CR57, 2008 U.S. Dist. LEXIS 13371, at *13 (D. Conn. 2008); United States v. Abu-Jihaad, No. 3:07CR57, 2008 U.S. Dist. LEXIS 7653, at *3 (D. Conn. 2008).

[242] *See Abu-Jihaad*, 630 F.3d at 140–41; United States v. Yunis, 867 F.2d 617, 623 (D.C. Cir. 1989) ("[C]lassified information is not discoverable on a mere showing of theoretical relevance in the face of the government's classified information privilege, [but requires that a defendant] is entitled only to information that is at least 'helpful to the defense of [the] accused[.]'" (citations omitted)); *Abu-Jihaad*, 2008 U.S. Dist. LEXIS 13371, at *8–9, *10–12; *Abu-Jihaad*, 2008 U.S. Dist. LEXIS 7653, at *6.

[243] United States v. Aref, 533 F.3d 72, 80 (2d Cir. 2008) (quoting United States v. Stevens, 985 F.2d 1175, 1180 (2d Cir. 1993)); *see* Brady v. Maryland, 373 U.S. 83, 87 (1963).

consideration by that officer.'"[244] Once it is determined that the test does apply, then the court determines if the information is helpful or material to the defense.[245]

The district court found that most of the information excluded had nothing to do with his defense and that he already had knowledge of a substantial amount of the information.[246] In the government's second motion for protective orders, the district court found that four of the six categories of information were not discoverable (because they were not helpful to the defense), but that two were.[247] However, one category of information was already provided to the defendant during actual discovery, and thus the district court maintained that it did not need to be disclosed again.[248] Regarding the second category of information that was discoverable, the court held that the government's disclosure obligations were "satisfied" via the transference of letters, FBI reports, and other materials to the defendant.[249]

Reviewing the district court's determination under an abuse of discretion standard, the circuit court found no such abuse, and actually commended the district court for its ability to adhere to CIPA.[250] Thus, the appellate court felt that Abu-Jihaad's argument—that the reviewing of materials *ex parte, in camera* was unconstitutional—was in fact supported by both CIPA and the Federal Rules of Criminal Procedure 16(d).[251] The court held that while the "government moves to withhold classified information from the defense, 'an adversary hearing with defense knowledge would defeat the very purpose of the discovery rules.'"[252]

The circuit court further maintained that "[i]nformation that is helpful or material to the defense, 'need not rise to the level that would trigger the Government's obligation under [*Brady*], to disclose exculpatory information.'"[253] Overall, the court found that:

---

[244] *Aref*, 533 F.3d at 72 (quoting United States v. Reynolds, 345 U.S. 1, 8, 10 (1953)).

[245] *See Aref*, 533 F.3d at 72 (citing *Brady*, 373 U.S. at 87).

[246] *Abu-Jihaad*, 630 F.3d at 142 ("'[M]ost of the information ha[d] nothing whatsoever to do with any issue in th[e] case or any criminal activity at all;' (b) none of the information could be deemed 'helpful or beneficial to the defense,' let alone exculpatory or impeaching; and (c) because Abu-Jihaad already had knowledge and/or possession of much of the information, its production would have been duplicative." (quoting *Abu-Jihaad*, 2008 U.S. Dist. LEXIS 7653, at *5)).

[247] *See Abu-Jihaad*, 630 F.3d at 142.

[248] *See id.*

[249] *See id.*

[250] *See id.*

[251] *See id.* at 142–43.

[252] *Id.* at 143 (quoting United States v. Aref, 533 F.3d 72, 81 (2d Cir. 2008)).

[253] *Abu-Jihaad*, 630 F.3d at 141 n.33 (quoting *Aref*, 533 F.3d at 80); *see* United States v.

the state secret privilege had been applied properly by the district court; the government had demonstrated the potential for a reasonable danger had the information been disclosed; and Abu-Jihaad was not denied any information that was helpful or material to his defense.[254]

This case did not even involve any motions to admit evidence under § 5 of CIPA, or to then make a motion to substitute that information by the government under § 6.[255] However, this case itself deals with the structural impediments that a defendant must overcome, despite claims that CIPA attempts to remedy the issue.[256] Furthermore, this puts judges in the position of advocating on behalf of the defense counsel, yet viewing the very information that counsel is precluded from seeing.[257] This position is evidenced during both *ex parte* hearings under § 4 and determination hearings under § 6.[258]

The evidence in Abu-Jihaad's case was ostensibly overwhelming.[259] Each element was shown and demonstrated beyond a reasonable doubt, and both the district and circuit courts seemingly acted "by the book" with the FISA and CIPA challenges.[260] The case overview itself yields less meaning for Abu-Jihaad's situation, and is more valuable for understanding how complex the procedural mechanisms are under both FISA and CIPA, especially in cases involving both. Moreover, when information is substituted, a defendant's ability to obtain a summary of exculpatory evidence may be skewed by the government in light of the inculpatory evidence.[261] Thus, while this

Mejia, 448 F.3d 436, 457 (D.C. Cir. 2006) ("[I]nformation can be helpful without being 'favorable' in the *Brady* sense.").

[254] *See Abu-Jihaad*, 630 F.3d at 141–43.

[255] *See id.* at 139–40.

[256] United States v. Moussaoui, 382 F.3d 453, 477 (4th Cir. 2004) ("CIPA adequately conveys the fundamental purpose of a substitution[:] to place the defendant, as nearly as possible, in the position he would be in if the classified information (here, the depositions of the witnesses) were available to him.").

[257] United States v. Amawi, 695 F.3d 457, 471 (6th Cir. 2012) ("When reviewing a district court's decision to withhold information under CIPA, this court is placed in a somewhat unfamiliar posture. Rather than neutrally deciding disputes with an open record based on the adversarial process, we must place ourselves in the shoes of defense counsel, the very ones that cannot see the classified record, and act with a view to their interests.").

[258] Classified Information Procedures Act, 18 U.S.C. app. §§ 4, 6 (2012).

[259] *See, e.g., Abu-Jihaad*, 630 F.3d at 109, 112.

[260] *See id.* at 143–44.

[261] *See* United States v. Sedaghaty, 728 F.3d 885, 905–06 (9th Cir. 2013) (dealing only with CIPA challenges, in that the defendant, who was charged with providing material support to a Chechnyan terrorist group, was provided with an inadequate substitution under § 6) ("In isolation, the characterization of the evidence may not be a sufficient basis to reject the

case only focused on § 4, this section presumably poses the most significant issues for defendants in that information may be excluded altogether during the process of discovery, whereas § 6 still allows for the exclusion and substitution of information, but relates to information already known to the defendant.[262] In sum, Abu-Jihaad's case presents a best-case scenario for how terrorists, albeit all criminals, can be prosecuted under provisions from both FISA and CIPA. This case study briefly demonstrates how several aspects of using classified information can go wrong during the prosecution of terrorists in federal court, and the hurdles placed in front of the defendant. While these obstacles are not wholly improper, and do serve a valid purpose in curbing the use of classified information in open court, the nature of CIPA and FISA as used in criminal courts depicts the criminal justice system as being the secondary rather than the primary tool in the War on Terror.

VI. WHAT SHOULD BE DONE?

So now that the obstacles and issues inherent in how "secret" evidence may be used is known, how does this relate to real-world application in terms of its impact at the policy level? Put simply, the legality of both CIPA and FISA has been disputed over and over again,[263] but why might our current situation be more or less desirable as compared to restricting the use of information under CIPA or FISA? This section provides an overview of the recommendations made by others for reforms and revisions to both CIPA and FISA, along with the recommendations that this article adopts. In essence, this article calls for FISA to be relieved of its duty as it pertains to *just* foreign intelligence, and instead embrace the fact that the "wall" between intelligence and law enforcement is forever gone, and that criminal intelligence is needed moving forward.

---

substitution. More troubling, however, is the exclusion from the summary of further information that is helpful to Seda's defense. The classified nature of the material highlights the awkward nature of our review: Seda is forced to argue for the relevance of the material without actually knowing what the classified record contains, while we know what it contains but are unable to describe it on the public record." (citing *Amawi*, 695 F.3d at 471)).

[262] *See Sedaghaty*, 728 F.3d at 904–05 (citing Roviaro v. United States, 353 U.S. 53, 60–61 (1953)).

[263] *See, e.g.,* Alan Butler, *Standing Up to* Clapper*: How to Increase Transparency and Oversight of FISA Surveillance*, 48 NEW ENG. L. REV. 55, 56 (2013); Chandra, *supra* note 4, at 1416 n.26, 1420–21, 1424, 1428 n.116.

A. FISA

Given the discussion on FISA and the overview of its application, albeit in conjunction with CIPA, there are many aspects of FISA that can be reformed.[264] Again, this is not to say that FISA is not necessary or needed. However, many have called for FISA to be updated to meet the standards of contemporary criminal justice.[265] Some of those advocating for reform have called for:

- "[I]ncreased public reporting, mandatory disclosure of FISC opinions, and more adversarial briefing at the FISC;"[266]
- Proper demonstration of probable cause in obtaining surveillance powers;[267]
- The adoption of an "inextricably intertwined" test (from *In re Sealed Case*) in place of the primary/ significant purpose test;[268]
- The "wall" between law enforcement and the IC should come down;[269] and
- The "wall" between law enforcement and the IC should be maintained and/or strengthened.[270]

Regarding the "wall" arguments, much of the necessity for the

---

[264] *See, e.g.,* Butler, *supra* note 263, at 57.

[265] *See id.* at 57, 60–61.

[266] *See id.* at 57.

[267] *See* Mayfield v. United States, 504 F. Supp. 2d 1023, 1030 (D. Or. 2007).

[268] *See generally* William Pollak, Note, *Shu'Ubiyya or Security? Preserving Civil Liberties by Limiting FISA Evidence to National Security Prosecutions*, 42 U. MICH. J.L. REFORM 221, 223 (2008). Overall, the author argues that this test would essentially restrict the admissibility of all FISA material to the prosecution of national security-related crimes, as opposed to "ordinary crimes," as cautioned in *In re Sealed Case. See id.* at 247–48, 247 n.130. The author contends that for FISA material to be admissible, the crimes prosecuted must be "inextricably intertwined" with national security matters, and that a judge must review, *in camera*, the government's proposed link between the foreign intelligence crimes and the prosecution. *See id.* at 247–48.

[269] *See generally The Dark Side of Counterterrorism*, 33 WM. MITCHELL L. REV. 1675, 1677 (2007) ("[A professor said that] *The 9/11 Commission Report* makes clear that the 'wall' between agencies must come down, though it is important to remember why those barriers were originally established. He noted that because the FBI focuses on building a case for a criminal trial, while the CIA has an institutional 'need to know,' their different missions justified the existence of the 'wall.' This would no longer work in a world where the time from planning to execution is drastically shortened. That the sharing of information between such agencies will play a key role is correct, [he] argued, but he lamented that such a change is easier to propose than to implement.").

[270] *See generally* Heath H. Galloway, *Don't Forget What We're Fighting For: Will the Fourth Amendment Be a Casualty of the War on Terror?*, 59 WASH. & LEE L. REV. 921, 931, 960–61 (2002) (discussing many of the reasons why the "wall" between law enforcement agencies and intelligence agencies was both erected and destroyed).

"wall" arose from the 1947 National Security Act[271] and the creation of the CIA, along with the rampant abuses of executive authority that then ensued.[272] Furthermore, FISA and its progeny required that this "wall" be used to protect against unnecessary executive action, and that orders be certified by a judge.[273] Nonetheless, there is also the argument that absent defense counsel review of the FISA warrant process, the prosecution is free to make decisions without the traditional adversarial check on discretion.[274] In fact, a report by the Office of the Inspector General found that reports of misconduct by the government to the Intelligence Oversight Board ("IOB") fell into these three categories: "(1) improper utilization of authorities under FISA; (2) failure to adhere to Attorney General Guidelines or implementing FBI policy; and (3) improper utilization of authorities involving National Security Letters."[275] However, reports to the IOB are classified, and if released under a Freedom of Information Act ("FOIA") request, are heavily redacted.[276]

In addition, the PATRIOT Act relaxed the requirements needed to obtain a National Security Letter ("NSL"),[277] which is an investigative order granted by an FBI official, not a judge, that requires businesses to provide electronic, billing, and telecommunications records.[278] The FBI official only has to certify that the records are for an "authorized" investigation pertaining to international terrorism.[279] Furthermore, § 215 of the PATRIOT Act also relaxed the requirements needed to obtain information under FISA.[280] Similar to the certification of NSLs, the government was also allowed to "self-certify" that the records sought were related to an authorized investigation, and § 215 greatly expanded the type of records that were subject to government access, with the only

---

[271] *See id.* at 958.

[272] *See id.* at 959.

[273] *See id.*; *see also* Foreign Intelligence Surveillance Act, 50 U.S.C. § 1805(a) (2012).

[274] *See* Joshua L. Dratel, *Section 4 of the Classified Information Procedures Act: The Growing Threat to the Adversary Process*, 53 WAYNE L. REV. 1041, 1047 (2007).

[275] OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, REPORT TO CONGRESS ON IMPLEMENTATION OF SECTION 1001 OF THE USA PATRIOT ACT 24 (2006), http://www.usdoj.gov/oig/special/s0603/final.pdf.

[276] *Id.* at 21.

[277] *See* Stephen J. Schulhofer, *The PATRIOT Act and the Surveillance Society*, *in* YOU DECIDE! CURRENT DEBATES IN CRIMINAL JUSTICE 379 (Bruce Waller ed., 2009).

[278] *See id.*

[279] *See id.*

[280] *See* Stephen J. Schulhofer, *The New World of Foreign Intelligence Surveillance*, 17 STAN. L. & POL'Y REV. 531, 548 (2006) ("[After 9/11,] Congress relaxed threshold requirements in the government's least supervised intelligence-gathering regimes—the FISA document-production order and the NSL—making these tools easier to invoke.").

difference being that access required a court order.[281]

If this doesn't seem like it could become an issue, the aforementioned Inspector General's report makes it clear that in regard to reports provided to the IOB, "[a]pproximately 54 percent . . . examined for FY 2004 and 47 percent . . . examined for FY 2005 fell into the category of improper use of FISA authorities."[282] While this only constitutes violations presented to the IOB, it does seem plausible that the issue could be larger, given the reliance on reporting.

However, in keeping in line with prior recommendations, it would be wise to allow potential and confirmed violations of FISA to be made publicly available—without all of the "red tape."[283] Even though the membership and information surrounding the IOB is technically public information, the IOB is still part of the President's Intelligence Advisory Board ("PIAB"), which is part of the Executive Office of the President of the United States.[284] The overall function of this board is to report to the President on the effectiveness and legality of foreign intelligence gathering.[285] The Privacy and Civil Liberties Oversight Board ("PCLOB") is similar but is an independent agency that focuses on the actions of the executive branch in response to terrorism and ensures that civil liberties are considered in the effort to combat terrorism.[286] Each of these boards are comprised of leading members of society that are appointed by the President to conduct analyses of executive action and adherence to requisite laws.[287]

---

[281] *See* Schulhofer, *supra* note 277, at 379–80.

[282] *See* OFFICE OF THE INSPECTOR GEN., *supra* note 275, at 27 (depicting the types of reports provided to the IOB regarding the improper use of FISA).

[283] *See, e.g.,* Philip Bump, *A Search for the Truth on Secret Courts for Surveillance—and Drones*, ATLANTIC (May 23, 2013), https://www.theatlantic.com/politics/archive/2013/05/secret-federal-courts-surveillance-drones/314952/ (describing the struggle that occurred in an attempt to get one classified ruling of the FISC made public).

[284] *See About the PIAB*, PRESIDENT'S INTELLIGENCE ADVISORY BOARD & INTELLIGENCE OVERSIGHT BOARD: OBAMA WHITE HOUSE ARCHIVES, https://obamawhitehouse.archives.gov/administration/eop/piab/about (last visited Sept. 30, 2017).

[285] *See id.*

[286] *See generally About the Board*, PRIVACY & CIV. LIBERTIES OVERSIGHT BOARD, https://www.pclob.gov/about-us.html (last visited Sept. 30, 2017). The primary purposes of the PCLOB are:

> (1) to review and analyze actions the executive branch takes to protect the nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties, and (2) to ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the nation from terrorism.

Id.

[287] *See id.*; *About the PIAB*, *supra* note 284.

An issue with IOB, though, is that it reports directly to the President, and membership is determined by the President.[288] Also, it seems that there is little communication or cooperation between these two oversight committees.[289] While they do perform different objectives, they both deal with the legality of programs and laws aimed at thwarting terrorism.[290] Cooperation between the two boards would be mutually beneficial, especially in the wake of the PCLOB's report on the legality and efficacy of the National Security Administration's ("NSA") programs under § 215 and the effectiveness of the FISC and FISCR.[291]

While § 215 and the NSA's program are outside the scope of this article, it is of note that the report concluded: "FISA does not provide a mechanism for the court to invite non-governmental parties to provide views on pending government applications or otherwise participate in FISC proceedings prior to approval of an application."[292] Furthermore, the report recommended that the government should proactively engage in classification review of FISC opinions,[293] with the added recommendation that both the government and FISC (and FISCR) should become more transparent in the dissemination of information relating to intelligence gathering and legal interpretations.[294]

This article agrees with both recommendations by the PCLOB, and adds that increased transparency, especially concerning legal interpretations, may only help the legitimacy of the FISC, which ostensibly struggles to serve as a true democratic institution due to its secretive nature. Aside from the massive amount of information that may need to be redacted, summarized, and altered, making the court more accessible to the public, especially if non-governmental organizations are able to participate in proceedings, will also bring

---

[288] *See About the PIAB*, *supra* note 284.

[289] *See* Benjamin S. Mishkin, Note, *Filling the Oversight Gap: The Case for Local Intelligence Oversight*, 88 N.Y.U. L. REV. 1414, 1435–36 (2013) (inferring that because the PIAB acts in secret, the decision to take further action on the PIAB's findings is up to the President and Attorney General, but because the PCLOB is truly independent, information sharing may be at a minimum, if not non-existent).

[290] *See About the Board*, *supra* note 286; *About the PIAB*, *supra* note 284.

[291] PRIVACY & CIV. LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 15–16 (2014), https://fas.org/irp/offdocs/pclob-215.pdf (expressing concerns over the legality and constitutionality of the NSA's § 215 bulk telephone records program and advocating for greater transparency within the FISC).

[292] *See id.* at 13–14.

[293] *See id.* at 15.

[294] *See id.*

back some of the adversarial nature that has been excluded due to the function of the court.[295]

If the government wants to get rid of the stigma that the FISC is a rubber stamp on governmental action,[296] both the IOB and PCLOB should also have authority to subpoena court documents and materials to ensure transparency, since the PCLOB currently can only request the DOJ to do so.[297] Since the FISC is not part of the criminal justice system,[298] giving an independent body subpoena power over a court that they already have the authority to investigate seems beneficial.[299] Further, making the IOB independent of the President may increase the chances of mutual benefit and cooperation between these review boards, and changes to legislation that would allow the FISC to hear non-governmental views—including the IOB and PCLOB's views—could only result in more legitimacy for all parties.[300] Such cooperation may help to preclude the possibility of misinterpretations of FISA authorities.

Among other recommendations that the PCLOB report advocated for, were to:

- Create "Special Advocates" to serve as outside counsel to FISC and FISCR matters;[301]

---

[295] *See* Butler, *supra* note 263, at 66 ("The problem of secret law is exacerbated by the limited judicial review of important constitutional and statutory issues related to modern FISA surveillance. . . . FISA does not currently provide for adversarial hearings in the FISC, even when presented with complex and novel issues.").

[296] *See* Eric Lichtblau, *In Secret, Court Vastly Broadens Powers of N.S.A.*, N.Y. TIMES (July 6, 2013), http://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html ("The FISA judges have bristled at criticism that they are a rubber stamp for the government . . . .").

[297] *See About the Board*, *supra* note 286 ("[T]he Board may request in writing that the Attorney General subpoena on the Board's behalf parties outside of the executive branch to produce relevant information.").

[298] *See* Foreign Intelligence Surveillance Act, 50 U.S.C. § 1822(c) (2012); *About the Foreign Intelligence Surveillance Court*, FOREIGN INTELLIGENCE SURVEILLANCE CT., http://www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court (last visited Sept. 30, 2017).

[299] *See, e.g.,* PRIVACY & CIV. LIBERTIES OVERSIGHT BOARD, *supra* note 291, at 8 ("The Board's examination has also included a review of the operation of the Foreign Intelligence Surveillance Court . . . .").

[300] *See, e.g., id.* at 187 ("[P]roviding an independent voice in FISC proceedings will increase public confidence in the integrity of those proceedings.").

[301] *Id.* at 17–18 ("Congress should authorize the establishment of a panel of outside lawyers to serve as Special Advocates before the FISC in appropriate cases. . . . The attorneys should be capable of obtaining appropriate security clearances and would then be available to be called upon to participate in certain FISC proceedings. . . . The role of the Special Advocate, when invited by the court to participate, would be to make legal arguments addressing privacy, civil rights, and civil liberties interests. The Special Advocate would review the government's application and exercise his or her judgment about whether the proposed surveillance or collection is consistent with law or unduly affects privacy and civil liberties interests.").

- Provide statistics and reports on the use of Special Advocates, how and when they were used, and whether they were successful in seeking FISCR review of a legal matter;[302]
- Expand the opportunities for appellate review of FISC and FISCR cases;[303]
- Expand the amount of declassified cases available to the public, with as little redacting as feasible;[304] and
- "The Attorney General should fully inform the PCLOB of the government's activities under FISA and provide the PCLOB with copies of the detailed reports submitted under FISA to the specified committees of Congress[, including] . . . the FISC decisions required to be produced under [§] 601(a)(5)."[305]

Each of these recommendations provided in the report, among others, would significantly increase the legitimacy of FISC and FISA in general, and would also give the American people the transparency they deserve. The use of independent review bodies that have authority over FISC and FISA activities, along with the aforementioned measures that provide more government transparency, are excellent modes of governmental and non-governmental checks on executive power.[306]

Nonetheless, with specific regard to FISA, it does seem undeniable that the "wall" has come down, given the rise in post-9/11 counter-terrorism legislation and the transformation of the FBI into a quasi-intelligence agency. There also has been a massive growth in the amount of Joint Terrorism Task Forces ("JTTFs") since 9/11 as well.[307] Given this context, it seems futile to preclude the introduction of FISA-related information and communications in criminal prosecutions.[308] In fact, the wall coming down may serve to bridge the gap between many of the issues both sides have faced since 9/11, along with both sides being able to capitalize on

---

[302] *Id.* at 19.
[303] *Id.* at 18.
[304] *Id.*
[305] *Id.* at 20.
[306] *See id.* at 2.
[307] *See generally Protecting America: National Task Force Wages War on Terror*, FED. BUREAU INVESTIGATION (Aug. 19, 2008), https://archives.fbi.gov/archives/news/stories/2008/august/njttf_081908 (stating that the number of JTTFs has expanded from 35 to 104 since 9/11).
[308] *See id.*

the other side's strengths. While potential abuses will always remain, allowing the use of FISA-obtained information, even pursuant to a "'significant purpose" test, does appear to aid in the prosecution of terrorists.[309] However, domestic terrorism will always outnumber international terrorism in terms of the number of incidents.[310] Thus, the application for a FISA warrant in those cases hinges on whether there are international communications or cooperation with a "foreign power."[311] Such is not as likely as in higher profile cases such as Abu-Jihaad's. Thus, FISA is less likely to be used in most terrorism prosecutions, especially considering that most are prosecuted under financially related crimes.[312]

The main issue that remains then is the application of the "probable cause" standard. Building on the conversation in Parts II and III, it seems FISA allows a lower burden of proof for a warrant as compared to a warrant obtained from a federal court under Title III, which requires probable cause to be demonstrated prior to obtainment.[313] Again, while demonstrating that there is probable cause to believe that an individual is an agent of a foreign power is less likely than a showing that there is probable cause to believe that a crime has been committed, the former standard allows law enforcement (and intelligence agencies) to circumvent Title III requirements.[314] Whereas the determination of the purpose is required to show the reasonableness of probable cause at hand, it seems that adding to—rather than repealing—the "significant purpose" standard would be more beneficial so as to not prevent the prosecution of terrorists in those cases where officers acted in good faith in obtaining a FISA warrant, and later used the information.

While the "inextricably intertwined" standard may prove useful,[315] it requires a showing that the crimes prosecuted are linked to national security matters.[316] Again, many crimes for which terrorists are prosecuted are not directly linked to national

[309] *See* Galloway, *supra* note 270, at 963–64.

[310] *See generally Crafting a Mental Profile of a Terrorist*, NPR (Aug. 17, 2005), http://www.npr.org/templates/story/story.php?storyId=4804389 (stating that domestic terrorism outnumbers international terrorism approximately seven to one).

[311] *See* Branch, *supra* note 227, at 2080.

[312] *Cf.* Scott J. Glick, *FISA's Significant Purpose Requirement and the Government's Ability to Protect National Security*, 1 HARV. NAT'L SEC. J. 87, 140 (2010) (advocating for FISA's use in cases where the only way to obtain classified information is to prosecute terrorists for financially related crimes).

[313] *See* Galloway, *supra* note 270, at 952.

[314] *See id.* at 952–53.

[315] *See* Pollak, *supra* note 268, at 256–57.

[316] *See id.* at 247–48.

security (e.g., financial crimes, tax evasion, violations of RICO, etc.).[317] A standard that is similar to the "significant purpose" standard would be a "specific purpose" standard.[318] This would require the Attorney General's Office to certify that the specific purpose of the surveillance was to obtain information needed to prosecute all crimes—including foreign intelligence and national security-related crimes—if found during the course of intelligence gathering.[319] However, this certification would also require that the Attorney General classify the "related" crimes that the individual was reasonably believed to have committed, is committing, or will commit.[320] This would make the "significant purpose(s)"—to obtain foreign and criminal intelligence—one in the same.[321] However, this standard should more closely reflect the "probable cause" standard under Title III. In sum, a statutory change would look similar to the proposed language below—in light of current FISA language—by adding to 50 U.S.C. § 1805(a)(2) and 18 U.S.C. § 2518(3)(b):

> (a) The target of the surveillance is reasonably believed to be a foreign power or an agent of a foreign power who is committing, has committed, or will commit such crimes enumerated under Title 18 of the U.S.C. against the United States government or its citizens;
>
> (b) Each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by such an agent; and
>
> (c) There is probable cause for belief that particular communications concerning that offense will be obtained through such interception(s).[322]

Also, FISA warrants would be subject to the same procedures in certifying affidavits under Title III.[323] This would bridge the gap between Title III and FISA by allowing for the prosecution of those involved in crimes that are discovered intentionally through foreign surveillance, while at the same time combining the probable cause

---

[317] *See* Glick, *supra* note 312, at 140.

[318] *See id.* at 140–41.

[319] *See id.* at 92–93, 140–41.

[320] *See id.* at 140–41; Pollak, *supra* note 268, at 226.

[321] *See* Pollak, *supra* note 268, at 223, 239, 247–48.

[322] *See* Foreign Intelligence Surveillance Act, 50 U.S.C. § 1805(a)(2)(A)–(B) (2012); Classified Information Procedures Act, 18 U.S.C. § 2518(3)(b).

[323] *See* U.S. DEP'T JUST.: OFF. U.S. ATT'YS, CRIMINAL RESOURCE MANUAL § 29(A)–(H) (2012), https://www.justice.gov/usam/criminal-resource-manual-29-electronic-surveillance-title-iii-affidavits.

standards of both Acts to remedy any confusion therein or potential arguments against (such as Abu-Jihaad's). The new standard would also allow for the use of criminal intelligence in prosecutions if discovered inadvertently through foreign surveillance via the procedures that already exist. The primary element that the new standard would do is open up FISA to be used in all criminal prosecutions, albeit only if the certification is narrowly tailored. This would get rid of any incentive to circumvent FISA by certifying that a "significant purpose" is to gather foreign intelligence, while a primary purpose may actually be prosecution. This would allow the Attorney General and requisite agencies to be held accountable per the certification, while still allowing flexibility if information was discovered inadvertently or in "good faith" during conventional foreign intelligence.

Furthermore, it would get rid of the need for foreign surveillance to be used for the 'significant purpose' of gathering intelligence, with the chance of it being used later in criminal prosecution, and instead would allow criminal prosecution, in essence, to be a "significant purpose" of gathering intelligence. This, coupled with the breaking down of the "wall," would allow law enforcement and intelligence agencies to work more closely together along with the DOJ in thwarting international crime, especially terrorism, that may be shrouded in conventional crime. Also, it would allow the Attorney General's Office to be held responsible for the certifications that it makes, in that if criminal prosecution is presumed, then it must be declared prior to obtaining a FISA warrant. These revisions would also preclude the prosecution of United States citizens unless they are involved in international crimes. Further, it would give the executive more latitude in prioritizing what crimes it may pursue, while also being transparent during the process, yet not disclosing information that is related to national security.

Overall, these alterations and recommendations from others meet the needs of globalizing justice without sacrificing more civil liberties by holding the government more accountable and making it more transparent, yet giving the executive more leeway in prosecuting crimes that negatively impact United States security. In a way, these alterations would radically change the "purpose" of FISA, in that criminal activity and subsequent prosecution would be the primary goal as opposed to just foreign surveillance as a means of informing decisionmaking. Nonetheless, these revisions would also need to be examined within the context of an international

arena because not all prosecutions and gathering of criminal intelligence is used exclusively within the American criminal justice system. As such, the DOJ and Attorney General should be prepared for the hurdles that may arise concerning criminal procedure and rules of evidence when criminal intelligence is used in other justice systems.

B. CIPA

CIPA continues to be an issue for criminal cases involving national security or intelligence information.[324] It also allows both sides—the defense and prosecution—to stake their claim to using and excluding classified information, respectively.[325] Namely, § 4 through § 6 are the basis of the headache for defendants,[326] and similar to FISA, there are also numerous recommendations provided by others to cure the headache.[327] Some of these recommendations include:

- "[I]nclusion of defense counsel in the discovery process and . . . clearer standards to govern discoverability[;]"[328]
- "[A] limited and qualified declassification requirement in select cases involving the Foreign Intelligence Surveillance Act (FISA)[;]"[329]
- "[B]ifurcation of admissibility hearings[;]"[330]
- Tests that structure the application of the "silent witness" rule or substitution of information under CIPA;[331]
- To get rid of the "silent witness" rule or substitution of information;[332] and

---

[324] *See* Chandran, *supra* note 4, at 1412–13, 1451–52.

[325] *See id.* at 1417, 1436–37.

[326] *See id.* at 1443–45, 1448.

[327] *See* Reid, *supra* note 156, at 274; Chandran, *supra* note 4, at 1413.

[328] Chandran, *supra* note 4, at 1413.

[329] *Id.*

[330] *Id.*

[331] *See* Kateland Jackson, *The Silent Witness Rule: A Secret Safeguard to the First and Sixth Amendments*, 24 GEO. MASON C.R. L. J. 325, 347–48 (2014) ("Both tests are satisfied only if the government demonstrates (1) an overriding reason for closing the trial, (2) the closure is narrowly tailored to protect that interest, (3) no reasonable alternatives to closure exist, and (4) that the use of the silent witness rule provides defendants with substantially the same ability to make their defense as would disclosure of the classified information.").

[332] *See* Stephen I. Vladeck, *Terrorism Trials and the Article III Courts after Abu Ali*, 88 TEX. L. REV. 1501, 1522, 1532 (2010) ("[T]he clear Confrontation Clause violation resulting from the trial court's use of the 'silent witness' rule shows both the settling effect of harmless

- To delineate when the prosecutor should request intelligence information that is "material" to the defendant from the intelligence community.[333]

Each of these recommendations are arguably warranted to some extent. While some are more structured than others, given the prior discussion on CIPA and its application, it would seem that balancing tests that structure the substitution of information under § 4 of CIPA, and statutorily elucidating when the prosecutor should request information "material" to the defendant from the IC, are extremely viable to CIPA. However, more important are the declassification procedures and inclusion of defense counsel in § 4 hearings.[334]

The declassification process would help alleviate the burden that is imposed on defendants under § 5,[335] who wish to disclose classified information that they already have access to.[336] This issue is further aggravated in cases where defendants are in possession of classified information because it takes the form of their own intercepts or communications, as opposed to those who used "graymailing" as a means to circumvent prosecution due to the defendant's prior knowledge of classified information.[337] This implicates the insider-outsider context previously discussed.[338] Given this distinction, this article agrees with the proposed alteration to § 1 of CIPA.[339] This alteration reads as follows:

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

error doctrine and the extent to which procedural flaws sometimes derive not from the laws but from the judges who apply them.").

[333] *See* Reid, *supra* note 156, at 297–98 (outlining certain events that trigger an obligation to search, including that the intelligence agency: is involved with the prosecution; frequently investigates on similar matters; and more); *id.* at 297 n.110 (explaining how prosecutors are already required to search for information material to the defendant's case within the IC due to the U.S. Attorneys' Criminal Resource Manual § 2502—an initiative that can possibly make prosecutors more accountable).

[334] *See* Chandran, *supra* note 4, at 1443–44, 1447.

[335] *See id.* at 1446.

[336] *See id.* ("[A]mendments would alleviate the [§] 5 notice burden by requiring the government to declassify the defendant's personal communications if . . . discoverable and do not contain [classified] content . . . . [T]he amendments mandate declassification of information that was classified solely because of method of acquisition, not content.").

[337] *See id.* at 1432.

[338] *See id.*

[339] *See* Chandran, *supra* note 4, at 1442–43.

> 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.[340]

Concomitantly, allowing defense counsel access to § 4 hearings seems like an excellent idea on the surface, but it is not without its caveats. For one, many defendants—especially in terrorism cases—like to represent themselves *pro se*.[341] This is obviously an issue that cannot be remedied. Second, defense counsel would need a security clearance.[342] In cases where private attorneys are retained, the process of obtaining security clearance is both long and arduous for the government,[343] and may hinder a defendant's right to a speedy trial.[344] Also, this process is open to abuse by the government, which seeks to forestall counsel from obtaining any information that is sensitive at all. Third, it undermines the entire purpose of an *ex parte* hearing, which is to preclude sensitive information from being used in court that is not material at all, or can be substantially summarized or substituted to protect national security efforts.[345]

But defendants need *all* information that is "material" to their case, irrespective of the sensitivity of the information.[346] FISA and CIPA together preclude defendants from having access to much of the material they need, and determining materiality is arguably best done by defense counsel.[347] However, there is still the concern that defense counsel could abuse this process by using classified information that would have been impossible to obtain following a § 4 hearing.[348] Since it is expected that defense counsel share all information with their clients, allowing them access to those hearings and then expecting them to not share the information that

---

[340] *Id.*

[341] *See* Steven A. Brick, *Self-Representation in Criminal Trials: The Dilemma of the* Pro Se *Defendant*, 59 CALIF. L. REV. 1479, 1479–80 (1971); Sharon Finegan, Pro Se *Criminal Trials and the Merging of Inquisitorial and Adversarial Systems*, 58 CATH. U. L. REV. 445, 476 (2009).

[342] *See* Chandran, *supra* note 4, at 1418.

[343] *See* Laura K. Donohue, *Terrorism Trials in Article III Courts*, 38 HARV. J.L. & PUB. POL'Y 105, 116–17 (2015).

[344] *See id.*

[345] *See* Chandran, *supra* note 4, at 1417–18.

[346] *See id.* at 1417–20.

[347] *See id.* at 1428, 1443–44.

[348] *See id.* at 1433.

was deemed immaterial or not relevant is too simplistic.

Thus, courts should require a non-disclosure agreement prior to admission to § 4 hearings for those that are cleared to attend. This non-disclosure agreement would preclude defense counsel from using any classified information that was heard during the hearing that was not material to the defendant's case. Such disclosure would result in official misconduct, which could enable the government to file criminal charges against counsel for the dissemination of classified materials and/or result in the attorney being disbarred. While defense counsel has a duty to zealously advocate for their clients,[349] and it can be conceded that allowing them admission to such hearings strengthens the adversarial process, it is not without proper disincentive.[350]

With regard to § 6 hearings that seek to curtail the information the defendant intends to use, this article adopts the revision to the section set forth in Chandran's seminal article:

> 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.[351]

This article adds only one element to this language: that such determinations made by the court be subject to objection by defense counsel in writing, and can then be used later on appeal.[352] The removal of "all" from such revision would allow redeterminations to be made later if warranted.[353] This mirrors the already established provisions that defense counsel can appeal the sealed information that is used in § 4 and § 6 hearings, but allows defense counsel to

---

[349] *See id.* at 1443–44.
[350] *See id.*
[351] *Id.* at 1448.
[352] *Cf. id.*
[353] *Cf. id.*

take a more proactive approach.[354] Again, the defendant can seek reconsideration under § 6 of the court's determination in *ex parte* proceedings.[355] Such should also be allowed in § 4 hearings, whereby the presence of defense counsel allows for the possibility of a redetermination of the court's decisions if needed later. These varying modes of *in camera*, *ex parte* sessions by defense counsel and the government seemingly create the need for a completely bifurcated hearing.[356]

When taking Abu-Jihaad's case and placing it within these new revisions, it seems plausible that even if the outcome remained unchanged, the number of challenges to CIPA and FISA might have been reduced, especially if more robust FISA declassification procedures existed along with allowing defense counsel participation during the § 4 hearing. While the court in that case maintained that including defense counsel "would defeat the very purpose of discovery rules,"[357] this article contends that inclusion still comports with discovery obligations and in fact provides the government with more protection on appeal when cases are reviewed under an abuse of discretion standard. Also, these recommendations can help insulate prosecution from potential prosecutorial misconduct claims that are directed at the total suppression of "material" evidence prior to discovery. Nonetheless, many of the aforementioned issues discussed would be ameliorated if FISA declassification and review of classification procedures were expedited and robust. Thus, while Abu-Jihaad's case was affirmed and there was no finding of procedural error or misinterpretation of CIPA or FISA,[358] the case still illuminates the difficulties that both CIPA and FISA present in the most routine terrorism and national security-related cases.

VII. CONCLUSION

Both CIPA and FISA pose numerous hurdles to the balance of order and liberty. The ever-present theme that appears throughout

---

354 Classified Information Procedures Act, 18 U.S.C. app. § 4 (2012).

355 *See id.* § 6(d).

356 *See* Chandran, *supra* note 4, at 1448–49. This was the idea presented by Chandran and is the idea that this article adopts. The author further explained that this would not be that rare, and discussed several cases in which both sides were precluded from *ex parte* proceedings under CIPA. *See id.* at 1449–50.

357 United States v. Abu-Jihaad, 630 F.3d 102, 143 (2d Cir. 2010) (citing United States v. Aref, 533 F.3d 72, 81 (2d Cir. 2008)).

358 *See id.* at 143, 144.

the criminal justice system is the struggle of said balance. In examining FISA and CIPA, there are several elements and provisions that can be altered or revised to make the process not only more just, but amenable to government action. Exceptions become expectations, and that is why allowing the government more freedom in regard to FISA can actually empower it to be more transparent and accountable throughout the process. While international crime- and terrorism-related cases may prove more difficult than traditional criminal cases in terms of applying procedure, it is always important to remember that certain mechanisms can be available to correct procedural mistakes made by judges.[359]

Overall, judicial discretion is an invaluable asset to aiding national security efforts, despite the fact that it is not flawless. The aforementioned revisions and recommendations put forth for both FISA and CIPA may serve to fill in some gaps that each presents in the adjudication of terrorists in federal courts, as well as the use of criminal intelligence in federal courts.

[359] *See generally* Vladeck, *supra* note 332, at 1504, 1505–06.