CONFLICTS IN WITHHOLDING CLASSIFIED EVIDENCE FROM CRIMINAL DEFENDANTS: LOOKING BEYOND STATUTORY COMPLIANCE IN *UNITED STATES V. DAOUD*, 755 F.3D 479, (7TH CIR. 2014)

Thomas R. Bowman*

I. INTRODUCTION

Sometimes, a seemingly mundane legal issue heard in the trial courts garners such interest that daily newspapers across the United States publicize the issue. On January 29, 2014, the *Los Angeles Times*[1] ran a story on an unexpected interlocutory order issued in federal case, *United States v. Daoud*,[2] which concerned a high-profile terrorism crime allegedly committed in Chicago, Illinois. The order was issued by the United States District Court for the Northern District of Illinois, Eastern Division, and was reversed five months later by the United States Court of Appeals for the Seventh Circuit.[3] The district court decision was mainstream newsworthy because Judge Sharon Johnson Coleman ordered the United States government to give accused domestic-terrorist, Abdel Daoud, access to evidence that had been classified "top secret"[4] by the federal government.[5] Through the discovery process, Daoud requested evidence collected against him under a surveillance warrant authorized under the Foreign Intelligence Surveillance Act of 1978 (FISA).[6] Daoud sought the classified information so he could determine whether the surveillance was constitutional under doctrine

---

* Thomas R. Bowman is a Southern Illinois School of Law alumnus (2016) and attorney with the Decatur, Illinois law firm Samuels, Miller, Schroeder, Jackson & Sly. Mr. Bowman is a Lieutenant Commander in the U.S. Navy Reserve and edited this case note while forward deployed to Combined Joint Task Force Horn of Africa located in Djibouti, Africa. Mr. Bowman thanks Associate Dean Christopher Behan for his guidance and feedback throughout the writing process.

1. Jason Meisner, *Defense in Loop Bomb Plot Case to Get Secret Terror Court Filings*, L.A. TIMES (Jan. 29, 2014), http://www.latimes.com/chi-adel-daoud-fisa-court-ruling-20140129-story.html.
2. United States v. Daoud, 755 F.3d 479 (7th Cir. 2014).
3. *Id*.
4. *Id*. at 484.
5. United States v. Daoud, No. 12 CR 723, 2014 WL 321384, at *3 (N.D. Ill. Jan. 29, 2014) *rev'd*, 755 F.3d 479 (7th Cir. 2014), *supplemented*, 761 F.3d 678 (7th Cir. 2014). Daoud was accused of attempting to detonate a weapon of mass destruction, a violation of 50 U.S.C. §2332a(a)(2)(D), and attempting to destroy a building by means of an explosive device, a violation of 50 U.S.C. § 844(i).
6. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§1801-1862 (2012); *Daoud*, 755 F.3d at 480.

established in *Franks v. Delaware*.[7] Since the surveillance warrant was considered extraordinary, the government had to justify the warrant to a FISA Court, a special court established to adjudicate FISA-related matters.[8] Typically the fact that a FISA warrant was granted remains secret and unknown to a surveillance target until the government announces its intent to use evidence during trial collected under the warrant.[9] The trial court's order was newsworthy because no court had previously allowed any defendant access to information shielded from disclosure by FISA.[10]

The government appealed the trial court order to the Seventh Circuit, which held the trial court failed to comply with FISA's plain language and committed error when it ordered the warrant's substantiating evidence released to Daoud.[11] From a statutory interpretation perspective, the Seventh Circuit made the correct decision. However, the *Daoud* concurrence highlighted FISA requirements create serious defendant rights issues because defendants, who seek a constitutionally guaranteed *Franks* hearing, must have knowledge of the evidence he or she desires to challenge in a *Franks* motion.[12] Under FISA, defendants are greatly disadvantaged because they are not allowed any FISA-protected evidence required to support a *Franks* motion.[13] Therefore, defendants may not receive full constitutional rights during FISA-involved criminal prosecutions.[14]

Judge Coleman's order provided Daoud constitutional protections consistent with the adversarial trial process. For reasons explained in this note, the United States Congress should take thorough notice of concerns raised by the *Daoud* concurrence and recognize the valid policy underpinning Judge Coleman's order. Future FISA amendments should provide adequate constitutional protections for criminal defendants seeking *Franks* hearings.

---

7. *Daoud*, 755 F.3d at 480; Franks v. Delaware, 438 U.S. 154 (1978).
8. 50 U.S.C. §§1804, 1823 (2012). FISA allows the Executive Branch to conduct searches and electronic surveillance on approved targets for the purpose of collecting foreign intelligence information. 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B) (2012). FISA actions most often include wiretapping a person's telephone conversations and email accounts. *See* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), at A1, http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html. Following initial enactment, FISA was extended to allow evidence gathered under its provisions to be used in criminal prosecutions. 50 U.S.C. §§ 1806(a), 1825(a). The search must be conducted for a "significant purpose." The threshold for "significant" is not legally defined. "That being said, it is less than what had been previously necessary when appellate courts had interpreted the original certification language to require that 'the primary purpose' of FISA surveillance be the collection of foreign intelligence information." Beryl A. Howell & Dana J. Lesemann, *FISA's Fruits in Criminal Cases: An Opportunity for Improved Accountability*, 12 UCLA J. INT'L L. & FOREIGN AFF. 145, 151 (2007). The FISA process is more fully detailed in section III of this note.
9. *See* 50 U.S.C. § 1806(c).
10. *Daoud*, 2014 WL 321384, at *3.
11. *Daoud*, 755 F.3d at 481.
12. *Id.* at 485–96 (Rovner, J., concurring).
13. *Id.*
14. *Id.*

For context, this note's Section II provides the *Daoud* case exposition. Section III provides background concerning FISA, *Franks* hearings and the Classified Information Procedures Act (CIPA). Section IV provides analysis and argument that the trial court's order was the most protective of the defendant's rights because the order respected the Sixth-Amendment Confrontation Clause, a cornerstone of the American criminal prosecutorial system. The analysis is followed by a recommendation lawmakers should consider when crafting future FISA amendments. Conclusions are provided in the final section, Section V.[15]

II. CASE EXPOSITION

In *United States v. Daoud*, the appellate court reviewed whether a defendant could legally receive classified FISA material through the discovery process following a district court's order that such material be released to the defendant.[16] The decisions rendered by both the district court and court of appeals were historic firsts in American jurisprudence, which highlight conflicts inherent to handling classified information.[17] *Daoud* contains implications that are certain to influence future cases involving classified evidence.[18]

A. Facts and Procedural Posture

On September 14, 2012, eighteen-year-old American citizen, defendant and appellee, Adel Daoud, allegedly attempted to detonate an explosive device outside a downtown Chicago bar.[19] The fake bomb, which Daoud acquired and believed to be real, was supplied to him by a Federal Bureau of Investigation (FBI) agent at the height of an investigation into Daoud's radical activities.[20] The FBI had investigated Daoud since May 2012, after discovering Daoud's radical Islam-type messages posted online.[21] Based in

15. While this note does not directly address FISA's constitutionality, constitutional concerns are recognized and this note provides recommendations that support solutions to constitutional problems. FISA's constitutionality has been widely addressed. *See generally* Ellen Yaroshefsky, *Secret Evidence is Slowly Eroding the Adversary System: CIPA and FISA in the Courts*, 34 HOFSTRA L. REV. 1063, 1067 (2006); James J. Benjamin, Jr., *In Pursuit of Justice: Prosecuting Terrorism Cases in the Federal Courts—2009 Update and Recent Developments*, 42 CASE W. RES. J. INT'L L. 267, 270–71 (2009).
16. *Daoud*, 755 F.3d at 481.
17. *Id*.
18. *Id*.
19. *Id*. at 480.
20. *Id*.
21. *Id*.

part on information gathered under approved FISA surveillance warrants, it was discovered that Daoud was planning violent Jihad[22] on American soil.[23]

Undercover FBI agents pretended to support Daoud's ideology and met with him on six occasions.[24] While gauging Daoud's commitment to his plan, an agent warned Daoud the bomb could destroy a building and kill hundreds of people.[25] Daoud's response: "that's the point."[26] In September 2012, after taking steps to detonate the fake explosive, Daoud was arrested and indicted for attempting to use a weapon of mass destruction and attempting to damage and destroy a building by means of an explosive device.[27]

Following indictment, the government notified Daoud it intended to introduce electronic surveillance-type evidence at trial, which had been collected under a FISA warrant.[28] Daoud filed a motion that sought access to the classified materials the government used in justifying its FISA warrant request.[29] Daoud's motion erroneously characterized FISA's explicit requirement for a mandatory in camera, ex parte hearing on the motion by stating the district court must conduct the FISA material review ex parte and in camera "unless 'disclosure [to the defendant] is necessary to make an accurate determination of the legality of the surveillance.'"[30]

Through two separate responses, the government contested Daoud's motion.[31] One unclassified response was heavily redacted and provided to Daoud.[32] The second response was classified and was provided to the district court only.[33] The classified response was accompanied by an affidavit from the United States Attorney General who proclaimed release of the requested information or that any adversarial hearing held relating to the information could harm the United States' national security.[34] The purported harm was detailed in a classified affidavit was signed by the FBI's Acting Assistant Director for Counterterrorism.[35]

---

22. A holy war waged on behalf of Islam as a religious duty. *Jihad Definition,* MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary/jihad (last visited Oct. 11, 2014).
23. *Daoud*, 755 F.3d at 480.
24. *Id*.
25. *Id*.
26. *Id*.
27. *Id*.
28. *Id*.
29. *Id*.
30. *Id*. at 481–82 (quoting Daoud's motion).
31. *Id*. at 481.
32. *Id*.
33. *Id*.
34. *Id*. (An affidavit from the Attorney General is required under FISA in order to trigger the mandatory ex parte, in camera evidentiary hearing).
35. *Id*.

In accordance with FISA, the trial court studied the material Daoud requested in order to determine whether the material should be released.[36] The district court acknowledged FISA's requirement to hold an in camera, ex-parte hearing before ruling on the motion. Nonetheless, without satisfying FISA's requirements, Judge Coleman ordered Daoud be given the classified information because she believed the "probable value of disclosure and the risk of nondisclosure outweigh the potential danger of disclosure to cleared counsel," because Daoud's counsel possessed a government security clearance.[37] Though the district court's order was interlocutory, such orders are immediately appealable under FISA.[38] The government appealed and asserted the trial court had incorrectly interpreted FISA requirements in granting its order.[39] Following the Seventh Circuit's unfavorable ruling, as briefly discussed above, Daoud appealed to the United States Supreme Court, which on February 23, 2015, without any explanation, denied Daoud's petition for writ of certiorari.[40]

As of September 6, 2017, a trial date had not been set for Daoud.[41] On August 25, 2016, Judge Coleman determined Daoud was "not mentally competent," and could not stand trial until found competent.[42]

B. Majority Opinion

The Seventh Circuit was tasked to determine whether the district court abused its discretion when it ordered the government to disclose information used in obtaining a FISA order to surveil Daoud.[43] The Seventh Circuit determined the district court incorrectly interpreted the FISA statute, and an ex parte, in camera hearing was absolutely required anytime the government declares harm to national security could possibly result from disclosing classified information sought by a criminal defendant.[44] The district court judge simply failed to adhere to FISA provisions.[45] The Seventh Circuit's ruling explained "[t]he judge appears to have believed that adversary

36. *Id*.
37. *Id*.
38. 50 U.S.C. § 1806(h) (2006) (Only final decisions from the district court are appealable under 28 U.S.C. § 1291).
39. *Daoud*, 755 F.3d at 481.
40. Daoud v. United States, 135 S. Ct. 1456 (2015).
41. United States v. Daoud, No. 12 CR 723 (N.D. Ill. Crim. Aug. 8, 2017) (PACER).
42. Patrick M. O'Connell, *Man Accused of Trying to Detonate Bomb in Loop Mentally Unfit for Trial: Judge*, CHI. TRIB. (Aug. 25, 2016, 1:59 PM), http://www.chicagotribune.com/news/local/breaking/ct-adel-daoud-competency-ruling-20160825-story.html.
43. Brief for Appellee at 2, United States v. Daoud, 755 F.3d 479 (7th Cir. 2014) (No. 14-1284), 2014 WL 1879055, at *1.
44. *Daoud*, 755 F.3d at 481–82.
45. *Id.* at 482.

procedure is always essential to resolve contested issues of fact."[46] However, the Seventh Circuit went beyond analyzing the trial court's statutory interpretation.

The Seventh Circuit evaluated the evidentiary information Daoud's motion requested and determined there were compelling reasons to classify the information and the surveillance did not violate FISA provisions.[47] Therefore, there would not have been any support to justify the defense's *Franks* motion and Daoud would not have met the standard to receive a *Franks* hearing anyway.[48] The Seventh Circuit reversed the trial court's order, but did not remand the case to the lower court because the FISA requirements, which direct an ex parte, in camera hearing, are so one-sidedly clear that the trial court did not need to reevaluate its decision based on the Seventh Circuit's holding.[49]

C. Concurring Opinion

There was no dissenting opinion to the three-judge panel's opinion.[50] The concurring judge, Judge Rovner, agreed the trial court failed to follow FISA and the majority holding was correct.[51] Although Judge Rovner agreed with the majority concerning the trial court's error, she wrote a lengthy concurrence that explained her concerns about the serious conflict between the defendant's constitutional rights protected in *Franks* and the government's legitimate interest in protecting national security.[52] Judge Rovner's concurrence conveyed how strongly she felt the *Franks* hearing was a "vital part of the criminal process," which is in place to test the validity and honesty behind warrant applications.[53]

Judge Rovner's concurrence also highlighted a "FISA order qualifies as a warrant for purposes of the Fourth Amendment even if it authorizes only the interception of electronic communications as opposed to a physical search."[54] The Judge stated other courts have recognized *Franks* applies to FISA warrants, and she declared the majority in *Daoud* assumed that right as well.[55]

Judge Rovner's main concern was *Franks* cannot apply to situations involving national security and suggested the legislative and executive

46. *Id.*
47. *Id.*
48. *Id.* at 483–84.
49. *Id.* at 485.
50. *Id.*
51. *Id.* (Rovner, J., concurring).
52. *Id.* at 485–96.
53. *Id.* at 489.
54. *Id.*
55. *Id.* (citing 13 federal opinions from the years 1984 to 2014).

branches, not the judiciary, must lead in taking action to correct the *Franks*-FISA incongruity.[56] Judge Rovner further recognized there are a number of ideas for amending FISA to mitigate constitutional issues inherent to the Act, but anything less than a *Franks* hearing will be less vigorous or not constitutionally acceptable.[57]

III. LEGAL BACKGROUND

FISA is the primary federal law that gave rise to issues found in *Daoud*. Even though not specifically discussed in the *Daoud* decision, the CIPA is relevant to the case because it functions as a structure for disclosure and an informed decision-making process for the government regarding classified information.[58] Both CIPA and FISA function together to protect classified information from unauthorized disclosure. FISA rules apply "whenever any motion or request is made by an aggrieved person" who is a criminal defendant in cases relating to electronic surveillance or information derived under FISA.[59] CIPA or FISA application "depends not upon the content or sensitivity of the classified material but upon how the issue is raised in the course of litigation."[60] This section discusses the contents and applicability of FISA procedures in relation to *Franks* hearings and provides general information concerning CIPA.

A. Foreign Intelligence Surveillance Act and *Franks*

FISA was enacted in 1978, two years prior to CIPA, and had the initial purpose to manage the federal government's use of electronic surveillance methods in collecting foreign intelligence information.[61] FISA was created to fill the lack of surveillance oversight that existed prior to 1978, because, up until that time, the executive branch had the unilateral, unchecked power to conduct domestic surveillance.[62] FISA mitigated unchecked power because it provided judicial and legislative branch oversight by requiring judicial approval and review of FISA surveillance applications, while congressional committees were to receive regular executive branch reports concerning the FISA program.[63]

---

56. *Id.* at 495.
57. *Id.* at 494.
58. *See* Fred Manget, *Spies, Secrets, and Security: The New Law of Intelligence: Oversight of Intelligence: Intelligence and the Criminal Law System*, 17 STAN. L. & POL'Y REV. 415, 424 (2006).
59. 50 U.S.C. § 1806(f) (2012).
60. Howell & Lesemann, *supra* note 8, at 157.
61. *Id.* at 146.
62. *Id.* at 149.
63. *Id.* at 150.

Since enactment, FISA's authority has been broadened in scope, most notably through the 2011 USA PATRIOT Act.[64] Such expansion allows the government, without probable cause, to use a wider range of surveillance techniques across a wider range of targets if the surveillance purpose is in furtherance of a "significant purpose" to collect foreign intelligence.[65] The FISA court interpreted this new power to mean intelligence gathering allowed under FISA could be used to prosecute crimes if the criminal act constituted a foreign intelligence crime.[66] The United States Foreign Intelligence Surveillance Court of Review deemed all crimes listed in FISA §1801(a)-(e) as foreign intelligence crimes.[67] Examples listed in the Act include: conducting sabotage, conducting clandestine intelligence gathering, and assuming a false identity.[68] For FISA to apply, crimes listed in the statute must have been committed on behalf of a foreign power.[69]

FISA provides evidentiary discovery provisions that are problematic for criminal defendants because FISA rules are vague and difficult to challenge.[70] Generally, FISA allows an authorized federal official to petition a specially created FISA court[71] for an order "approving electronic surveillance of a foreign power[72]or an agent of a foreign power for the purpose of obtaining foreign intelligence information."[73] A FISA surveillance authorization is a broad authorization to conduct surveillance on a target and is classified secret.[74] Criminal defendants typically do not know they were FISA surveillance targets until the government provides them notice that it plans to use evidence collected during FISA surveillance in the defendant's prosecution.[75]

FISA also makes a criminal defendant's challenge to the basis for the FISA warrant difficult. In non-FISA criminal cases, the defense is generally given unfettered access to the evidentiary basis that supported a surveillance warrant.[76] Because the defendant had access to the warrant-support evidence, he can challenge the admissibility of evidence collected under a warrant.[77] In *Franks v. Delaware*, the United States Supreme Court first recognized all

64. Yaroshefsky, *supra* note 15, at 1077.
65. *Id.*
66. *In re* Sealed Case, 310 F.3d 717, 723 (FISA Ct. Rev. 2002).
67. *Id.*
68. 50 U.S.C. § 1801(a)-(e) (2012).
69. *Id.*
70. Howell & Lesemann, *supra* note 8, at 156.
71. *See* 50 U.S.C. § 1803 (2012).
72. *Id.* § 1801 (defining terms, "foreign power" and "agent" as broad terms that cover international terrorism, also defined within the act).
73. United States v. Duggan, 743 F.2d 59, 69 (2d Cir. 1984).
74. Yaroshefsky, *supra* note 15, at 1077.
75. *Id.*; *See* 50 U.S.C. § 1806(c).
76. *See generally* Yaroshefsky, *supra* note 15, at 1077–78.
77. Franks v. Delaware, 438 U.S. 154 (1978).

criminal defendants have a constitutional right under the Fourth Amendment to judicially challenge a search warrant's legitimacy; such became known as a *Franks* motion.[78] When mounting a challenge, a *Franks* motion must be supported by evidence the warrant application was based on material misrepresentations and omissions.[79] *Franks* requires a warrant be voided and any evidence collected under the voided warrant be excluded from trial when: "(1) a defendant proves by a preponderance of the evidence that the affidavit on which the search warrant was based contained false statements that were either deliberately or recklessly made, and (2) the court determines that the remainder of the affidavit was insufficient by itself to establish probable cause."[80]

As a general matter of criminal procedure, *Franks* motions are routinely filed, but hearings on the motion are infrequently granted.[81] Obtaining a *Franks* hearing is not easy because "the defendant must make a 'substantial preliminary showing'" there was a serious problem with the warrant application process.[82] A presumption exists that a warrant application is valid and the petitioning defendant must prove specific portions of the application are false.[83] Mere allegations of negligence or the occurrence of an innocent mistake in the warrant application are not enough for a defendant to prevail at a *Franks* hearing.[84] Moreover, even if one portion of the warrant application contained dishonest information, but the rest of the application contained enough honest information to justify the warrant, the warrant will stand and no hearing will be granted.[85] *Franks* hearings are only granted when the defendant overcomes the high standard.[86]

If the government intends to use FISA-gathered evidence during trial, FISA requires the defendant receive notice of such.[87] Even after defendants receive notice, it is virtually impossible for defendants to access classified information that supported the FISA surveillance request.[88] This lack of access makes it impossible for the defendant to meet basic *Franks* hearing request requirements. Courts treat FISA-related discovery requests differently than non-FISA discovery requests for classified information.[89] Howell and Lesemann describe the mechanics of discovery under FISA:

---

78. *Id.*
79. United States v. Daoud, 755 F.3d 479, 486 (7th Cir. 2014).
80. *Id.* at 486.
81. *Id.* at 488.
82. *Id.* (quoting Franks v. Delaware, 438 U.S. 154, 155 (1978)).
83. *Id.*
84. *Id.*
85. *Id.*
86. *Id.* at 489.
87. *See* 50 U.S.C. § 1806(c) (2012) (only requiring "the Government . . . notify the aggrieved . . . that the Government intends to so disclose or so use such information.").
88. Yaroshefsky, *supra* note 15, at 1078.
89. Howell & Lesemann, *supra* note 8, at 154.

> The differences between FISA discovery rules and the rules governing discovery under CIPA or of criminal search warrants and electronic surveillance orders are stark. Judges are not permitted to disclose FISA applications, orders "or other materials" when the attorney general asserts under oath "that disclosure . . . would harm the national security." Following in camera and ex parte review, the judge may disclose portions of the FISA materials "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." In practice, however, the defendant requests disclosure, the Attorney General opposes it, and the court denies the defendant's request.[90]

Until *Daoud*, no trial court had allowed a defendant or his counsel access to a FISA warrant application.[91]

B. Classified Information Procedures Act

CIPA is a federal statute that governs classified information disclosure policies.[92] Enacted in 1980, CIPA addresses the problem of handling classified information during criminal trials.[93] CIPA aids a court's decision-making process concerning the admissibility of classified evidence; five of CIPA's sixteen sections cover every aspect of the criminal-trial process.[94] Importantly, admissibility rules found in the Federal Rules of Evidence are not replaced by CIPA provisions.[95]

CIPA defines classified information as "any information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security."[96] Federal courts have determined the executive branch is responsible, not the judiciary, for classifying information.[97] Presidential Executive Order 13,526 authorizes the executive branch to classify information so long as the information being

90. *Id*. at 156 (quoting 50 U.S.C. § 1806(f) (2000)).
91. *Daoud*, 755 F.3d at 481.
92. 18 U.S.C. app. III §§ 1-16 (2012); *see* John D. Cline & K. C. Maxwell, *Criminal Prosecutions and Classified Information*, L.A. Law., Sept. 2006, at 35.
93. *See generally* 18 U.S.C. app. III §§ 1-16.
94. *See id.* §§ 2-6.
95. United States v. Baptista-Rodriguez, 17 F.3d 1354, 1363 (11th Cir. 1994); FED. R. EVID. 402. (Relevant evidence is admissible in a case unless specifically disallowed by the United States Constitution, federal statute, other federal rules of evidence or other rules prescribed by the United States Supreme Court).
96. 18 U.S.C. app. III § 1(a).
97. United States v. Collins, 720 F.2d 1195, 1198 n.2 (11th Cir. 1983).

classified could potentially harm national security.[98] Only the executive branch has the authority to declassify and release classified information.[99]

There are three classified-information categories: (1) top secret; (2) secret; and (3) confidential.[100] Category differences concern the measure of damage that unauthorized information release could potentially cause national security.[101] A person must satisfy three requirements to access classified information: (1) possess a security clearance; (2) possess a need to know the information; and (3) have signed a non-disclosure agreement acknowledging the clearance holder's requirement to restrict disclosure of any classified information unless authorized.[102]

IV. ANALYSIS

Protecting classified information from unauthorized disclosure is of vital importance to national security. Evidence exists that "public disclosure of sensitive national security information could actually endanger lives, compromise ongoing operations, and jeopardize critical diplomatic and security arrangements with other states."[103] Although these are critical concerns, national security issues must reconcile with a criminal defendant's constitutional rights. National-security concerns aside, the district court's decision was well founded in that its order attempted to preserve Daoud's Sixth Amendment constitutional rights and the adversarial process. Unfortunately, *Daoud* demonstrates that a criminal defendant's constitutional rights are subordinate to FISA.

A. *Franks* and the Constitution

The Sixth Amendment to the United States Constitution, the Confrontation Clause, was provided to ensure English civil-law practices such as ex parte examination of prosecution witnesses or trial by affidavit would never occur in the American courtroom.[104] In 1965, the United States Supreme Court confirmed during both federal and state criminal prosecutions, "the accused shall enjoy the right . . . to be confronted with the witnesses against him."[105] In 2004, a majority opinion written by United

98. Exec. Order No. 13,526 § 3.3(b)(6), 3 C.F.R. §§ 299-300 (2009).
99. *Id.* § 3.1, 3 C.F.R. §§ 305-06.
100. *Id.* § 1.2(1)-(3), 3 C.F.R. §§ 298-99 (classifications in descending order).
101. *Id.*
102. *Id*. § 4.1(a)(1)-(3).
103. Christopher W. Behan, *Military Commissions and the Conundrum of Classified Evidence: A Semi-Panglossian Solution*, 37 S. ILL. U. L.J. 643, 671 (2013).
104. CHRISTOPHER W. BEHAN, EVIDENCE AND THE ADVOCATE: A CONTEXTUAL APPROACH TO LEARNING EVIDENCE 372 (2012).
105. Pointer v. Texas, 380 U.S. 400, 400–01 (1965).

States Supreme Court Justice Antonin Scalia specified, in interpreting the Sixth Amendment, one must remember "the principal evil at which the Confrontation Clause was directed was . . . particularly its use of ex parte examinations as evidence against the accused."[106] The *Daoud* trial court pronounced the adversarial process is critical in supporting a defendant's right to effective assistance of counsel, which is protected under the Sixth Amendment.[107]

The trial court's order simultaneously maintained the adversarial trial process and Daoud's Sixth Amendment rights.[108] To further justify its order that Daoud receive the requested evidence, the trial court rationally relied on the fact that Daoud's attorney held a top-secret security clearance.[109] When the trial court gave the government the opportunity, the government failed to make a compelling oral argument as to how a defense attorney holding a valid government security clearance may jeopardize national security if given classified material.[110]

The trial court granted Daoud's motion because the court believed "that the probable value of disclosure and the risk of nondisclosure outweigh the potential danger of disclosure to cleared counsel."[111] Providing a security-cleared defense attorney access to classified information was not a new, radical idea pioneered by Judge Coleman.[112] In a Second Circuit Court of Appeals decision, *In re Terrorist Bombings of U.S. Embassies in E. Africa*, the court asserted a defendant's constitutional rights were not violated when the trial court ordered, in accordance with CIPA, classified discovery documents be released only to persons possessing a security clearance.[113] If the court directs the government to release classified information to the defense, CIPA's language creates "a presumption that the Court possesses the authority to require defense counsel to seek security clearance before the Court will provide them with access to classified materials."[114] This idea recognizes that a security-cleared attorney does not generally constitute a risk for disclosing classified evidence.

106. Crawford v. Washington, 541 U.S. 36, 36 (2004).
107. United States v. Daoud, No. 12 CR 723, 2014 WL 321384, at *3 (N.D. Ill. Jan. 29, 2014), *rev'd*, 755 F.3d 479 (7th Cir. 2014), *supplemented by a classified opinion*, 761 F.3d 678 (7th Cir. 2014).
108. *Id*.
109. *Id.* at *2.
110. *Id.*
111. *Id*.
112. *In re* Terrorist Bombings of U.S. Embassies in E. Afr., 552 F.3d 93, 127 (2d Cir. 2008).
113. *Id*.
114. United States v. Bin Laden, 58 F. Supp. 2d 113, 118 (S.D.N.Y. 1999).

B. The Trial Court Understood Statutory Requirements

A close reading of the trial court's order reveals the judge understood FISA's hearing requirements.[115] The order's second page summarized the high points from FISA's relevant subsection[116] and specifically recognized the in camera, ex parte hearing was required when the Attorney General asserts national security is at risk if the FISA materials were released.[117] Throughout the entire three-page order, there is no indication that the trial court was confused or misled into thinking that it did not have to conduct a closed hearing.[118]

However, the Seventh Circuit declared Daoud's brief misled the trial court into approving the motion.[119] The appellate court emphasized the brief contained a cropped quotation from FISA[120] that could have caused the trial court to believe that an ex parte hearing was not necessary if "the defendant's lawyers believed disclosure necessary."[121] The Seventh Circuit postulated the trial court's thought process in deciding to direct release of the material was that because the defendant's lawyers thought disclosure necessary, then the information could be released to the defense attorney.[122] However, the trial court's order makes no indication that it relied on the condensed law provided in the defendant's brief.

In a situation where the criminal process was being treated as secondary to FISA requirements, which were already considered constitutionally suspect, Judge Coleman saw little danger in the classified evidence being misused considering the defense attorney had a security clearance. Judge Coleman, recognized an opportunity to maintain the adversarial process through Daoud's case. The judge's order remarked the clearance "would allow [the defense counsel] to examine the classified FISA application material if he were in the position of the Court or the prosecution."[123] The trial court was simply providing the defense and prosecution equal opportunities to review evidence, and in the end, to truly provide the defendant due process.

Without any material support for its supposition, the Seventh Circuit criticized the trial court's deference given defense counsel's security

115. United States v. Daoud, No. 12 CR 723, 2014 WL 321384, at *2 (N.D. Ill. Jan. 29, 2014) *rev'd*, 755 F.3d 479 (7th Cir. 2014), *supplemented by a classified opinion*, 761 F.3d 678 (7th Cir. 2014).
116. 50 U.S.C. § 1806(f) (2012) (requirements for ex parte, in camera hearings).
117. *Daoud*, 2014 WL 321384, at *2.
118. *See id.*
119. United States v. Daoud, 755 F.3d 479, 481–82 (7th Cir. 2014).
120. 50 U.S.C. § 1806(f).
121. *Daoud*, 755 F.3d at 482.
122. *Id.*
123. United States v. Daoud, No. 12 CR 723, 2014 WL 321384, at *2 (N.D. Ill. Jan. 29, 2014) *rev'd*, 755 F.3d 479 (7th Cir. 2014), *supplemented by a classified opinion*, 761 F.3d 678 (7th Cir. 2014).

clearance and asserted the defense counsel would likely disclose classified information to his client.[124] In her concurrence, Judge Rovner made a similar assumption by insisting even if defense counsel were given the classified information, a true *Franks* process would not occur because counsel would not be able to share classified information with the accused so that the information's usefulness could be validated from the defendant's perspective.[125] The inability to validate classified information through the accused limits the efficacy of the *Franks* process because counsel would not be able to confirm the evidence through the accused's perspective.[126] However, the appellate court's concern in this regard is overly cautious.

Based on the abundance of governing laws and directives, classified information handling procedures seem time tested and largely effective. With sound procedures in place, it is fair to conclude releasing classified material to a security cleared defense attorney poses little disclosure risk. When granting a security clearance, the government itself confirms to the world that it deems a cleared person trustworthy to handle classified material.[127] The standard classified information nondisclosure agreement,[128] signed by every person granted a security clearance, states in paragraph one that the signee accepts the obligations to protect classified information from unauthorized disclosure.[129] Moreover, some of the most important clauses from the nondisclosure agreement state:

> (2) I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures;
>
> (3) I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone . . . .[130]

---

124. *Daoud*, 755 F.3d at 484.
125. *Id.* at 493.
126. *Id*.
127. OFF. OF THE DIRECTOR OF NAT'L INTELLIGENCE, CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT (2013).
128. Exec. Order No. 13,526 § 4.1, 3 C.F.R. §§ 314-15 (2009), *see supra* Part III.B.
129. OFF. OF THE DIRECTOR OF NAT'L INTELLIGENCE, *supra* note 127.
130. *Id.*

The above excerpts exemplify how comprehensive, clear, and serious the twelve-paragraph, two-page nondisclosure agreement is in regards to a person's responsibilities in safeguarding classified information.[131] A cleared defense attorney that has signed the agreement indisputably knows his nondisclosure duties and the potential consequences for violating them.

Upholding a criminally accused's constitutional rights is worth the minimal risks of disclosure. It is fair to assume that a security cleared defense attorney will, in an effort to adhere to the nondisclosure agreement, likely find a clever way to use classified evidence in his client's defense without disclosing the classified information. Based on the nondisclosure agreement, the attorney also has incentive for self-preservation and would not likely subject himself to penalty for disclosing classified information when unauthorized to do so.

Anyone can postulate a number of different scenarios in which classified evidence could be compromised during a criminal trial. Alternatively, an equal number of solutions to such scenarios can be asserted. However, the best, time-honored and constitutionally tested policy is to respect the Sixth-Amendment Confrontation Clause and allow the defendant to mount an unrestricted defense.

C. Alternative to FISA Evidentiary Problems

For reasons explained above, FISA as currently enacted does not support the adversarial trial process and infringes on criminal defendants' constitutional rights. Had FISA facilitated Daoud's traditional *Franks* right, he may have had the opportunity for an adversarial hearing concerning the surveillance warrant's authorization and evidence gathered under it. In the interest of preserving a defendant's constitutional rights, Congress must recognize problems inherent to FISA and correct those problems. When Congress amends FISA in the future, it should consider the below-discussed option already in practice with one division of American jurisprudence.

Section 949 of The Military Commissions Act of 2009 (MCA 2009) provides a possible remedy to FISA constitutional problems.[132] The MCA 2009 provides for Military Commissions, which are trial courts that provide a semblance of due process to foreign fighters captured during America's war on terrorism, which has largely been fought in Afghanistan.[133] The MCA 2009 guides everything from discovery to evidentiary rules and constitutes an amalgamation of best practices found in the military's courts-martial and federal court systems, but is superior to both systems in the context of

131. *Id*.
132. The Military Commissions Act of 2009, 10 U.S.C. §§ 948(a)-950(w) (2009).
133. Behan, *supra* note 103, at 661.

handling classified information.[134] The MCA 2009 specifically states "[a]ny information [including classified information] admitted into evidence pursuant to any rule, procedure, or order by the military judge shall be provided to the accused."[135] Section 949 provides the Military Commission judge procedures for considering classified information that may be used at trial, but those procedures give the judge more latitude and do not seem as restrictive as FISA procedures.[136] Moreover, the Military Commission judge, jury members, court personnel and trial counsel must possess appropriate government security clearances so they may hear classified information presented in the courtroom.[137] This requirement allows for unencumbered discussion of the classified information without the need for special security provisions.[138] The MCA 2009 even provides for the use of protective orders that forbid persons to disclose classified information presented.[139] As emphasized in this note, FISA contains no such provisions.[140] There is something inherently wrong with a system that affords a foreign-fighter terrorist greater protections and opportunity to mount a defense than it provides an American citizen, like Daoud, who faces terrorism charges in a criminal court governed under the Constitution of the United States.

V. CONCLUSION

In the end, *Daoud* is a case about the struggle between an accused criminal's constitutional rights and efforts to preserve national security. The government did not demonstrate exactly how national security was in danger if the court provided the defendant full *Franks* rights, especially considering Daoud's attorney possessed a government security clearance. What is certain however, is that a defendant's constitutional rights are abrogated under the current FISA.

The Seventh Circuit overturned the trial court's order because the trial court undisputedly failed to observe FISA requirements. The judiciary does not have the authority to make new law when an unambiguous statute exists. Perhaps the trial court could have attacked FISA on constitutional grounds, and found in favor of Daoud. However, the trial, appellate and supreme courts left constitutional issues unanswered. Congress must enact meaningful changes to FISA to prevent future Daoud-type injustices.

---

134. *Id.* at 645–61.
135. 10 U.S.C. § 949p-1(b).
136. 10 U.S.C. §§ 949p-1 – 949p-7.
137. U.S. DEP'T OF DEF., REG. FOR TRIAL BY MIL. COMM'N 72 (2011).
138. Behan, *supra* note 103, at 670.
139. 10 U.S.C. § 949p-3.
140. Behan, *supra* note 103, at 670.

Lastly, consider that the United States Constitution gave birth to our country. There would be neither the United States nor a national security to protect without the Constitution. Constitutional provisions must be upheld in order to uphold our nation, the rule of law, and national security. We cannot ignore the very document and framework that provides for our nation and security. The government and prosecutors must innovate, while adhering to constitutional rights, to effect criminal prosecutions that involve classified evidence.