SMU | Dedman School of Law

SMU Law Review

Volume 68 | Issue 2 Article 5

January 2015

NSA and DEA Intelligence Sharing: Why it is Legal and Why Reuters and the Good Wife Got it Wrong

Melanie M. Reid
Lincoln Memorial University - Duncan School of Law

Recommended Citation
Melanie M. Reid, *NSA and DEA Intelligence Sharing: Why it is Legal and Why Reuters and the Good Wife Got it Wrong*, 68 SMU L. Rev. 427 (2015)
https://scholar.smu.edu/smulr/vol68/iss2/5

This Article is brought to you for free and open access by the Law Journals at SMU Scholar. It has been accepted for inclusion in SMU Law Review by an authorized administrator of SMU Scholar. For more information, please visit http://digitalrepository.smu.edu.

NSA and DEA Intelligence Sharing: Why it is Legal and Why Reuters and the Good Wife Got it Wrong

*Melanie Reid**

I. INTRODUCTION

EVERYONE knew about the existence and mission of the National Security Agency (NSA) prior to June 2013. The NSA was known for breaking codes and monitoring conversations in the interest of national security. However, the specifics of who was monitored and how it was accomplished remained a mystery. That is, until Edward Snowden began a blitzkrieg of disclosures as to the NSA's various methods of collection and programs analyzing both metadata[1] and content in telephone conversations and emails.

The Snowden disclosures about NSA programs led to additional media reports that the NSA is sharing intelligence information with other agencies. Specifically, Reuters in August of 2013 reported "[a] secretive U.S. Drug Enforcement Administration [DEA] unit is funneling information from intelligence intercepts, wiretaps, informants, and a massive database of telephone records to authorities across the nation to help them launch criminal investigations of Americans."[2] The article stated that Drug Enforcement Administration (DEA) agents utilize "parallel construction" to hide the original source that initiated the criminal investigation. According to the article, "[f]ederal agents are trained to 'recreate' the investigative trail to effectively cover up where the information originated."[3]

Americans imagined the worst—not only was the government illegally monitoring their phone conversations, but it was then using this informa-

* Associate Professor of Law, Lincoln Memorial University-Duncan School of Law. I want to thank the participants at the Constitutional Law Colloquium at Loyola University Chicago School of Law where I presented *The Snowden Effect: U.S. Intelligence Collection and Its Impact on Prosecutor's Discovery Obligations, the Classified Information Procedures Act, and a Defendant's Right to a Fair Trial*, a precursor to this article. I would also like to thank Lauren Mullins, JaneAnne Murray, Stephen Henderson, Bruce Beverly, Pat Laflin, and Bob Reid for their invaluable assistance on this article.

1. Metadata can "encompass everything from the nearest cell tower to the caller at the time the call was placed, to the routing information the call took to reach its recipient, and sometimes even the GPS location of a cell phone when it places a call." Brian Pascal, *How Technology Broke Privacy*, 40 No. 3 Litig. 20, at 25 (Spring 2014).

2. John Shiffman & Kristina Cooke, *Exclusive: U.S. directs agents to cover up program used to investigate Americans*, Reuters, Aug. 5, 2013 *available at* http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805.

3. *Id.*

tion to initiate criminal investigations and then cover up where and how the initial information originated. It is easy to imagine the worst when the government remains silent, and we are left to guess whether the "cover-up" is to protect classified sources and methods or to hide any illegalities.

This latest news story developed into a popular TV plot line. In one of the many lawyer TV shows, "The Good Wife," the NSA intercepts the phone calls of lead character, Alicia Florrick, after Florrick represents a client, Danny Marwat, an Arab-American translator who worked for the military as a contractor until he was accused of collaborating with the Taliban.[4] The show explains that the NSA obtained a "two-hop" Foreign Intelligence Surveillance Act (FISA) court warrant on Marwat, which allowed them to listen to Marwat, his lawyers, and his lawyers' contacts for the past two years.[5] Florrick's son later receives multiple calls from his ex-girlfriend who is distraught over their break up and whose father happens to be a politically connected Somali national and potential Hamas sympathizer.[6] This information gives the NSA the needed connection to allow for a "three-hop" warrant that supposedly will allow the NSA the ability to listen to Marwat, his lawyers, those in contact with his lawyers, and anyone they contact.[7]

A few episodes later, Florrick meets with her drug dealer client, Lemond Bishop, who asks her to be on-call on February 26th, as he may be involved in "trouble" (a drug transaction) that day.[8] On February 26th, the DEA arrests Bishop.[9] The court conducts a probable cause hearing, and the government presents a witness who testifies that she saw Bishop and others moving duffel bags filled with white packets (presumably drugs) on the 26th.[10] The episode, interestingly enough, is titled "Parallel Construction, Bitches," referring to the fact that the government had pulled the wool over the defense's eyes by creating a phony witness to cover up the NSA's involvement in the investigation without the knowledge of the judge, prosecutor, and defense counsel.[11]

With any television show, it is easy to blend fact with fiction, and boring reality be damned. What is fact and what is fiction? Is this new revelation, the "Snowden phenomenon," another sign of government misconduct and abuse of power? Or is this massive collection of platform and intelligence sharing acceptable and necessary in a technologically savvy age where law enforcement is continually playing catch-up and intelligence sharing merely levels the playing field?

---

4. *The Good Wife: The Bit Bucket* (CBS television broadcast Oct. 6, 2013); *The Good Wife: Executive Order 13224* (CBS television broadcast Nov. 6, 2011).
5. *Id.*
6. *Id.*
7. *Id.*
8. *The Good Wife: Parallel Construction, Bitches* (CBS television broadcast Mar. 9, 2014).
9. *Id.*
10. *Id.*
11. *Id.*

Our liberty and privacy interests must be balanced with the government's responsibility to protect American citizens against foreign threats and its responsibility to investigate and enforce the laws of the United States. There is no easy solution; that is why Congress, the Supreme Court, lower courts, and FISA courts constantly reevaluate this balancing act. There is clearly a need to create a system of checks and balances to ensure our government is not abusing its power. However, it is also imperative to remember these checks and balances are not meant to satisfy our own personal curiosity and instinctive need-to-know.

This article explores the constitutionality of "parallel construction," the relationship between the intelligence community and law enforcement, and whether the non-disclosure of how a criminal investigation was initiated constitutes a violation of a defendant's right to discovery pre-trial and right to a fair trial. The article first examines each investigative tool mentioned in the Reuters article[12] used to initiate investigations and analyzes the legality of doing so. Part II of this article focuses on the legality of collecting, accessing, and analyzing information gathered by the intelligence community (IC), specifically the NSA, and the subsequent disclosure of intelligence to other law enforcement entities for use in criminal investigations. Part III discusses the recent revelations that the DEA has been hiding its sources and methods used to initiate a criminal investigation and has been able to protect them from disclosure in many instances. Part IV assesses the impact of this disclosure by determining how tools typically used to initiate investigations (anonymous tips, cooperating witnesses, informants, etc.) are treated by the courts and whether they are discoverable compared to the tools recently revealed to be used by the DEA (to include domestic and foreign wiretaps, NSA intercepts, and phone log databases). Part V specifically examines the legality of the DEA's use of NSA intercepts to initiate investigations and whether this practice should be abandoned. Currently, the Classified Information Procedures Act (CIPA) is in place to prevent the discovery of classified material and protect the government's sources and methods by setting forth procedures to be used in any criminal case where classified information is at issue.[13] These procedures are said to protect against the disclosure of classified information while at the same time ensuring the defendant a right to a fair trial by having the judge in the case review the evidence *ex parte* and determine whether it should be disclosed to the defendant in redacted form (thereby fulfilling the prosecutor's discovery obligations). This article explores whether CIPA is effective and up to the task of ensuring that the defendant's concerns are taken care of while placing sufficient checks and balances on the government to ensure the DEA does not take advantage of its privilege of keeping IC information secret. I argue that the existing procedures put in place, CIPA and Federal Rule of

12. Shiffman & Cooke, *supra* note 2. The Reuters article's authors utilize internal DEA documents and PowerPoint presentations to support their conclusions.

13. 18 U.S.C. App. 3 §§ 1–16 (2012).

Criminal Procedure 16,[14] adequately protect the defendant's right to discovery and right to a fair trial. While public concerns as to the DEA's use of NSA material, which bring to the forefront the broad consequences of intelligence sharing, appear to be well-founded, the question that must be asked is whether law enforcement should be allowed to tackle proactive cases in which it attempts to prevent the crime from occurring in the first place. If so, then law enforcement needs sufficient investigatory tools and the ability to take advantage of intelligence sharing opportunities. If not, then law enforcement outside the counterterrorism context should not be included as a recipient of NSA intelligence information and intelligence sharing, and existing federal regulations that currently allow this practice should be narrower in scope.

II. THE LEGALITY OF THE DISCLOSED NSA PROGRAMS AND THE FISA PROCESS

The first questionable method mentioned in Reuters that is used to initiate DEA criminal investigations is information gathered from the IC, specifically through NSA "intercepts."[15] Therefore, it is important to evaluate the known NSA programs capable of producing valuable intelligence that can be passed to law enforcement and whether this tool is, in fact, legal.

A. THE BIRTH OF THE NSA

The NSA, one of many agencies within the U.S. intelligence community, is largely a signals intelligence (SIGINT)[16] agency that falls under the direction of the Department of Defense (DOD).[17] Established in 1952 by President Harry Truman,[18] the NSA is housed at Fort Meade, Maryland,[19] has more than 35,000 employees,[20] and is accountable for $10.8 billion, or approximately twenty percent, of the annual intelligence

14. FED. R. CRIM. P. 16.

15. Shiffman & Cooke, *supra* note 2. It is unclear whether the article is referring to metadata or the monitoring of actual conversations.

16. "SIGINT is intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons systems. SIGINT provides a vital window for our nation into foreign adversaries' capabilities, actions, and intentions." NATIONAL SECURITY AGENCY, http://www.nsa.gov/sigint/index.shtml (last visited Aug. 11, 2014).

17. *Frequently Asked Questions, Oversight*, NATIONAL SECURITY AGENCY, http://www.nsa.gov/about/faqs/oversight.shtml (last visited Aug. 11, 2014).

18. *Frequently Asked Questions, About NSA*, NATIONAL SECURITY AGENCY, http://www.nsa.gov/about/faqs/about_nsa.shtml (last visited Aug. 11, 2014).

19. *National Security Agency (NSA) Headquarters*, THE CENTER FOR LAND USE INTERPRETATION, http://clui.org/ludb/site/national-security-agency-nsa-headquarters (last visited Aug. 11, 2014).

20. Masuma Ahuja, *FAQ: What you need to know about NSA surveillance and Edward Snowden*, WASHINGTON POST, July 24, 2013, http://apps.washingtonpost.com/g/page/world/faq-what-you-need-to-know-about-nsa-surveillance-and-edward-snowden/333/.

budget.[21]

Its origins can be traced back to 1917 during World War I when Herbert O. Yardley "established America's first permanent agency to intercept foreign messages and break codes"[22] named the Cipher Bureau.[23] In order to begin gathering information, the unit persuaded the Western Union Telegraph Company to allow military intelligence to copy messages passing through the company's wires.[24] Ironically, the unit's operation was shut down in 1929 by then-Secretary of State Henry Stimson who famously stated, "[G]entlemen do not read each other's mail."[25]

In May 1949, all cryptologic activities were centralized under a national organization called the Armed Forces Security Agency (AFSA).[26] Unfortunately, the AFSA was unable to centralize communications intelligence and "largely ignored the interested civilian agencies—the Department of State, the [Central Intelligence Agency] CIA, and the [Federal Bureau of Investigation] FBI."[27] Thus, inter-agency coordination has been lacking since before NSA's inception.

In December 1951, President Harry Truman created the Brownell Committee, a panel to investigate how AFSA had failed to achieve its goals.[28] As a result of this investigation, the AFSA was re-designated and renamed the National Security Agency.[29]

"The NSA is responsible for the collection and analysis of foreign electronic intelligence and for ensuring the security of classified U.S. computer systems."[30] Its mission, as set forth in Executive Order 12333,[31] is to

---

21. *The Black Budget*, WASHINGTON POST, http://www.washingtonpost.com/wp-srv/special/national/black-budget/ (last visited June 2, 2015). The total budget for the National Intelligence Program is $52.6 billion. *Id.*

22. DAVID KAHN, THE READER OF GENTLEMEN'S MAIL: HERBERT O. YARDLEY AND THE BIRTH OF AMERICAN CODEBREAKING ix (2004).

23. *Cryptologic Heritage*, NATIONAL SECURITY AGENCY, http://www.nsa.gov/about/cryptologic_heritage/center_crypt_history/pearl_harbor_review/black_chamber.shtml (last visited Aug. 11, 2014).

24. KAHN, *supra* note 22, at 58.

25. *Id.* at ix.

26. *Cryptologic History Calendar*, NATIONAL CRYPTOLOGIC MUSEUM FOUNDATION, https://cryptologicfoundationorg.presencehost.net/support/event_calendar.html/event/2018/05/20/1526792400/afsa-created-in-1949 (last visited Aug. 12, 2014).

27. THOMAS L. BURNS, THE ORIGINS OF THE NATIONAL SECURITY AGENCY 1940-1952 (U) 59 (1990), *available at* http://www.nsa.gov/public_info/_files/cryptologic_histories/origins_of_nsa.pdf. Unfortunately, this was just one of many failed attempts to coordinate efforts and share information with other intelligence agencies.

28. NATIONAL SECURITY AGENCY, *Cryptologic Almanac 50th Anniversary Series, The Creation of NSA – Part 2 of 3: The Brownell Committee, available at* http://www.nsa.gov/public_info/_files/crypto_almanac_50th/The_Creation_of_NSA_Part_3.pdf.

29. *Id.*

30. Ahuja, *supra* note 20.

31. Exec. Order No. 12,333, 3 C.F.R. 1981, *available at* http://www.archives.gov/federal-register/codification/executive-order/12333.html. Department of Defense Personnel Security Program Regulation, 3 C.F.R. 1981, 32 C.F.R. § 154 (2012). "The collection of foreign intelligence or counterintelligence within the United States shall be coordinated with the FBI as required by procedures agreed upon by the Director of Central Intelligence and the Attorney General." *Id.* at 1.8. "Agencies with the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States per-

collect information that constitutes "foreign intelligence or counterintelligence" while *not* "acquiring information concerning the domestic activities of United States persons." NSA has declared that it relies on the FBI to collect information on foreign intelligence activities within the borders of the United States, while confining its own activities within the United States to the embassies and missions of foreign nations.[32]

Unfortunately, NSA's capabilities were abused during a covert action program that lasted from 1956 to 1971 when the agency collected intelligence and surveilled various United States citizens, including suspected communists in the 1950s and civil rights activists, such as Dr. Martin Luther King, Jr., and Vietnam War protesters, such as Jane Fonda, Joan Baez, and Dr. Benjamin Spock, in the 1960s.[33] Additionally, it was revealed that thousands of American citizens were subjects of illegal intelligence operations.[34] In response, a Congressional committee was created in 1975.[35] Headed by Senator Frank Church of Idaho, the committee found that Congress had failed to provide the necessary statutory guidelines to ensure that intelligence agencies carried out their necessary missions in accordance with constitutional processes.[36] The NSA would no longer be permitted to conduct domestic eavesdropping for security and political purposes.

Based upon the Church Committee's findings, Congress passed the Foreign Intelligence Surveillance Act of 1978 (FISA),[37] which was meant to limit the practice of mass surveillance in the United States.[38] FISA represented a compromise between the President and Congress.[39] FISA would be used to oversee the executive branch's foreign intelligence activities.[40] FISA established the Foreign Intelligence Court (FISC or FISA Court) to review FISA warrant applications that were meant to target specific and identified agents of foreign powers.[41] The FISC currently consists of eleven federal district judges appointed for seven-year terms by the Chief Justice of the Supreme Court, and three judges are required

---

sons only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General." *Id.* at 2.3.

32. INT'L BUS. PUBL'NS, UNITED STATES MILITARY INTELLIGENCE HANDBOOK 85 (vol. 1, 2011).

33. NAT'L COMM'N TERRORIST ATTACKS UPON THE UNITED STATES, 9/11 COMMISSION REPORT 75 (July 22, 2004) [hereinafter 9/11 COMMISSION REPORT], *available at* http://www.9-11commission.gov/report/911Report.pdf; JAMES E. BAKER, IN THE COMMON DEFENSE 77 (Cambridge Univ. Press 2014).

34. *Senate History: January 27, 1975 Church Committee Created*, UNITED STATES SENATE, https://www.senate.gov/artandhistory/history/minute/Church_Committee_Created.htm (last visited June 2, 2015).

35. *Id.*

36. *Id.* "It is this indifference to constitutional restraints that is perhaps the most threatening of all the evidence that emerges from the findings of the Church Committee." *Id.* (quoting historian Henry Steele Commager).

37. Foreign Intelligence Surveillance Act of 1978, Pub.L. 95-511, 92 Stat. 1793 [hereinafter FISA of 1978] (codified at 50 U.S.C. §§ 1801 to 1811 (2014)).

38. BAKER, *supra* note 33 at 78–79.

39. *Id.* at 79.

40. *Id.*

41. *Id.* at 79–80.

to reside within twenty miles of Washington D.C.[42]

The FISA warrant application must consist of sufficient probable cause to believe that "the target of the electronic surveillance is a foreign power or agent of a foreign power," and the information sought must be related to national security.[43] Originally, the agent had to certify that the information to be sought was foreign intelligence information, and the purpose of the surveillance was to obtain foreign intelligence information.[44] A FISA warrant, unlike a Title III[45] wiretap application, does not require probable cause to believe that the target has or will commit a crime, but the warrant affidavit needs some predicate conduct to demonstrate the target is an agent of a foreign power.[46]

The FISA standard is different for foreign and U.S. persons.[47] Foreign persons can be targeted even without a court order if there is "no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party."[48] If there is no court order because the target is foreign, a call in which U.S. persons are inadvertently intercepted must be minimized.[49] Most of the surveillance done by the NSA falls under the category of foreign-to-foreign and therefore is not technically covered by FISA since the surveillance is directed overseas and usually against foreign persons.[50]

The FISA procedure also provides for cases of exigent circumstances during which the Attorney General could authorize electronic surveillance in advance of FISC approval.[51] However, the court must be notified, and an application must be made no later than seventy-two hours

---

42. *Id.*; *see also* FISA of 1978, amended from seven to eleven judges with the USA PATRIOT Act in 2001. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, sec. 208(1), Pub. L. No. 107-56, 115 Stat. 272 [hereinafter PATRIOT Act] (codified in scattered titles of U.S.C.), *available at* http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf.

43. 50 U.S.C. § 1804(a)(4)(A) (2014).

44. FISA of 1978, *supra* note 37.

45. Title III, or T3, is a federal wiretap and is a short-hand reference to the section of the Omnibus Crime Control and Safe Streets Act of 1968 Pub. L. No. 90-351, 82 Stat. 197 (codified as amended in scattered sections of 42 U.S.C.A.), which authorized federal law enforcement agencies to conduct electronic surveillance. 18 U.S.C.A. § 2518 (2000 & Supp. 2014) sets forth the procedural requirements for interception.

46. BAKER, *supra* note 33, at 80.

47. *Id.* "'United States person' means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States . . . ." 50 U.S.C.A. § 1801(i) (2014).

48. 50 U.S.C.A. § 1802(B) (2014).

49. BAKER, *supra* note 33, at 81.

50. SHANE HARRIS, THE WATCHERS: THE RISE OF AMERICA'S SURVEILLANCE STATE 163 (Penguin Books, 2011); NATIONAL SECURITY AGENCY, UNITED STATES SIGNALS INTELLIGENCE DIRECTIVE [hereinafter USSID 18] (Jan. 26, 2011), *available at* http://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf; Exec. Order No. 12,333, *supra* note 31.

51. BAKER, *supra* note 33, at 82.

after the Attorney General authorizes the interception.[52] To maintain congressional oversight, annual reports from the Attorney General are also mandated, which must include the number of orders obtained during the previous year.[53]

Although FISA warrants have not been made public, enough information has come out which would indicate FISA applications and affidavits are relatively complex and lengthy.

James E. Baker writes *In the Common Defense* that

> [f]ollowing passage of the [FISA] Act a specialized and compartmented bureaucracy emerged at Department of Justice, the FBI, and the CIA to handle the processing of FISA requests. By requiring submission of applications by the attorney general, along with certification from designated senior officials "that the purpose of surveillance is to obtain foreign intelligence," the Act generates a process of layered executive review. That is because the attorney general does not generate his or her own paperwork, and senior attorneys within a bureaucracy are less likely to send documents to the attorney general, along with other certifying officials, without careful review. Indeed, some argue, the process is too layered and therefore cumbersome, resulting in delays while paperwork transits up the bureaucracy to the attorney general even in cases of emergency authorization.[54]

In 1979, the FISC approved 199 warrants, a total of 635 in the 1980s, and 886 in the 1990s; in 2000 there were 1,005 approved applications and the number of applications doubled from 2000 to 2005.[55] In 2001, there were 932 approved applications,[56] and in comparison, the FISC approved 2,072 applications in 2005.[57] In FISA's most recent report to Congress, it is shown that 1,588 applications were approved in 2013.[58] Some have argued that FISA warrants are easier to obtain than Title III warrants. However, the percentage of FISA warrant applications that are approved is consistent with the number of applications and authorizations for Title III warrants.[59]

Between 1978 and 2001, there were no significant changes made to the

---

52. *Id.*

53. *Id.*

54. BAKER, *supra* note 33, at 83–84.

55. *Id.* at 83.

56. U.S. DEP'T OF JUSTICE, FISA 2001 ANNUAL REPORT TO CONGRESS, *available at* http://fas.org/irp/agency/doj/fisa/2001rept.html.

57. U.S. DEP'T OF JUSTICE, FISA 2005 ANNUAL REPORT TO CONGRESS, *available at* http://fas.org/irp/agency/doj/fisa/2005rept.html.

58. U.S. DEP'T OF JUSTICE, FISA 2013 ANNUAL REPORT TO CONGRESS, *available at* http://fas.org/irp/agency/doj/fisa/2013rept.pdf.

59. BAKER, *supra* note 33, at 83. "In 2005, for example, there were 1,774 [Title III] applications and 1,773 applications authorized. In 2004, there were 1,710 applications and 1,710 authorizations." *Id.*; *see also* UNITED STATES COURTS, WIRETAP REPORTS ARCHIVE, *available at* http://www.uscourts.gov/Statistics/WiretapReports/WiretapReports_Archive.aspx.

FISA process.[60] FISA as it stood was considered a check on blanket presidential authority to intercept conversations outside the standard warrant process. Then suddenly post-9/11, the old ways of conducting business within the IC no longer worked. The gloves came off as American citizens wanted answers, and the executive branch and 9/11 Commission asked the IC to share its information and collaborate with various federal and state agencies, predict terrorist activity before attacks occur, and quite simply, perform better.

B. The "Wall" Between the IC and Law Enforcement

Pre-9/11, a wall had been created between law enforcement and the intelligence community. The concern was that law enforcement might use FISA information to negate the necessity of a lawful Title III order and intentionally evade the requirement of developing probable cause to determine whether a target has been or is committing a crime.[61] In July 1995, procedures had been put in place to regulate "the manner in which [FISA] information could be shared from the intelligence side of the house to the criminal side" as it related to agents and criminal prosecutors.[62] DOJ did not want FISA information used "to circumvent traditional criminal warrant requirements."[63] However, the procedures were misinterpreted in a way that even an FBI agent on the intelligence side and an agent working on a criminal investigation on the same subject could not share information.[64] Since the FISA statute indicated its sole purpose for surveillance was intelligence, the wall could only be crossed with the Attorney General's approval and the FISC's blessing.[65] With this system in place, there was no need to worry that the intelligence information would be used against a defendant in a criminal trial.

Post-9/11, the wall disintegrated. The 9/11 Commission criticized the barriers that had been placed between FBI intelligence sections and criminal/law enforcement sections, as well as the barriers placed between intelligence agencies and faulted these barriers for being a large part of the reason why the IC and law enforcement did not catch the terrorists prior to the hijacking of the four planes on 9/11.[66] The 9/11 Commission recommended a unification of "the many participants in the counterterrorism effort and their knowledge in a network-based information-sharing sys-

60. Baker, *supra* note 33, at 84. However, in the early 1990s, the President sought an amendment to FISA "to grant the FISC jurisdiction and authority to issue warrants for physical searches for foreign intelligence purposes." *Id.*

61. 9/11 Commission Report, *supra* note 33, at 79.

62. *Id.*

63. *Id.* at 78.

64. *Id.* at 79.

65. Baker, *supra* note 33, at 85.

66. 9/11 Commission Report, *supra* note 33, at 345. The Commission stated: "A 'smart' government would *integrate* all sources of information to see the enemy as a whole. Integrated all-source analysis should also inform and shape strategies to collect more intelligence." *Id.* at 401.

tem that transcends traditional governmental boundaries."[67]

Post-9/11, the FISA process was also criticized as too slow and cumbersome. As described in one DOJ memo in 2006, "[t]he FISA process, by design, moves more slowly. It requires numerous lawyers, the preparation of legal briefs, approval from a Cabinet-level officer, certification from the National Security Advisor or another Senate-confirmed officer, and finally, the approval of an Article III judge."[68]

However, NSA officials testified during a March 2005 report to President Bush that the FISA process had "not posed a serious obstacle to effective intelligence gathering."[69]

In response to the 9/11 Commission's criticisms, as well as other criticisms of the government's ability to predict terrorist attacks and protect the nation from other similar attacks, Congress passed the PATRIOT Act on October 25, 2001.[70] The PATRIOT Act under section 203, entitled "Authority to Share Criminal Investigative Information," broke down the wall that had been blocking the flow of information between the intelligence community and law enforcement, specifically as it pertained to the FBI.[71] The National Counterterrorism Center was also created, which led to various agencies sharing and analyzing data under one roof.[72]

C. USA PATRIOT Act Section 215: the Collection of "Metadata"

Section 215 of the PATRIOT Act, entitled "Access to Certain Business Records for Foreign Intelligence and International Terrorism Investigations,"[73] made it easier for the government to collect telephony

67. 9/11 Commission Report, *supra* note 33, at 400.

68. U.S. Dep't of Justice, The NSA Program to Detect And Prevent Terrorist Attacks Myth v. Reality 3 (Jan. 27, 2006), *available at* http://www.justice.gov/opa/documents/nsa_myth_v_reality.pdf.

69. Matthew M. Aid, The Secret Sentry: The Untold History of the National Security Agency 297 (Bloomsbury Press 2009) (during a hearing on the U.S. intelligence community's performance against the Iraqi WMD programs).

70. PATRIOT Act, *supra* note 42, at sec. 203.

71. Amending Fed. R. Crim. P. 6 and 18 U.S.C.A. § 2517 (2000 & Supp. 2014), Section 203(a) discussed the authority to share grand jury information, section (b) discussed the authority to share electronic, wire, and oral interception information, and section (c) discussed the authority to share foreign intelligence information. PATRIOT Act, *supra* note 42, at sec. 203.

72. *See* Exec. Order No. 13,354, 3 C.F.R. 13,354 (2004), *available at* http://www.gpo.gov/fdsys/pkg/CFR-2005-title3-vol1/pdf/CFR-2005-title3-vol1-eo13354.pdf; *see also* Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, 118 Stat. 3638 (codified at 50 U.S.C.A. § 402 (2003 & Supp. 2014)), *available at* http://www.nctc.gov/docs/irtpa.pdf.

73. Section 215 of the PATRIOT Act amended the "business records" provision of Title V, Section 501 of FISA. PATRIOT Act, *supra* note 47, at sec. 215. Section 215 was reauthorized in the USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192, *available at* http://www.gpo.gov/fdsys/pkg/CRPT-109hrpt333/pdf/CRPT-109hrpt333.pdf; *see also* 50 U.S.C.A. § 1861 (2014).

metadata[74] and conduct records searches.[75] Metadata includes "much of the information that appears on a customer's telephone bill: the date and time of a call, its duration, and the participating phone numbers" and can include the nature of "how the call was routed from one participant to the other through the infrastructure of the telephone companies' networks."[76] Electronic communications metadata includes "the 'to,' 'from,' and 'cc' lines of an email and the email's time and date."[77]

Section 215 allows the government to obtain a secret court order requiring third parties, such as telephone companies, to hand over any records or other "tangible thing" if deemed "relevant" to an investigation "to obtain foreign intelligence information not concerning a U.S. person or to protect against international terrorism or clandestine intelligence activities."[78]

To collect these records, the government must obtain a Section 215 order from the FISC.[79] Under Section 215, the government can apply to the FISC to compel businesses other than companies to hand over user records as long as the records are "relevant" to a terrorist investigation.[80]

Section 215 data related to U.S. persons can only be passed on to the FBI or others in the IC, and the leads from the metadata are limited only

---

74. "Telephony metadata includes comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call. Telephony metadata does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer." Doug Aamoth, *Verizon, Telephony Metadata, the National Security Agency, and You*, TIME, June 6, 2013, http://techland.time.com/2013/06/06/verizon-telephony-metadata-the-national-security-agency-and-you/.

75. Section 216 governs access to online activity, such as email contact information or Internet browsing histories. PATRIOT Act, *supra* note 42, at sec. 216.

76. PRIVACY AND CIVIL 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 8 (Jan. 23, 2014), *available at* https://www.eff.org/files/2014/01/23/final_report_1-23-14.pdf.

77. Press Release, Office of the Director of National Intelligence, NEWLY DECLASSIFIED DOCUMENTS REGARDING THE NOW-DISCONTINUED NSA BULK ELECTRONIC COMMUNICATIONS METADATA PURSUANT TO SECTION 402 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (Aug. 11, 2014), *available at* http://www.dni.gov/index.php/newsroom/press-releases/198-press-releases-2014/1099-newly-declassified-documents-regarding-the-now-discontinued-nsa-bulk-electronic-communications-metadata-pursuant-to-section-401-of-the-foreign-intelligence-surveillance-act. A now discontinued NSA program to collect bulk electronic communications metadata was authorized pursuant to Section 402 of the FISA ("PRTT provision"). "This collection was done only after the Foreign Intelligence Surveillance Court approved the government's applications, and pursuant to court order generally lasting 90 days. NSA was not permitted to collect the content of any electronic communications." *Id.*

78. PATRIOT Act, *supra* note 42, at sec. 215; *see also* BRENNAN CENTER FOR JUSTICE, ARE THEY ALLOWED TO DO THAT? A BREAKDOWN OF SELECTED GOVERNMENT SURVEILLANCE PROGRAMS 1 http://www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf.

79. In 2009, there were 21 Section 215 applications before the FISC; in 2012, there were 212 applications. BRENNAN CENTER FOR JUSTICE, *supra* 78, at 2.

80. *Id.* at 3.

to counterterrorism investigations.[81]

Section 215 also established congressional oversight for the FISA program, requiring the DOJ to conduct an audit of the program and the "effectiveness" of Section 215 and to submit an unclassified report on the audit to the House and Senate Committees on the Judiciary and Intelligence.[82]

Section 215 has gone under extensive review by the Privacy and Civil Liberties Oversight Board,[83] an independent agency within the executive branch, and the President's Review Group on Intelligence and Communications Technologies.[84] Various bills are currently before the House and Senate revising or eliminating the program.[85]

Since the telephony metadata collection program is only used for counterterrorism investigations as it pertains to U.S. persons, this data would not be passed to the DEA or other agencies investigating non-terrorism cases.

D. USA PATRIOT Act Section 218: Expanding FISA Authority

Section 218 expanded the application of FISA to situations where foreign intelligence gathering was merely "a significant" purpose of the investigation rather than, as prior 1978 FISA law provided, "the sole or primary purpose."[86] Section 218 effectively destroys the wall and allows for the exchange of advice among the IC and law enforcement on FISA search and surveillances. Critics argue that adding the term "significant" will lead to overuse of the FISA process as a FISA warrant may be requested for non-foreign intelligence purposes.[87] Some believe that the new standards under FISA will cause law enforcement agents to request a FISA warrant rather than attempt to obtain a more stringent Title III

81. PATRIOT Act, *supra* note 42, at sec. 215.

82. *Id.*

83. Privacy and Civil Liberties Oversight Board, http://www.pclob.gov/ (last visited Sept. 18, 2014). *See generally* Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies (Dec. 12, 2013).

84. Office of the Director of National Intelligence: The Review Group, http://www.dni.gov/index.php/intelligence-community/review-group. *See generally* Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies (Dec. 12, 2013).

85. *See* USA FREEDOM Act, H.R. 3361, 113th Cong. (2013-2014); Relevancy Act, H.R. 2603, 113th Cong. (2013-2014); Surveillance Order Reporting Act of 2013, H.R. 3035, 113th Cong. (2013-2014): FISA Court Reform Act of 2013, H.R.3228, 113th Cong. (2013-2014); FISA Transparency and Modernization Act, H.R. 4291, 113th Cong. (2013-2014); H.Res. 590, 113th Cong. (2013-2014); FISA Accountability and Privacy Protection Act of 2013, S. 1215, 113th Cong. (2013-2014); FISA Court Reform Act of 2013, S. 1467, 113th Cong. (2013-2014); Intelligence Oversight and Surveillance Reform Act, S. 1551, 113th Cong. (2013-2014); USA FREEDOM Act, S. 1599, 113th Cong. (2013-2014); USA FREEDOM Act of 2014, S. 2685, 113th Cong. (2013-2014).

86. Electronic Privacy Information Center, http://epic.org/privacy/terrorism/usapatriot/ (last visited Aug. 23, 2014); *see also* PATRIOT Act, *supra* note 42, at sec. 218.

87. *Id.*

warrant for criminal evidence.[88]

In May 2002, a FISC judge held that section 218 was unconstitutional, thereby rejecting the government's attempt to dismantle the "wall" that inhibited intelligence investigators from sharing FISA surveillance with law enforcement and prosecutors.[89] However, months later, the FISA Court of Review overturned the ruling, stating "[s]o long as the government entertains a realistic option of dealing with the agent other than through criminal prosecution, it satisfies the significant purpose test."[90] The court noted the seamless nature of intelligence and law enforcement inquiries; for example, foreign intelligence information might necessarily evidence criminal conduct like espionage.[91] In light of this nexus, the court wrote "a standard which punishes such cooperation could well be thought dangerous to national security."[92] The court concluded that the balance struck in the amended FISA was consistent with concerns in the 1960s and 1970s about domestic wiretapping that had led to the creation of FISA in the first place.[93] Therefore "the FISA as amended is constitutional because the surveillances it authorizes are reasonable."[94]

E. Disclosure of the NSA's Terrorist Surveillance Program

On December 16, 2005, the *New York Times* ran an article revealing that for four years, the NSA had monitored the communications of Americans without obtaining warrants from the FISC in violation of FISA.[95] The legal authority for these wiretaps came from the executive branch and with the approval of the Department of Justice.[96]

Following the news article, the DOJ issued a public memorandum explaining that the program applied to communications where at least one party was located outside of the United States.[97] The program was meant to focus on members of al Qaeda and affiliated groups, and interceptions would occur "if there is a reasonable basis to believe that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda."[98] The memo also argued that the President had legal authority to authorize the NSA "terrorist surveillance program" as Commander-in-Chief and Chief Executive and that the President had "inherent authority to conduct

88. Baker, *supra* note 33, at 85.
89. *In re* All Matters Submitted to Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 729 (FISA Ct. 2002).
90. *In re* Sealed Case, 310 F.3d 717, 735 (FISA Ct. Rev. 2002).
91. *Id.* at 743.
92. *Id.*
93. *Id.* at 746.
94. *Id.*
95. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times (Dec. 16, 2005), *available at* http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all&_r=0.
96. *Id.*
97. U.S. Dep't of Justice, *supra* note 68, at 2.
98. *Id.*

warrantless surveillance to gather foreign intelligence even in peacetime."[99] Moreover, the Authorization for Use of Military Force (AUMF) passed by Congress after the September 11th attacks authorized the President to use "all necessary and appropriate military force against those nations, organizations, or persons he determines planned, authorized, committed, or aided in the terrorist attacks that occurred on September 11, 2001," which included the authority to authorize the surveillance program.[100]

It was later disclosed that then-White House counsel Alberto Gonzales and DOJ lawyer John Yoo had written memos justifying the legality of these NSA surveillance programs and finding that the special needs exception to the warrant requirement applied in this set of circumstances. In his memo, John Yoo pointed to *Vernonia School District 47J v. Acton*, where the Court explained that a warrantless search can be constitutional "when special needs, beyond the normal need of law enforcement, make the warrant and probable-cause requirement impracticable."[101] He also explained, "the Court has found warrantless searches reasonable when there are 'exigent circumstances,' such as threat to the safety of law enforcement or third parties."[102]

Moreover, even if the NSA's surveillance targeted U.S. persons, including those inside the United States, the administration decided that any communication involving foreign parties made the entire communication "foreign intelligence."[103] Yoo wrote in a later memo, "unless Congress made a clear statement in FISA that it sought to restrict presidential authority to conduct warrantless searches in the national security area—which it has not—then the statute must be construed to avoid such a reading."[104]

Even though Congress had intended FISA to be a check on the president's surveillance powers,[105] the administration believed the FISA process impeded the swift approach of catching terrorists if the NSA had to wait for a federal judge to issue a warrant for each and every suspect who appeared. Under the inherent powers of the President and the executive

---

99. *Id.* at 1.

100. *Id.*

101. Memorandum from John C. Yoo, Deputy Assistant Attorney Gen., to David S. Kris, Assoc. Deputy Attorney Gen. 2 (Sept. 25, 2001) (citing *Vernonia Sch. Dist. 47J*, 515 U.S. 646 (1995)), *available at* http://www.justice.gov/opa/documents/memoforeignsurveillanceact09252001.pdf.

102. *Id.*

103. *Id.*

104. Memorandum for the Attorney Gen. from John C. Yoo, Deputy Assistant Attorney Gen. (Nov. 2, 2001), *available at* http://www.justice.gov/sites/default/files/olc/legacy/2011/03/25/johnyoo-memo-for-ag.pdf. Matthew Aid submitted an FOIA request to the DOJ in October, 2009. In a response dated August 10, 2011, the DOJ stated that it "[was] withholding two of the documents in full pursuant to FOIA Exemptions One and Five, 5 U.S.C.A. § 552(b)(1) & (5) (2007 & Supp. 2014), because they are classified and are protected by the deliberative process privilege." *See* Matthew Aid, FOIA Request to Justice Department, *available at* http://fas.org/sgp/news/2011/08/aid-olc.pdf.

105. FISA of 1978, *supra* note 37.

branch,[106] the NSA had the authorization to intercept Americans inside the country without a warrant as long as one party to the communication was outside the United States and the analyst reasonably suspected one party was a terrorist or an associate or member of an organization affiliated with terrorism, specifically al Qaeda.[107]

F. Congress's Response: the Protect America Act of 2007 and the FISA Amendments Act of 2008 (Section 702)

The Protect America Act was a temporary surveillance law that was enacted in 2007 and meant to expire in one year.[108] The government argued in support of the bill that,

> changes in technology since 1978 had the effect of expanding the scope of FISA's coverage to include intelligence collection efforts that Congress excluded from the law's requirements. This unintended expansion of FISA's scope meant the government, in a significant number of cases, needed to obtain a court order to collect foreign intelligence information against a target located overseas. This created an unnecessary obstacle to our Intelligence Community's ability to gain real-time information about the intent of our enemies overseas and diverted scarce resources that would be better spent safeguarding the civil liberties of people in the United States, not foreign terrorists who wish to do us harm.[109]

The "changes in technology since 1978" referred to the fact that FISA statutory language had been interpreted such that if an electronic communication touched a fiber optic cable in the United States, the NSA would need a FISA warrant before it could monitor the conversation.[110] This proved to be a problem with quick, real-time surveillance of a foreign target.[111]

The Protect America Act was designed to allow the IC to collect foreign intelligence information on targets in foreign lands without first receiving FISA court approval, as well as protect third parties from private lawsuits arising from the assistance they provide the IC.[112] Thus, the IC would be able to obtain blanket authorizations (as long as targeting and minimization procedures are approved by the FISC) and not individual warrants to target non-U.S. persons reasonably believed to be located

---

106. Article II of the Constitution designates the president as Commander-in-Chief and gives him authority over foreign affairs. U.S. Const. art. II, § 2, cl. 1.

107. U.S. Dep't of Justice, *supra* note 68, at 2.

108. Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (codified at 50 U.S.C.A. §§ 1805a to 1805c (2003 & Supp. 2014)).

109. The White House, George w. Bush, Fact Sheet: The Protect America Act of 2007 (Aug. 6, 2007), *available at* http://georgewbush-whitehouse.archives.gov/news/releases/2007/08/20070806-5.html.

110. James Bamford, The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America 298 (Anchor Books, 2009).

111. *Id.*

112. *Id.*

outside the United States.[113] The FISC would review the IC procedures used to ensure that they had a reasonable basis to believe that the targets were of foreign intelligence value, and that the surveillance was not intended to target Americans.[114] Unfortunately, although the Protect America Act specifically did not permit the warrantless surveillance of U.S. persons inside the United States, the fear was that "thousands, potentially hundreds of thousands, of Americans' communications would be swept up as the NSA monitored the global telecom system."[115] The Protect America Act gave the government extraordinary surveillance powers, and thus, Congress placed its trust in the fact that the Attorney General would submit to the FISC the procedures being used so there would be some sort of outside review.[116] In turn, the FISA judges had to rely on the government's assurances that these massive new surveillances and targeting and minimization procedures were not inadvertently collecting the conversations of people they should not monitor.[117]

Since the Protect America Act was only to last one year, Congress passed the FISA Amendments Act of 2008[118] (otherwise known as section 702 or FAA), which has been criticized as authorizing most of the powers that the Bush administration had used under its Terrorist Surveillance Program.[119] Section 702 was not much different from the Protect America Act. It gave the government authority to monitor communications outside the FISA or Title III traditional warrant process and set forth "procedures for targeting certain persons outside the United States other than United States persons."[120] The Amendments stated, "[t]he Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[121]

Minimization procedures were established in the 702 programs in order to protect the privacy of U.S. persons inadvertently monitored.[122] The content and identity of the U.S. person must be deleted unless (1) there is a reasonable belief the phone call between the foreign target and the U.S.

---

113. HARRIS, *supra* note 50, at 341; Protect America Act of 2007, *supra* note 108.
114. *Id.*; Protect America Act of 2007, *supra* note 108.
115. *Id.* at 341–42.
116. *Id.* at 342.
117. *See* THE WHITE HOUSE, GEORGE W. BUSH, *supra* note 109.
118. H.R. 6304, 110th Cong. (2007-2008), *available at* http://www.gpo.gov/fdsys/pkg/BILLS-110hr6304enr/pdf/BILLS-110hr6304enr.pdf.
119. Jacob Sommer, *FISA Authority and Blanket Surveillance: A Gatekeeper Without Opposition*, 40 No. 3 LITIGATION, (Spring 2014), *available at* http://www.americanbar.org/publications/litigation_journal/2013-14/spring/fisa_authority_and_blanket_surveillance_gatekeeper_without_opposition.html.
120. 50 U.S.C.A. § 1881(a) (2003 & Supp. 2014).
121. *Id.*
122. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (July 2, 2014), *available at* http://www.pclob.gov/All%20Documents/Report%20on%20the%20Section%20702%20Program/PCLOB-Section-702-Report-PRE-RELEASE.pdf.

person contains significant foreign intelligence, (2) the call reveals evidence of a crime, (3) the call is encrypted, or (4) the U.S. person poses a threat of serious harm to life or property.[123]

Therefore, the NSA was authorized to target only foreign persons in foreign countries outside the warrant process and not persons in the United States, United States persons located in foreign countries, or persons located outside the United States "if the purpose of such acquisition [wa]s to target a particular, known person reasonably believed to be in the United States."[124] Moreover, the NSA must certify to the FISC that "a *significant* purpose of the acquisition is to obtain foreign intelligence information" rather than the previous certification that "the purpose" is to obtain foreign intelligence information.[125]

As with section 215's telephone metadata collection program, there are critics of section 702. Most of the criticisms focus on 702's minimization and targeting procedures and the perceived lack of enforcement of these procedures. The concern is that Americans' conversations are routinely being collected and inadvertently being analyzed. Contrary to their concerns with section 215, the Privacy and Civil Liberties Oversight Board and President's Review Group have found the 702 program to be legal, relatively effective, and valuable.[126]

III. THE RELATIONSHIP BETWEEN THE NSA AND THE DEA AND "PARALLEL CONSTRUCTION"

After the initial Snowden disclosures in June 2013, a series of articles came out expanding on the impact the NSA intercepts had on other law enforcement agencies. On August 5, 2013, Reuters published an article indicating that law enforcement agencies such as the DEA were using NSA intercepts,[127] wiretaps by foreign governments, court-approved domestic wiretaps, and phone log databases to initiate criminal investigations.[128] The article used the acronym "DICE" to refer to a phone log and Internet data database, which is said to contain approximately one billion records which were gathered legally by the DEA through "subpoenas, arrests and search warrants nationwide."[129] It is used so that law enforcement agents can "connect the dots" and make connections between targets of investigations.[130]

123. *Id.*
124. 50 U.S.C.A. § 1881a(b)(1-4) (2003 & Supp. 2014).
125. *Id.* § 1881a(g)(2)(A)(v) (2003 & Supp. 2014) (emphasis added).
126. LIBERTY AND SECURITY IN A CHANGING WORLD, *supra* note 83.
127. The Reuters article did not reveal whether the intercepts came from the FISA warrant process and/or Section 702 programs and/or Executive Order 12,333. The section 215 bulk collection telephony metadata would not be considered a source as that program deals only with metadata and any U.S. person information can only be used in counterterrorism investigations.
128. Shiffman & Cooke, *supra* note 2.
129. *Id.*
130. *Id.*

According to Reuters, initial information derived from the previously mentioned sources is effectively "scrubbed" at a central location called the Special Operations Division (SOD) before being sent out to field agents with the DEA, Internal Revenue Service, FBI, and Homeland Security.[131] The SOD's main function is to act as the central coordinator for multi-jurisdictional and international investigations, "connecting agents in separate cities who may be unwittingly investigating the same target and making sure undercover agents don't accidentally try to arrest each other."[132]

Reuters uncovered internal DEA PowerPoint presentation slides which encouraged "agents to omit the SOD's involvement [in the collection of tips] from investigative reports, affidavits, discussions with prosecutors and courtroom testimony. Agents are instructed to then use 'normal investigative techniques to recreate the information provided by the SOD.'"[133] Normal investigative techniques would include "independent sources [such] as investigative files, subscriber and toll requests, physical surveillance, wire intercepts, and confidential source information."[134]

The practice of taking a classified tip, which SOD prefers not to be used as evidence, and conducting a separate investigation and developing independent evidence that would be admissible at trial has been called "parallel construction."[135] Reuters found DEA sources that said, "Parallel construction is a law enforcement technique we use every day . . . it's decades old, a bedrock concept."[136]

Since this disclosure, defense attorneys and others have argued that "parallel construction" violates a defendant's constitutional rights to a fair trial and to confront witnesses against him/her, and violates pretrial discovery rules by burying evidence that could prove useful to criminal defendants.[137] By circumventing court procedures for weighing whether sensitive, classified, or FISA evidence must be disclosed to a defendant, the practice of "parallel construction" prevents the defendant from knowing about evidence that might be exculpatory and arguably prevents an opportunity to challenge the accuracy of the investigation. It also misleads the court.[138] If defendants are not informed as to how an investigation began, "they cannot know to ask to review potential sources of exculpatory evidence—information that could reveal entrapment, mis-

131. *Id.*

132. *Id.*

133. *Id.*

134. John Shiffman & David Ingram, *Exclusive: IRS manual detailed DEA's use of hidden intel evidence*, REUTERS (Aug. 7, 2013), http://www.reuters.com/article/2013/08/07/us-dea-irs-idUSBRE9761AZ20130807.

135. *Id.*

136. Shiffman & Cooke, *supra* note 2.

137. *Id.*

138. *Id.*; Hanni Fakhoury, *DEA and NSA Team Up to Share Intelligence, Leading to Secret Use of Surveillance in Ordinary Investigations*, ELEC. FRONTIER FOUND. (Aug. 6, 2013), https://www.eff.org/deeplinks/2013/08/dea-and-nsa-team-intelligence-laundering.

takes or biased witnesses."[139]

Several senators and congressmen asked former Attorney General Eric Holder to answer questions about the Reuters report, and the DOJ is currently said to be reviewing the practice.[140] Some senators wrote, "[t]hese allegations raise serious concerns that gaps in the policy and law are allowing overreach by the federal government's intelligence gathering apparatus."[141] The DEA has stated the practice is legal, and the purpose is to protect confidential sources and investigative methods, not to withhold evidence.[142]

Some critics have gone so far as to argue that parallel construction is doublespeak for "intelligence laundering" and that "the SOD's insulation from even judges and prosecutors stops federal courts from assessing the constitutionality of the government's surveillance practices."[143]

Because so little has been said publicly about the allegations, there are bound to be misinterpretations of this particular DEA policy. Some commented "[i]t certainly can't be that the agents can make up a 'parallel construction,' a made-up tale, in court documents, testimony before the grand jury or a judge, without disclosure to a court."[144] One former federal judge is quoted as saying, "It sounds like they are phonying up investigations."[145]

Upon disclosure of this new information, the question to be asked is two-fold:

1. How do courts handle information that is typically used to initiate a criminal investigation? Is that information, if not used as evidence at trial, nevertheless discoverable?
2. How do courts handle this recently revealed information (to include NSA intercepts, intelligence sharing from wiretaps by foreign governments, court-approved domestic wiretaps, and phone log databases)? Is this information also discoverable or should it be immune from court scrutiny merely because the material came from a classified source or technique?

A Typical Initiation of an Investigation: From Hunch/Tip to Probable Cause to Arrest

Criminal investigations, drug cases in particular, have many origins. Some of the more common ways a case is initiated is through an anony-

139. Shiffman & Cooke, *supra* note 2.

140. John Shiffman, *Holder pressed on U.S. drug agency use of hidden data evidence*, Reuters (Aug. 26, 2013), http://www.reuters.com/article/2013/08/27/us-usa-security-dea-idUSBRE97P0Y520130827.

141. *Id.*

142. Shiffman, *supra* note 140.

143. Fakhoury, *supra* note 138.

144. David Ingram & John Shiffman, *U.S. defense lawyers to seek access to DEA hidden intelligence evidence*, Reuters (Aug. 8, 2013), http://www.reuters.com/article/2013/08/08/us-dea-irs-idUSBRE9761AZ20130808.

145. Shiffman & Cooke, *supra* note 2.

mous tip to the DEA or local law enforcement ("I think my neighbor is growing marijuana in his home"), or an ex-girlfriend or spouse (there's nothing like a woman scorned), or a friend, family member, or co-worker who has contacted the authorities and would like for them to investigate suspected criminal activity.

Another common way investigations are initiated is through a defendant's encounter with the police (e.g., traffic stop) or encounter with a confidential informant working with the DEA. Sometimes, an investigation is simply a spin-off from another local investigation targeting a different group of defendants or an investigation or wiretap that began in another state. The fire department is also sometimes called to put out a fire at a home that turns out to be a meth lab. This type of information is turned over to local law enforcement for further investigation and potential prosecution.

In order to evaluate whether hiding the tools described in the Reuters' report is lawful and whether "parallel construction" is an acceptable practice, it is important to also evaluate these initial investigative tools that are normally not disclosed to the defendant until closer to trial, or many times, not at all.

It is also important to review a prosecutor's discovery obligations. A defendant is not entitled to every piece of information collected during an investigation.[146] Discovery rules are reciprocal and govern what the defendant and prosecution are entitled to pre-trial.[147]

Federal prosecutors must comply with discovery obligations under the Federal Rules of Criminal Procedure,[148] the United States Constitution, and the court's inherent supervisory power.[149] Prosecutors have a duty to disclose exculpatory evidence under *Brady v. Maryland*[150] and evidence that would tend to impeach the credibility of cooperating government witnesses under *Giglio v. United States*.[151] Lastly, prosecutors must turn over to the defense any Jencks Act material, which would be any previous statements signed or adopted by a witness that relates to the subject matter of the testimony of the witness, at the close of a witness's direct examination, and preferably earlier.[152]

---

146. Classified Information Procedures Act [hereinafter CIPA], Pub. L. No. 96-456, 94 Stat. 2025 (codified as amended at 18 U.S.C. app. 3 §§ 1-16).

147. *Id.*

148. FED. R. CRIM. P. 16.

149. "Some judges use this authority to issue orders requiring the disclosure of certain information, such as the names and addresses of the witnesses who will be called to testify." NEIL P. COHEN, DONALD J. HALL & STANLEY E. ADELMAN, CRIMINAL PROCEDURE: THE POST-INVESTIGATIVE PROCESS, CASES, AND MATERIALS 276 (3d ed. 2008).

150. Brady v. Maryland, 373 U.S. 83, 87 (1963). "We now hold that the suppression by the prosecution of evidence favorable to an accused upon request 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." *Id.*

151. Giglio v. United States, 405 U.S. 150 (1972).

152. Jencks v. United States, 353 U.S. 657 (1957); 18 U.S.C. § 3500(b); *see* FED. R. CRIM. P. 26.2 (incorporating Jencks Act requirements into the Federal Rules of Criminal Procedure).

Discovery obligations are required in order to promote fairness to the defendant and promote good faith on the part of the prosecution in its ability to obtain statements, information, or items within the United States government's possession, custody, or control. Compared to civil litigation, discovery in a criminal proceeding is adversarial in nature. Those that argue against liberal discovery fear the defense will intimidate government witnesses or fabricate a defense or commit perjury based upon the prosecution's known theory of the case.[153] Significant discovery is now the rule rather than the exception. From 1963 to 1985, with cases such as *Brady*, *Giglio*, *Bagley*,[154] *Kyles*,[155] and *Agurs*,[156] the Supreme Court began to place discovery obligations on the prosecution and also demanded reciprocal discovery.[157] While the truth is supposed to emerge from an adversarial system, courts worry that it will not and that rules of discovery must be put in place to ensure fairness.[158]

On a defendant's request, F.R.C.P. 16(a)(1)(A)–(G) requires that the government disclose the defendant's statements, prior record, certain documents and tangible items, reports of examinations and tests, and written summaries of expert witness testimony.

A. Anonymous Tips, Informants, and Cooperating Witnesses

An anonymous tip, which is considered hearsay and inadmissible at trial, is typically not disclosed to the defense. A tip would not be considered discoverable unless it is somehow exculpatory. At trial, an agent cannot testify as to what the tip said but can mention what he/she did as a result of receiving the tip.[159]

Informants[160] and cooperating witnesses are also regularly used in drug investigations. Oftentimes, informants will suggest a particular target or case to an agent, and the agent will then decide whether to open an investigation. Once the case is initiated, the informant will meet with the target and, hopefully, record meetings and telephone conversations in order to

153. Joshua Dressler & Alan C. Michaels, Understanding Criminal Procedure: Adjudication 156 (4th ed. 2006).

154. United States v. Bagley, 473 U.S. 667 (1985) (explaining that favorable evidence is material if there is a "reasonable probability" that, had the evidence been disclosed to the defense, the result of the proceeding would have been different).

155. Kyles v. Whitley, 514 U.S. 419 (1995) (defining the materiality standard in terms of the cumulative effect of all suppressed evidence favorable to the defense, not the evidence considered item-by-item).

156. United States v. Agurs, 427 U.S. 97, 104 (1976) ("A fair analysis of the holding in Brady indicates that implicit in the requirement of materiality is a concern that the suppressed evidence might have affected the outcome of the trial.").

157. Williams v. Florida, 399 U.S. 78 (1970) (holding that requiring defendant to disclose his alibi defense to the government prior to trial does not violate his Fifth Amendment right against compulsory self-discrimination); *see also* Fed. R. Crim P. 12.1–12.3 (reciprocal discovery).

158. *Williams*, 399 U.S. at 78.

159. Brady v. Maryland, 373 U.S. 83, 87 (1963).

160. Informants are distinguished from cooperating witnesses as they are paid for their information, given immunity for past criminal acts, or charged with a lesser crime in return for their cooperation with the government.

develop probable cause. Many times, the agent will attempt to cut the informant out of the investigation and place an undercover agent in the informant's stead in order to protect the informant's identity. Any previous drug buys done with the informant will be excluded from any charges in the future indictment.[161] This is particularly useful if the informant has considerable baggage, such as a significant criminal history, acts of violence, prior inconsistent statements, and other impeachment evidence that could be used at trial.

The identity of an informant may be protected if he or she does not testify.[162] If an informant's information is used for intelligence purposes only and not at trial, there is a greater likelihood that the informant's identity can be protected. If the informant will not be called as a witness at trial, the defense will need to demonstrate that disclosure is "relevant and helpful to the defense of the accused, or is essential to a fair determination of a cause."[163] The purpose of the privilege is to encourage citizens to communicate such information to law enforcement officers by protecting their anonymity, and the scope of the privilege is limited by this purpose. Another government interest in non-disclosure lies in the fact that the disclosure of an informant could compromise other ongoing criminal investigations.[164]

In *Roviaro*, the Supreme Court considered the application of the informant's privilege to the general discovery rules, pursuant to which the government may withhold from disclosure the identity of its informants.[165] The Court noted that the privilege implicates two fundamental competing interests: (1) the interest of the defendant in mounting a defense; and (2) the public interest in enabling the government to protect its sources.[166] The Court relied on two basic principles to resolve the competing interests. First, it noted that the defendant's interest was triggered only when information in the government's possession was "relevant and helpful."[167] Second, when the evidence is deemed relevant and helpful, the Court held, resolving the interests "calls for balancing the public interest in protecting the flow of information against the individual's right to prepare his defense."[168] In order to determine whether the informer's privilege must give way to the defendant's right to prepare his defense, the Eleventh Circuit listed three factors that must be considered: (1) the extent of the informant's participation in the criminal activity; (2) the re-

161. Roviaro v. United States, 353 U.S. 53 (1957) (setting forth the government's informant privilege).

162. *See* Scher v. United States, 305 U.S. 251, 254 (1938); *Roviaro*, 353 U.S. at 59 ("What is usually referred to as the informer's privilege is in reality the government's privilege to withhold from disclosure the identity of persons who furnish information of violations of law to officers charged with enforcement of that law."); United States v. Fuentes, 988 F. Supp. 861 (E.D. Pa. 1997).

163. *Roviaro*, 353 U.S. at 59.

164. *Id.*

165. *Id.* at 55.

166. *Id.* at 62.

167. *Id.* at 60–62.

168. *Id.* at 62.

lationship between the defendant's asserted defense and the informant's probable testimony; and (3) the government's interest in non-disclosure.[169]

Even an informant's substantial role in an investigation, without more, will not warrant disclosure generally.[170] The defendant has the burden of showing that the informant's testimony would significantly aid in establishing an asserted defense[171] or that the informant was an active participant in the criminal matter.[172] Mere conjecture about the possible relevance of the informant's testimony is insufficient to warrant disclosure.[173]

As an alternative, courts have suggested the informant's identity not be revealed, but rather the informant should be made available for trial or for a defense counsel interview beforehand.[174]

Why would a defendant want to know the identity of an informant or cooperating witness if the witness will not be testifying at trial? Many times, the defendant wants to know the identity of the person who gave him up to the police, which can put the cooperator at risk for retaliation. Or, the defendant simply wants to know how they got caught so they can learn not to make the same mistake in the future. Usually, the defendant will be able to gather who the "informer" is from the law enforcement reports that are turned over during discovery.

B. Title III Wiretap Interceptions

Another common investigatory tool is to use a Title III wiretap to gather sufficient probable cause[175] against a particular target or group of individuals involved in drug trafficking and money laundering activities. Oftentimes, a wire intercept will reveal new players in a drug trafficking conspiracy and create spin-off investigations.

Title 18 U.S.C. §§ 2510-21 governs the lawful interception of wire and electronic communications.[176] To obtain authorization for the interception of wire or electronic communication, the affidavit must allege a violation of a federal offense[177] and must disclose the identities of the

169. United States v. Tenorio-Angel, 756 F.2d 1505, 1509 (11th Cir. 1985).

170. United States v. Gutierrez, 931 F.2d 1482, 1490–91 (11th Cir. 1991).

171. *Id.* at 1491; United States v. Staufer, 38 F.3d 1103 (9th Cir. 1994); United States v. Warren, 42 F.3d 647 (D.C. Cir. 1994).

172. United States v. Kerris, 748 F.2d 610, 613–14 (11th Cir. 1984); United States v. Gaston, 357 F.3d 77, 84 (D.C. Cir. 2004); McLawhorn v. North Carolina, 484 F.2d 1, 5 (4th Cir. 1973).

173. *Gutierrez*, 931 F.2d at 1491.

174. United States v. McDonald, 935 F.2d 1212 (11th Cir. 1991).

175. *See supra* text accompanying note 45.

176. 18 U.S.C.A. § 2510 (2000 & Supp. 2014) defines types of communication that can be intercepted. Wire communications are those communications that pass through a telephone line/wire while electronic communications refer to the interception of non-voice communications such as text messaging, email, fax, and over the internet.

177. To obtain authorization of the interception of wire communications, the federal offense must be listed in 18 U.S.C.A. § 2516(1) and listed in 2516(3) (2000 & Supp. 2014) for the interception of electronic communications.

targets, their criminal behavior, and how the targeted device/facility (phone, email account, etc.) is used in furtherance of the criminal activity.[178] An affidavit for a Title III wiretap is extensively reviewed within the United States' Attorney's Office before the Criminal Division's Office of Enforcement Operations reviews it.[179] Once the affidavit is finalized, a Deputy Assistant Attorney General must review the affidavit and authorize the prosecutor to proceed to seek approval from the district court judge.[180]

Many times, multiple wiretaps targeting one large drug trafficking or money laundering operation are being monitored at the same time. Agents attempt to keep these wiretaps under wraps until the entire investigation is finished. If it is a multi-district investigation, a significant amount of coordination is needed to ensure all wires and arrests are completed at the same time or risk defendants becoming fugitives, warning other targets, and destroying evidence.

In order to prevent the wire from being disclosed but developing additional evidence outside the wire, agents will "wall off" the wiretap and have state and local police initiate a traffic stop and collect evidence. Police must find their own probable cause to stop the vehicle (e.g., observe a traffic violation) rather than use any probable cause that comes from a particular conversation on the wire. It is irrelevant whether the police would have stopped the vehicle under the general practice of the police department[181] or whether the officer may have had other subjective motives for stopping the vehicle as long as they had probable cause to believe a traffic law was violated.[182]

For example, during a particular intercepted conversation, a target may refer to "twenty window panes" that he will deliver tomorrow at three p.m. to a particular location. Agents have previously surveilled the target's home and know which car he drives. The agents working the case alert the local state trooper as to the particular car and the area where it might be found at three p.m. The following day, the state trooper identifies the target's car on the highway and observes him speeding. The target is issued a speeding ticket and consents to the search of his car. The officer finds twenty kilograms of cocaine hidden underneath the back seat of the car. If the cocaine is seized and the target is free to leave, the wiretap need not be disclosed. If the target is subsequently arrested, the wiretap need not be disclosed until the discovery process and, even then, it is possible that state discovery rules may delay discovery or not require

178. 18 U.S.C.A. § 2518 (2000).

179. DEP'T OF JUSTICE, U.S. ATTORNEYS' MANUAL (USAM), TITLE 9, CRIMINAL RES. MANUAL 29, *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00029.htm.

180. *Id.*

181. United States v. McRae, 81 F.3d 1528, 1533 (10th Cir. 1996).

182. Whren v. United States, 517 U.S. 806 (1996).

disclosure unless exculpatory evidence exists on the wire.[183]

There have also been occasions in which a Title III wiretap has not been disclosed in a search warrant affidavit, even though it was part of the probable cause used to obtain the warrant in order to protect ongoing investigations. Instead, the source of the information has been said to come from a confidential informant rather than the true source, the Title III wiretap.[184] The key to approval hinged on whether the agent informed the magistrate judge of the information's true source before the magistrate signed the warrant. In *United States v. Glinton*,[185] the Eleventh Circuit stated:

> In a broad generic sense, the wiretap served as a reliable provider, or "informant," of information. If there had been a live confidential informant under the circumstances set forth here, the government would not have been required to reveal the informant's name. We certainly do not condone a position that it is proper to lie under oath in a search warrant affidavit as long as the affiant orally tells the truth to the issuing magistrate judge. However in this instance, we do not feel that the warrant should be suppressed because the magistrate judge was not "misled by information." The fact that a wiretap was the basis for gaining confidential information does not detract from the reliability or veracity of the source. In fact, upon learning of the means by which this information was obtained, the magistrate judge could gain reassurance as to the veracity of the information.[186]

While Title III affidavits must be placed under seal, the government may use information from Title III affidavits or recordings in arrest warrants, search warrants, complaints, indictments, and trial briefs.[187] When Title III affidavits or documents containing Title III information must be disclosed in response to discovery requests, the government may seek a protective order asking the court to redact or keep the pleadings sealed if there are ongoing investigations that may be compromised.[188] Defense counsel may also be precluded from sharing contents of the Title III affidavit and recordings with others outside the defendant and the defense team.[189]

---

183. If a federal prosecution ensues, the recordings of the defendant on the wiretap will eventually be disclosed under FED. R. CRIM. P. 16(a)(1)(B)(i).

184. United States v. Cruz, 594 F.2d 268, 271–72 (1st Cir. 1979); United States v. Leon, 468 U.S. 897, 923 (1984); State v. Beney, 523 So. 2d 744, 745 (Fla. Dist. Ct. App. 1988); *cf.* United States v. McCain, 271 F. Supp. 2d 1187, 1193 (N.D. Cal. 2003) ("Courts have rejected the notion that law enforcement may make misrepresentations in warrant affidavits in order to protect the confidentiality of their sources."); United States v. Broward, 594 F.2d 345, 351 (2d Cir. 1979) ("We emphatically do not condone the insertion of false material into affidavits for arrest or search warrants. Such an egregious practice defeats the whole point of the procedure, having a judicial officer make an independent assessment of whether probable cause exists.").

185. 154 F.3d 1245 (11th Cir. 1998) (where the magistrate did not know that the "confidential source" was actually a wiretap).

186. *Id.* at 1255 (citation omitted).

187. 18 U.S.C.A. § 2517(1)–(2) (2000 & Supp. 2014).

188. CIPA, *supra* note 146, § 4.

189. *Id.*

C. Toll Records/Phone Log Data[190] via Administrative or Grand Jury Subpoena and Phone Log Databases

Many investigations begin as spin-offs from other investigations. For example, a target whose phone calls are being intercepted by the DEA is found calling an individual who happens to be distributing narcotics in another area of town or different district and is looking for another supplier. An agent would then request toll records from the individual's phone provider and see if there are any additional links between the individual's phone and other "known" drug distributors, buyers, suppliers, or co-conspirators. Toll records can include the date, time, and duration of incoming and outgoing phone numbers of calls.[191] If the agent finds sufficient information from toll records, as well as from surveillance, cooperating witnesses, and informants, then the agent may want to place a trap and trace[192] or pen register device[193] on that particular phone number to capture the phone numbers of all incoming and outgoing calls to that particular number. By doing this, the agent is attempting to see if there are any connections between this individual and a drug trafficking organization. Wire interceptions of the new phone number may be necessary in order to further identify co-conspirators, supervisors or suppliers, or understand the scope of the ongoing conspiracy.

The Reuters article indicated that some of the leads sent out to the field came from a phone log and Internet data database, which contains approximately one billion records that were gathered legally by the DEA

190. Meaning "any record (except a record pertaining to content) maintained by an electronic communication service provider identifying the telephone numbers called from a particular telephone or attributable to a particular account for which a communication service provider might charge a service fee. The term includes but is not limited to all records maintained of individual calls made from a particular telephone or attributed to it that are or could be the subject of a particularized charge depending upon the billing plan offered by the provider and accepted by the customer. In other words, the term is broad enough to cover all records of calls from or attributed to a particular number regardless of whether, in fact, a separate charge is assessed for each call. *In re* Grand Jury Subpoenas to Sw. Bell Mobile Sys., Inc., 894 F. Supp. 355, 356 (W.D. Mo. 1995). 18 U.S.C.A. § 2709 (2000 & Supp. 2014) governs access to telephone toll and transactional records.

191. *See Toll Records*, Am. Civil Liberties Union, https://www.aclu.org/files/cellphonetracking/20120328/celltrackingpra_renopd_renonv_4.pdf.pdf (last visited June 5, 2015).

192. "[T]he term 'trap and trace device' means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication." 18 U.S.C.A. § 3127(4) (2000 & Supp. 2014).

193. [T]he term 'pen register' means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business. 18 U.S.C.A. § 3127(3).

through "subpoenas, arrests and search warrants nationwide."[194]

The Office of the Inspector General (OIG) on its own website stated:

> The OIG is examining the DEA's use of administrative subpoenas to obtain broad collections of data or information. The review will address the legal authority for the acquisition or use of these data collections; the existence and effectiveness of any policies and procedural safeguards established with respect to the collection, use, and retention of the data; the creation, dissemination, and usefulness of any products generated from the data; and the use of 'parallel construction' or other techniques to protect the confidentiality of these programs.[195]

The concern here is similar to the concern of the collection of data by the NSA—the DEA is collecting various metadata on citizens, compiling it into one database, and accessing the data at will. However, the DEA acquired its information legally and in a different manner, i.e., via administrative and grand jury subpoenas issued during particular investigations. Subscriber-type information and billing records may be obtained on a case-by-case basis via administrative or grand jury subpoena pursuant to 18 U.S.C. § 2703(c)(1)(C). Federal Rule of Criminal Procedure 17(c) provides that the court can quash or modify the subpoena for records on a particular investigation if compliance would be unreasonable or oppressive. On the other hand, the NSA database as described by Snowden, including data about every telephone call placed inside the United States, "is not used for domestic criminal law enforcement,"[196] and is not collected via subpoena power on a case-by-case basis but is gathered up wholesale from internet and telephone carriers' systems. Thus, NSA and DEA databases are entirely different.

The question becomes whether DEA should be able to hold onto the subpoena results after that particular investigation has been completed and whether that information can be compiled into one large database, which can later be accessed during other investigations. In essence, the database is streamlining the subpoena process so agents will not have to wait for results from telecommunications providers and can re-access information that has already been requested via subpoena and received from third parties. Telephone and Internet providers can sometimes take weeks to process toll record requests. If the records are already available in a database, agents will be able to make connections between targets of investigations quickly and attempt to "keep up with drug dealers when they switch phone numbers to try to avoid detection."[197]

---

194. Shiffman & Cooke, *supra* note 2.

195. *Ongoing Work*, DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GEN., DRUG ENF'T ADMIN., http://www.justice.gov/oig/ongoing/dea.htm (last visited Aug. 29, 2014).

196. Ingram & Shiffman, *supra* note 144.

197. Scott Shane & Colin Moynihan, *Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.'s,* N.Y. TIMES, Sept. 1, 2013, at A1, *available at* http://www.nytimes.com/2013/09/02/us/drug-agents-use-vast-phone-trove-eclipsing-nsas.html?pagewanted=all&_r=0 ("[R]ecords are maintained at all times by the phone company, not the government. . . .

Clearly, collecting legally acquired subscriber information from individual subpoenas into one database is cost effective. Third party service providers more than likely will not preserve this data for a significant period of time, and if asked to do so, would more than likely require a hefty fee from the government or pass the cost onto the consumer. Then, the data would be placed into a third party's hands with little or no oversight compared to government oversight of the database by entities such as Congress and the Office of the Inspector General (OIG).

As for discovery concerns, there does not appear to be any requirement under Federal Rule of Criminal Procedure 16 (Rule 16) to turn over toll records unless they will be used at trial or for some reason they would be considered exculpatory.

D. Foreign Government Lawful Wiretaps

Foreign government wiretaps could be useful to U.S. domestic law enforcement agents. Foreign wire intercepts, similar to out-of-state wire intercepts, potentially provide information as to new co-conspirators in a large drug trafficking organization. This information could be useful in the initiation of new investigations, provide support to ongoing local investigations through the use of search warrant or wiretap applications, and used as evidence at trial.[198]

Some foreign law enforcement agencies conduct unauthorized wiretaps for intelligence purposes. "In those cases, the foreign authorities may not allow the wiretap evidence to be used in an American court or referenced in search warrant affidavits or Title III affidavits."[199] Also, procedures in foreign countries may be different from the way a wiretap is conducted in our domestic investigations–there may be circumstances in which the U.S. prosecutor is unable to obtain all recordings or legal documents requesting and granting authorization for the foreign wiretap.[200]

Courts have held that Title III standards do not apply to electronic interceptions conducted outside the United States. Title III and its requirements of probable cause and procedures such as minimization, periodic reports, and the sealing of recordings, do not apply to wiretaps conducted by foreign authorities in their own countries.[201]

[Hemisphere] simply streamlines the process of serving the subpoena to the phone company . . . .").

198. In *United States v. Moreno*, information about an imminent heroin transaction in New York was obtained from a Colombian wiretap and was passed from a DEA agent in Colombia to a DEA agent in New York. 08-CR-605, 2009 WL 454548 (E.D.N.Y. Feb. 24, 2009) *aff'd*, 701 F.3d 64 (2d Cir. 2012). In examining whether probable cause existed for the arrest, the court found the Colombian wiretap to be reliable and that the information from the wiretap had been independently corroborated by the agents in New York during their surveillance of the target. *Id.*

199. Larry Schneider, *Obtaining and Using Foreign Wiretap Evidence* § 40.2, *in* U.S. Dep't of Justice, Federal Narcotics Prosecutions 926 (Mar. 2011).

200. *Id.* at 929.

201. United States v. Maturo, 982 F.2d 57, 60 (2d Cir. 1992); United States v. Peterson, 812 F.2d 486, 492 (9th Cir. 1987).

Since foreign police in their own respective countries obtain foreign wiretap evidence, foreign wiretap evidence can only be excluded at trial if the conduct of the foreign agents shocks the conscience of the U.S. court or if U.S. law enforcement officers substantially participate in the foreign search.[202]

Discovery rules would apply as they do in domestic wiretap scenarios. Recordings of the defendant must be turned over under Rule 16.

E. Synopsis

Similar to the more familiar and established methods and sources used by law enforcement to collect information and develop probable cause to initiate a criminal investigation, other tools used by the DEA such as court-approved domestic wiretaps, foreign government wiretaps, and phone log databases are also legal forms of case-initiation and may or may not be potentially discoverable according to Rule 16 and case law.

Anonymous tips, the identity of informants, and toll records would not be considered discoverable under Rule 16 and need not be turned over to the defense if they will not be used at trial. However, a prosecutor must disclose the evidence if it is favorable to the defendant, material to the defense, and it goes to the defendant's guilt or punishment.[203] Failure to disclose such evidence, whether it is willful or inadvertent on the part of the prosecution, violates due process and is grounds for reversing a conviction if the defendant can prove that non-disclosure was prejudicial to his defense when the outcome would have been different if the undisclosed evidence had been presented at trial.[204] It is highly unlikely that an anonymous tip or toll records would ever contain exculpatory evidence. If an informant has exculpatory evidence on a defendant, that information would clearly need to be turned over to the defense. However, an informant's identity, as previously mentioned, need not be disclosed unless the informant plans on testifying or the defense needs this information because it is "helpful" to its defense.[205]

Title III wiretaps and foreign wiretaps, on the other hand, implicate Rule 16 if the wiretaps contain a recorded statement made by the defendant, if "the statement is within the government's possession, custody or control," and "the attorney for the government knows—or through due diligence could know—that the statement exists."[206] These statements must be turned over regardless of whether the government intends to use the statements at trial.[207] Moreover, the recordings may have exculpatory evidence favorable to the defendant.

---

202. United States v. Rosenthal, 793 F.2d 1214, 1230 (11th Cir. 1986); *Maturo*, 982 F.2d at 60; United States v. Barona, 56 F.3d 1087 (9th Cir. 1995).
203. Brady v. Maryland, 373 U.S. 83, 87 (1963).
204. *Id.*; United States v. Bagley, 473 U.S. 667 (1985).
205. Roviaro v United States, 353 U.S. 53, 59 (1957).
206. Fed. R. Crim. P. 16(a)(1)(B)(i).
207. United States v. Safavian, 233 F.R.D. 12, 14 (D.D.C. 2005).

Thus, the greatest concern discussed in the Reuters article lies in DEA's use of NSA intercepts and other classified material which is used to initiate criminal investigations but this fact is not disclosed to the defense.

IV. THE LEGALITY OF "PARALLEL CONSTRUCTION" AND THE USE OF NSA INTERCEPTS TO INITIATE CRIMINAL INVESTIGATIONS

A. "Parallel" versus "Consecutive" Construction

Because the initial method of collection by the NSA is conducted separate and apart from the subsequent DEA domestic investigation, the term "parallel construction" is inappropriate. Rather, the term "consecutive construction" is better suited in this context. The initial collection intent is for intelligence, for foreign law enforcement purposes, or for other positive intelligence investigations, and then relevant and substantive information may be passed on to SOD for further evaluation.[208] The information is then analyzed, and a determination is made as to whether it might be useful to other field investigations.[209] Relevant information is extracted from these sources and sent to the field with sufficient predication to encourage the field agent to begin an investigation. Thus, there is no parallel investigation, but rather one in which information from one potentially classified source is used to initiate a new criminal investigation. Once that investigation is initiated, the field agent develops his or her own evidence, issuing subpoenas, conducting surveillance, interviewing witnesses, and developing probable cause in order to initiate a wiretap or conduct a search or an arrest.

B. Step 1: Was the NSA Intercept Legally Authorized at the Time of Interception?

In evaluating the legality of this practice, we must determine whether the NSA information disclosed to law enforcement was collected and accessed legally. From what has been publicly revealed, targets seem to be monitored via FISA or section 702 authorization or Executive Order 12,333 (E.O. 12,333) if it is a foreign target intercepted overseas. For example, a foreign narco-trafficker in Colombia speaking to an associate in Mexico could be intercepted without a FISA warrant.[210] A call between a targeted Colombian trafficker and a domestic distributor is more of a concern since the latter suspect may be a U.S. person who may later be a target of a criminal investigation. It is also possible that the targeted Colombian trafficker may be intercepted and extradited to the United States to also face drug trafficking charges under Title 18 United States Code section 959.

208. Shiffman & Cooke, *supra* note 2.
209. *Id.*
210. USSID 18, *supra* note 50; Exec. Order No. 12,333, *supra* note 31.

1. Lawful NSA Intercept

If the information was collected and accessed legally under FISA or 702 or E.O. 12,333, the only outstanding concern is whether we approve the policy of intelligence sharing between the IC and the domestic law enforcement community. Should the IC, including the NSA, share intelligence with law enforcement agents involved in wholly domestic criminal investigations? It is highly likely if the NSA targets a foreign narco-trafficker that it may inadvertently collect information on domestic distributors. If it is lawful for the NSA to collect data when there is a significant foreign intelligence purpose, should NSA be allowed to pass along any and all legally collected data, which may prove helpful to local law enforcement, even when the information collected contains U.S. person information?

The 9/11 Commission was clear in its recommendation that the "wall" be torn down between the IC and domestic law enforcement.[211] However, the Commission used the example of FBI agents, some working foreign counterintelligence and others working criminal cases that were involved in closely connected investigations, and those agents conducting foreign counterintelligence were unable to share classified information with criminal agents who were only cleared to view evidence that could be used in court.[212]

Perhaps IC information should only be passed on to those involved in terrorism cases as specified in the section 215, which describes the metadata collection program. That would allow FBI agents working on terrorism and espionage cases to have access to the information they need to conduct additional domestic terrorism investigations and hopefully prevent another 9/11 from occurring, but also preclude local law enforcement uninvolved in terrorism investigations from accessing intelligence gathered by the IC. On the other hand, why should legally obtained intelligence information relevant to criminal activity in the U.S. be withheld from domestic law enforcement merely because the suspect is not a terrorist but rather a garden-variety criminal?

Part of the DEA's mission is to work narco-terrorism cases. So far, there have been several defendants indicted under the 21 U.S.C. § 960(a) narco-terrorism statute. To name a few, Corredor-Ibaque was the first to be indicted under the statute. He was a Colombian trafficker and member of the FARC, an armed and violent organization that is engaged in armed conflict against the government of the Republic of Colombia.[213] Jimenez-Naranjo was a high-ranking leader of the Autodefensas Unidas de Colombia (AUC), which is a Colombian right-wing paramilitary and

211. 9/11 COMMISSION REPORT, *supra* note 33.

212. *Id.* at 96.

213. Superseding Indictment at 1, United States v. Corredor-Ibague, No. 04-212 (D.D.C. Oct. 26, 2006), 2005 WL 6227984; Dep't of Justice, *High-level Columbian Drug Trafficker Sentenced to 194 Months in Prison*, Sept. 16, 2013, http://www.justice.gov/opa/pr/2013/September/13-crm-1029.html.

drug trafficking organization.[214] Khan Mohammed was an associate of the Taliban, an organization which "engage[d] in drug trafficking in order to finance the acquisition of weapons, ammunition and equipment necessary to conduct its attacks on coalition forces, the Afghan government and anyone else who stands in their way."[215] Even though the narco-terrorism statute was not created until 2006,[216] Congress must have considered the DEA a likely user of IC-gathered information because part of the NSA's mission as described in Executive Order 12,333 is "to collect information concerning, and conduct activities to protect against, international terrorism, proliferation of weapons of mass destruction, intelligence activities directed against the United States, [and] *international criminal drug activities*".[217] The IC is directed to "participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers, or international terrorist or narcotics activities."[218]

Intelligence sharing has its benefits. Why should law enforcement not receive the benefit of intelligence initially derived for a different purpose? Perhaps rather than simply permitting any evidence of a crime to be passed on, Congress should elaborate on what particular crimes it deems sufficiently serious to justify the sharing of IC-related information with domestic law enforcement. One repercussion of re-building the wall (partially or otherwise) would be the reinstitution of the IC's old ways—remaining tight-lipped and highly protective of its own intelligence, which serves merely as a resource for government policy makers. Former NSA director Vice Admiral Bobby Inman described the NSA as "a loner organization" that "is often reluctant to share [classified materials] with others lest a leak spoil their ability to get that kind of information again."[219] Again, assuming the intelligence was collected legally, should we then cover our eyes and enact institutional amnesia? If we agree some sort of intelligence sharing should be permitted, the question left for debate becomes who should be entitled to IC information and what should be required of the potential user before access.

---

214. Indictment at 2–3, United States v. Jimenez-Naranjo, No. 05-235 (D.D.C. Sept. 25, 2007).

215. Superseding Indictment at 2, United States v. Mohammed, No. 06-357 (D.D.C. Jan. 23, 2008), 2008 WL 5979391; Government's Memorandum in Aid of Sentencing at 1–2, United States v. Mohammed, No. 06-357 (D.D.C. Aug. 26, 2008), 2008 WL 5979405.

216. USA PATRIOT Improvement and Reauthorization Act of 2005 § 122, 21 U.S.C.A. § 960a (2013) (creating a new offense covering narco-terrorism).

217. Exec. Order No. 12,333, *supra* note 31, § 1.4 (emphasis added). "The heads of elements of the Intelligence Community shall: '(g) Participate in the development of procedures approved by the Attorney General governing production and dissemination of information or intelligence resulting from criminal drug intelligence activities abroad if they have intelligence responsibilities for foreign or domestic criminal drug production and trafficking . . . .'" *Id.* § 1.6. Procedures set forth in Part 1 of this Executive Order "shall permit collection, retention, and dissemination of the following types of information: . . . (c) Information obtained in the course of a lawful foreign intelligence, counterintelligence, international drug or international terrorism investigation." *Id.* § 2.3.

218. *Id.* § 2.6.

219. AID, *supra* note 69, at 163.

2. Unlawful NSA Intercept

If the NSA intercept was collected and/or accessed illegally, then the question becomes whether the initial illegality on the intelligence side should prevent law enforcement from using that information on the domestic, criminal investigation side. Should the initial illegality by the NSA taint any subsequent evidence found as a result of the initial intelligence, or does this fall under the independent source exception to the exclusionary rule?

Despite the fact that agents entered a warehouse without a search warrant and discovered a bale of marijuana, the Court in *Murray v. United States* found that the subsequent search with a warrant was lawful; the subsequent search warrant was based upon probable cause and was completely separate and apart from the illegal initial search, and therefore, the exclusionary rule did not apply.[220] The Court did not appear concerned that agents might get in the habit of conducting illegal searches prior to obtaining a search warrant. Rather, the Court felt there was a disincentive for police to initially conduct illegal searches prior to seeking a search warrant.[221] Justice Scalia wrote,

> An officer with probable cause sufficient to obtain a search warrant would be foolish to enter the premises first in an unlawful manner. By doing so, he would risk suppression of all evidence on the premises, both seen and unseen, since his action would add to the normal burden of convincing a magistrate that there is probable cause, the much more onerous burden of convincing a trial court that no information gained from the illegal entry affected either the law enforcement officers' decision to seek a warrant or the magistrate's decision to grant it. Nor would the officer without sufficient probable cause to obtain a search warrant have any added incentive to conduct an unlawful entry, since whatever he finds cannot be used to establish probable cause before a magistrate.[222]

Using the above argument in the context of this article, those conducting the illegality would be the IC, and there would be repercussions on the intelligence side as monitors/analysts would suffer possible criminal penalties for their hypothetical misdeeds, but the illegally obtained information would be passed on to domestic law enforcement without its knowledge as to the origins of that information. Those conducting a criminal investigation would have no way of knowing how the information was gathered, as they are separate and apart from the IC and the information was presumably scrubbed and analyzed by the SOD before being sent out to the field. The information received would not be used as probable cause or as evidence in the criminal case, since probable cause would be developed under the "consecutive construction" technique. Therefore, the exclusionary rule would not apply even though the information in this

220. 487 U.S. 533, 537 (1988).
221. *Id.*
222. *Id.*

hypothetic example was obtained illegally. Even so, the best course of action would be to discard or ignore IC-collected information in this instance and thereby avoid any hint of impropriety. As it currently stands, FISA warrants, E.O. 12,333, and section 702 interceptions are legal and so if the NSA intercepts described in the Reuters article fall into one of these three categories, such concern regarding illegalities are unwarranted.

C. Step 2: Potential Disclosure of NSA Intercepts

Assuming we find the use of NSA intercepts (lawful or unlawful but permissible) to be an acceptable tool to initiate criminal investigations, should the NSA intercepts be disclosed to the defense?

We must first assume that the NSA intercept will not be used as evidence at trial. According to the Reuters article, the IC information is being used to initiate criminal investigations and is not used as a substitution for substantive evidence that can be used at trial.[223] Therefore, this is an entirely different scenario than those joint FBI cases in which information collected initially for foreign intelligence is then woven into a domestic terrorism case through the use of CIPA section 6. Section 6 allows the prosecution and defense to request that classified material be used at trial and rather than revealing the true source or identity of the information, either side is permitted to submit a "substitution" that the judge deems adequate.[224] At trial, the evidence is automatically entered into evidence without establishing the typical evidentiary foundations, and the jury is not aware of the actual source in order to protect the IC's sources and methods.[225]

Rather, the case here involves CIPA section 4 and a prosecutor's discovery obligations. If the material is discoverable, then the original IC material should be disclosed to the defense. However, under CIPA section 4[226] and Federal Rule of Criminal Procedure 16(d)(1),[227] the prosecution may file an ex parte motion to have the original classified material protected from disclosure or if discoverable, "substituted" and revealed in another form to protect the IC's sources and methods. This process is very similar to the prosecution's request for a protective order and denial

223. Shiffman & Cooke, *supra* note 2.

224. CIPA, *supra* note 146, § 6.

225. *Id.*

226. "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 . . . . The court may permit the United States to make a request for such authorization to be inspected by the court alone." CIPA, *supra* note 146, § 4.

227. "At any time the court may, for good cause, deny, restrict, or defer discovery or inspection, or grant other appropriate relief. The court may permit a party to show good cause by a written statement that the court will inspect ex parte. If relief is granted, the court must preserve the entire text of the party's statement under seal." Fed. R. Crim. P. 16(d)(1).

of defendant's request to disclose an informant's identity. In fact, this analogy was made in *United States v. Yunis:*

> We hold, in short, that classified information is not discoverable on a mere showing of theoretical relevance in the face of the government's classified information privilege, but that the threshold for discovery in this context further requires that a defendant seeking classified information, like a defendant seeking the informant's identity in *Roviaro*, is entitled only to information that is at least helpful to the defense of the accused.[228]

The only appellate case that seems to have addressed this exact topic is *United States v. Mejia*, in which following a jury trial, defendant Rafael Mejia was convicted of "conspiring to distribute five or more kilograms of cocaine with the knowledge and intent that such cocaine would be unlawfully imported into the United States, in violation of 21 U.S.C. §§ 959(a), 960(a)(3), 960(b)(1)(B)(ii) and 963."[229] "The investigation involved multiple wiretaps, which captured Colombian nationals Mejia and Rios discussing large drug transactions with other members of their drug trafficking organization."[230] In *Mejia*, the court issued an order notifying the parties that ex parte filings had taken place and asked counsel for both sides (who had been unaware of the previous filings) to file briefs "addressing 'whether, to what extent, and under what circumstances CIPA § 4 and Federal Rule of Criminal Procedure 16(d)(1) authorize the non-disclosure of information otherwise arguably subject to discovery under Rule 16.'"[231] While the defendants argued that they should be entitled to view the classified material in order to make an intelligent argument before the court, the court pointed out that CIPA section 4 governs only the discovery of classified information.[232] CIPA section 4 permits the judge to make such a decision ex parte.[233] The court referred to the House Report on CIPA, which stated, "'[s]ince the government is seeking to withhold classified information from the defendant, an adversary hearing with defense knowledge would defeat the very purpose of the discovery rules.'"[234]

Upset that neither side had been aware of such classified material existing prior to the appeal, the appellate court reminded the defendants that the district court had, in fact, reviewed the material prior to trial, and coupled with the Circuit court's de novo review, this "made up for any defici[ency] in that regard."[235] And, "[m]ore fundamentally, because the underlying classified material is unhelpful to the defendants, they did not suffer from its unavailability; and because that material was never shown

228. 867 F.2d 617, 623 (D.C. Cir. 1989).
229. 448 F.3d 436, 439 (D.C. Cir. 2006).
230. *Id.* at 438.
231. *Id.* at 454.
232. *Id.* at 454, 457.
233. *Id.* at 457.
234. *Id.* (quoting H.R. REP. NO. 96-831, pt. 1, at 27 n.22 (1980)).
235. *Id.* at 459.

to the jury, 'there is no question here of convictions based upon secret evidence furnished to the fact-finder but withheld from the defendants.' "[236]

Upon evaluating the classified material in order to determine whether a protective order was necessary or whether the material was, in fact, discoverable, the court agreed that the appropriate test was the *Roviaro* informant's privilege test. The court evaluated the discoverability of the material using a three part test: (1) did the information "cross the low hurdle of relevance?" (2) was "the assertion of privilege by the government . . . at least a colorable one?" and (3) was the information at least "helpful to the defense of the accused" as defined in *Roviaro*?[237] The court found that while the material was relevant and that the government had a privilege, the classified material fell short of the " 'helpful or beneficial character' necessary to meet the threshold showing for overcoming the privilege."[238]

If the IC information is not exculpatory, not helpful to the defense in preparation for trial, and will not be used as evidence at trial, there is no reason why the prosecution must disclose the information (in original form or otherwise). For example, if the NSA intercepts a conversation between a Colombian trafficker (the NSA target) in Colombia and a domestic distributor (the target of a subsequent criminal investigation), and the distributor makes inculpatory statements, there need be no disclosure. Under CIPA § 4, the prosecution could request a protective order to prevent such disclosure since the information does not fall under *Brady* or *Giglio*, nor is it "helpful to the defense" as defined in *Roviaro*. While Rule 16(a) requires disclosure of all recordings/statements of the defendant, the statements were made prior to the criminal investigation and will not be used as part of the evidence at trial.

However, in a second scenario, assume the Colombian trafficker told the distributor, "If you don't distribute my drugs, I will kill your family." This is evidence of illegal activity and, despite signs of clear duress, this information is passed on to law enforcement and they choose to prosecute the distributor when they learn he is head of a large drug distribution ring. (This would seem extremely unlikely.) That statement must be disclosed in some form. CIPA § 4 requires disclosure and permits the disclosure in substituted form as the defense may want to use this duress evidence at trial.[239]

Lastly, in a third scenario, assume the Colombian trafficker contacts an alleged distributor, and as he speaks about the drug trafficking operation with this distributor, the distributor says, "I have no idea what you are talking about. You have the wrong number." This, of course, would be exculpatory and should be disclosed; however, this type of information is

236. *Id.* (quoting United States v. Innamorati, 996 F.2d 456, 488 (1st Cir. 1993)).
237. *Id.* at 455–56 (quoting *Roviaro*, 353 U.S. at 60–61).
238. *Id.* at 456.
239. CIPA, *supra* note 146, § 4.

also unlikely to be passed to law enforcement in the first place due to its exculpatory nature. There is no domestic target to be investigated.

Defense attorneys have argued under scenario one that they need this type of protected information to ensure there is no entrapment, or that this protected information may have resulted in a mistake or bias. But this argument is difficult to justify. The defense is much more likely to encounter entrapment, mistake, or bias in a situation where information from an informant or spouse, family member, or a friend's tip to law enforcement initiated the investigation. A wire intercept, email, or even "metadata" collected by the NSA is much less "biased" than an informant who has a motive to lie/stretch the truth when it suits his or her needs.

The question to be asked is why does defense counsel really need this inculpatory yet non-evidentiary information? It could be curiosity, which is one of the reasons why many defendants want to know an informant's identity. Another reason could be because introducing an NSA intercept into the proceedings could muddy the waters at trial and cause the jury to focus on public outrage at the NSA's power, potential abuse, and their fears that the government has become a surveillance state.[240] Or, the defense does not trust that the government will turn the information over to the court for review and that the judge will be able to make a neutral decision on the issue without the defense's perspective. After all, the only party fully aware of what might be "helpful" to the defense is the defendant himself.

The lack of adversarial testing is always listed as the greatest concern regarding CIPA section 4 decisions during which defense counsel is neither provided notice nor asked for input. This concern was raised in the 5-4 Supreme Court decision, *Clapper v. Amnesty International*.[241]

In *Clapper*, the plaintiffs challenging the 702 program were unable to prove they had standing because the government never disclosed whether in fact the defendants had ever been intercepted under 702. The FAA (section 702) allows the use of evidence derived from FISA surveillance in criminal prosecutions.[242] However under FISA, the government must provide notice of its intent to use evidence obtained and derived from electronic surveillance pursuant to FISA orders.[243] The Solicitor General Donald B. Verrilli Jr. assured the Court that if the plaintiffs had been surveilled, the government would, in fact, provide notice if the government intended to "use or disclose information obtained or derived from" FISA or 702 surveillance so that "the affected person may challenge the

240. Challenging an NSA intercept's legality makes sense in a case in which the evidence derived from the intercept will be used against the defendant at trial, but it makes little sense when the information from the intercept will not be used and was not a part of the criminal investigation.

241. 133 S. Ct. 1138 (2013).

242. 50 U.S.C.A. §§ 1806(a), 1825(a).

243. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *supra* note 122.

lawfulness of the acquisition."[244] The Court accepted Verrilli's assurances as true and found the plaintiffs had no standing to challenge the 702 surveillance program since they could not prove they had been intercepted.[245]

Since *Clapper*, Verrilli learned that in some cases, the government had not provided notice to defendants.[246] The National Security Division has since changed its practice and has begun to provide full notice to defendants in cases where evidence used at trial derived from FISA or 702 programs.[247]

In the case of parallel construction, the evidence obtained or derived from the FISA or 702 surveillance is not intended to be used in judicial or administrative proceedings. It is merely being used to initiate a criminal investigation at which time law enforcement is developing separate evidence apart from the IC surveillance. Therefore, there is a significant difference between CIPA section 6 in which the government intends IC evidence to be used at trial where opposing counsel's input is required, and CIPA section 4 where the government does not intend to use IC evidence, nor is the evidence used at trial derived from IC evidence, because law enforcement initiated their own criminal investigation separate and apart from the original IC evidence. Classified material is not to be used as facts to support a search warrant or arrest, and therefore, evidence used at trial is not "derived from" FISA or 702 surveillance.

In this instance, defense counsel's input is not as critical, since the judge is merely making a determination as to whether the IC information is discoverable. Judges make these determinations frequently under Rule 16, which allows judges to make discovery decisions ex parte while also preserving the entire text for appellate purposes.[248]

However, the government must justify its reasons for requesting an ex parte decision. Why does the government want to protect this type of intelligence and are its concerns justified? Does the IC want to protect its sources and methods, or does the IC merely want to prevent legitimate scrutiny of certain NSA programs? If defense counsel and defendants were given the ability to access these intercepts, underlying FISA warrants, and details as to what, when, how, and when calls are intercepted and information collected, the IC would face more questions, more scrutiny and uncertainty, causing the IC to further justify both legally and

244. Transcript of Oral Argument at 4:12-17, Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013) (No. 11-1025); *see also Clapper*, 133 S. Ct. 1138 at 1154.

245. *Clapper*, 133 S. Ct. at 1154–55.

246. Adam Liptak, *A Secret Surveillance Program Proves Challengeable in Theory Only*, N.Y. TIMES, July 17, 2013, at A11, *available at* http://www.nytimes.com/2013/07/16/us/double-secret-surveillance.html?pagewanted=all&_r=0.

247. Devline Barrett, *U.S. Spy Program Lifts Veil in Court*, WALL ST. J., July 31, 2013, http://on.wsj.com/19nu8KC; Charlie Savage, *Federal Prosecutors, in a Policy Shift, Cite Warrantless Wiretaps as Evidence*, N.Y. TIMES, October 27, 2013, at A21, *available at* http://www.nytimes.com/2013/10/27/us/federal-prosecutors-in-a-policy-shift-cite-warrantless-wiretaps-as-evidence.html.

248. FED. R. CRIM. P. 16(d)(1).

morally their classified programs in the aftermath of the Snowden disclosures. The protection of sources and methods is the only legitimate justification for the government's request to withhold this type of information from defense counsel, and the basis for the judge's order of nondisclosure.

V. CONCLUSION

As it currently stands, there is nothing prohibiting the DEA from utilizing NSA intercepts under FISA or 702 or E.O. 12,333 as tips to initiate criminal investigations. If the NSA information was legally obtained and mandated by statute, then presumably, the NSA may share this intelligence with DEA.[249] However, if this information came from a program deemed illegal by the FISC or unsanctioned by Congress, then the tip should not be passed on to the DEA.

The larger question is whether we find unfettered intelligence sharing acceptable in the first place. National security is the government's number one priority. In cases where the IC collects positive intelligence of a criminal nature, doesn't it make sense to share? Sharing of resources and intelligence among local, state and federal law enforcement agencies has always been deemed to be efficient and cost effective, and necessary. The same applies for intelligence agencies and their assistance to the domestic law enforcement community. Many criminal organizations commit crimes that are investigated by multiple agencies—would it make sense to have an artificial wall between different agencies that would prevent them from sharing amongst themselves the information they individually develop while investigating the same target? As the rationale for the PATRIOT ACT pointed out, counterterrorism investigations and criminal law enforcement investigations are not mutually exclusive.

Some claim that intelligence sharing provides law enforcement with an "end-run" around Fourth Amendment protections. The courts are sensitive to these considerations, but Congress has authorized IC collection programs. In addition, the use of foreign wiretap information has been accepted as evidence in U.S. criminal proceedings despite the fact that foreign countries may or may not have the same probable cause/Fourth Amendment standards the United States requires, and yet this evidence is admissible and non-controversial.

The net effect of this controversy may well be that the IC will be reluctant to pass any information to law enforcement, or perhaps domestic law enforcement will be reticent to use this information to initiate criminal investigations due to an overabundance of concern that the classified tip will be repeatedly challenged during trial proceedings.

---

249. "Because warrantless eavesdropping on Americans is illegal, tips from intelligence agencies are generally not forwarded to the SOD until a caller's citizenship can be verified." Shiffman & Cooke, *supra* note 2.

With the shroud of secrecy covering NSA surveillance activity comes understandable confusion and subsequent over dramatization of reality. In the previously mentioned "The Good Wife" episodes, the line between fact and fiction about what the NSA can and cannot do is blurred. Let us examine and separate what is real and legal from what is fiction and illegal, which should put into perspective NSA's operational parameters.

The NSA obtains a FISA warrant against Arab-American translator Danny Marwat based upon a photo that shows military contractor Marwat in Afghanistan speaking to a known Taliban member.[250] Marwat claims he gave him food and medication because the Taliban member's daughter was suffering from dysentery.[251] The show claims this photo was not only sufficient probable cause to prove Marwat was a foreign agent for FISA purposes but also sufficient for the U.S. government to subsequently kidnap and torture him to elicit a confession that he was collaborating with the Taliban.[252] Based upon FISA's rigorous probable cause requirements and its known "cumbersome" process leading up to FISC review and approval, it is highly unlikely the NSA would obtain a FISA warrant on Marwat. Moreover, even under section 207 of the PATRIOT Act, a FISA wiretap can only last for 120 days (not two years as mentioned in "The Good Wife") and a one-year extension may be available if the government can demonstrate sufficient probable cause to stay up.[253] It is also highly unlikely the NSA would be listening to calls between Marwat and Florrick if they were not discussing matters related to foreign intelligence and national security as FISA requires that monitors follow minimization procedures, which would restrict monitoring calls that were not relevant to obtaining foreign intelligence.

The episode also mentioned that the FISA warrant on Marwat was a "two hop" warrant which not only allowed monitoring of Marwat, his lawyers, and his lawyers' contacts but later obtained a "three hop" warrant once Florrick's son received multiple "vague" calls from his ex-girlfriend because the phone number was associated with a Somali national and potential Hamas sympathizer.[254] Again, a personal call of this nature would be minimized and insufficient to establish probable cause for a FISA warrant, and more importantly, there is no such thing as a two hop or three hop FISA warrant. Two or three hop refers to the NSA's ability to access telephony metadata not content once a target phone number or email has been identified. No such thing exists under FISA. The show never suggests the NSA obtained a separate FISA warrant on Florrick or her co-workers or family members, and therefore, these NSA interceptions are illegal. (Nor does section 702 apply since only a foreign person outside the United States can be targeted, and Marwat is a U.S. citizen.)

250. *The Good Wife: The Bit Bucket*, *supra* note 4.
251. *The Good Wife: Executive Order 13224*, *supra* note 4.
252. *Id.*
253. PATRIOT Act, *supra* note 42, sec. 207.
254. *The Good Wife: The Bit Bucket*, *supra* note 4.

Putting aside the illegality of the surveillance, the TV show leaves us with the perception that NSA monitors have the ability to simply pick up the phone and meet with law enforcement agents on a regular basis in order to pass on anything that might be useful to police.[255] While the NSA may disclose evidence of a crime to the DEA, in this episode, the DEA agent informed no one of his original source and in fact, had a witness cover it up. This is not an example of "parallel construction." The agent did not receive a tip and develop his own probable cause to arrest Bishop – the agent solely relied upon the NSA intercept to develop probable cause to arrest.[256] Under CIPA, a government attorney would have had to make the judge aware of the classified material prior to the hearing and if it was necessary to use the information as evidence, request a substitution under section 6. The defense would have been aware of the substitution that more likely than not would have been in the form of a statement or agent testimony (e.g., perhaps indicate that a confidential informant reported the impending narcotics transaction rather than reveal the actual intercept). In reality, a series of checks and balances have been put into place by requiring this type of information to go through an agent, government attorney, and judge before determining the discoverability of the particular classified material in each criminal case.

For clarification, the NSA intercept would not be used as evidence at trial because the police should have developed their own probable cause during their investigation and the NSA intercept would have been discussed under CIPA section 4 as an ex parte discovery matter between the judge and prosecutor. If the NSA intercept contained information that was exculpatory, a substitution would be created to protect the FISA warrant, and the defense would be given the evidence in discovery, and a protective order for the classified material would be issued. A witness would not perjure himself in open court, and the DEA would not have kept all parties in the dark as to the original source of the information.

FISA has been around since 1978; CIPA since 1980. They are effective tools that provide a certain level of fairness to the defendant and government by balancing the government's need to protect its sources and methods and the defendant's need for discovery and right to a fair trial.

This fictional television show addresses unreal but imagined NSA abuses that are farcical in the real world, albeit plausible in the realm of American imagination. Unfortunately, our imagination does run wild when information about secret government programs is leaked and media and entertainment sources mislead the general public. In reality, as opposed to "The Good Wife," the three Colombian drug trafficking scenarios discussed in this article seem much more likely: a foreign narcotics trafficker with narco-terrorism ties is targeted by the NSA and makes contact with a domestic distributor/supplier, and the NSA chooses to pass that information along to domestic law enforcement.

255. *The Good Wife: Parallel Construction, Bitches*, *supra* note 8.
256. *Id.*

Our greatest concern lies in the fact that we distrust the government. In light of the Snowden disclosures, Americans have found these NSA programs to be distasteful and a violation of our privacy. However, as discussed, domestic-to-domestic communications are not being monitored unless approved through the FISA process and foreign-to-domestic communications must be minimized to prevent inadvertent interception of U.S. persons unless one of the listed exceptions applies in the case of section 702.

Defense attorneys and the public, in general, have grave doubts that the government will fulfill its discovery and CIPA obligations and turn over classified material that is exculpatory or "helpful to one's defense." At least with a confidential informant, the defendant has a greater chance of learning about the presence of an informant than if it were IC information—there are usually audio and/or video recordings of their encounters or agent reports or affidavits refer to a confidential informant. With an NSA intercept, the defendant (and possibly the local prosecutor) will have no idea how the case was initiated, and therefore, must trust that the government will disclose that information to the judge under CIPA § 4. Thus, an ongoing discussion as to whether sufficient oversight and adversarial testing exists to protect a defendant's constitutional rights is critical. Permitting a defense attorney with an adequate security clearance to attend and participate in the CIPA section 4 discovery hearing during which it is determined whether the classified material is, in fact, "discoverable" might solve many of the issues raised by the defense bar.

In determining whether the overall practice of intelligence sharing should be acceptable, the question is, what do we expect as citizens and taxpayers from our law enforcement agencies? Should law enforcement merely respond to crimes after they are committed, or should law enforcement be proactive and implement programs to prevent crime before it occurs? The answer is fairly obvious. If we want law enforcement to protect and defend us from harm, be proactive and take the fight to the criminal element within our society, then we need to provide them with the necessary tools to do just that.

The practice of sharing IC intelligence with law enforcement is not illegal. The procedure by which intelligence is transmitted to the field and protected from the defendant under CIPA § 4 is not flawed and seems to work as designed. What these recent disclosures by Snowden and the media have brought to the forefront is our natural suspicions that the government is abusing its power and hiding information from us, and our natural curiosity feeds our paranoia. We want to know what we do not know. And we do not trust our government to disclose classified information when it is the right thing to do, and there is a moral and legal imperative to do so.