Echelon's Effect: The Obsolescence of the U.S. Foreign Intelligence Legal Regime

Matt Bedan*

* J.D. Candidate, Indiana University School of Law—Bloomington. Thanks to Pete, Professor Cate, Shaun, Tatum, Amanda, the Lord God and Holy Spirit, Marcus Fenix, Jill, Charlie, Nate, Jake, Evan, Leslie, Joe, Joe, Phil, and Dan. I would also like to say hello to my Mom and Dad.

I. INTRODUCTION

In December of 2005, the *New York Times* first reported that President George W. Bush had secretly authorized the National Security Agency ("NSA") to conduct warrantless domestic surveillance in an effort to combat terrorism.[1] Almost immediately, the story ignited controversy and national debate over the program and whether it violated any of a number of statutes, orders, and federal court decisions which make up the U.S. foreign intelligence legal regime. This Note discusses this regime and the capabilities of the agencies which operate under its purview.

Part II gives an outline of the regime and the context in which it developed. Particular emphasis is given to the Foreign Intelligence Surveillance Act ("FISA") and the enigmatic court which interprets it. Part III describes the Echelon Interception System and the manner in which the United States gathers and shares foreign signals intelligence. Part III then goes on to discuss the implications of intelligence sharing and concludes that some aspects of the current practice are incompatible with the principles, if not the jurisprudence, of the Fourth Amendment.

This Note does not seek to argue that the type and degree of foreign intelligence surveillance currently being undertaken by the federal government is illegal, oppressive, or unwise. Rather, it seeks to point out how technological advancements have rendered America's foreign intelligence legal regime irrelevant by causing a massive disconnect between its goals and its real world impact.

II. CONSTRUCTION OF U.S. FOREIGN INTELLIGENCE SURVEILLANCE LAW

A. Pre-FISA

Presidents going back as far as Abraham Lincoln have claimed that the Constitution confers upon their office the "inherent authority" to conduct warrantless surveillance for the purposes of national security and foreign affairs.[2] Beginning most notably with the Roosevelt administration, "presidents have claimed the right to conduct warrantless electronic surveillance in matters involving the defense of the nation, with each successive administration continuing to broaden this amorphous 'national security exception' to the warrant requirement of the Fourth Amendment."[3]

---

1. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at 1.

2. *See* Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1270 (2004).

3. John J. Dvorske, *Validity, Construction, and Application of Foreign Intelligence*

In an effort to clarify Executive authority, Congress enacted the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III").[4] Title III was the first piece of legislation to require the President to obtain a court order before conducting electronic surveillance.[5] The statute sought to distinguish criminal from foreign surveillance, and in fact began with an explicit disclaimer stating:

> Nothing contained in this chapter . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack . . . of a foreign power, [or] to obtain foreign intelligence information deemed essential to the security of the United States . . . .[6]

Title III thus validated presidential authority to conduct warrantless surveillance for the purposes of national security, but it did not consider any applicable limits to such authority.

The unchecked and expansive power over surveillance granted to the President under Title III led inevitably to its exploitation. Media investigations of the 1960s and 1970s alarmed Americans by uncovering numerous incidents of abuse by a government that seemed to have become fundamentally unconcerned with many of the civil liberties guaranteed by the Constitution.[7] The CIA and FBI's illegal "Cointelpro" and "Chaos" Operations, which tried to publicly discredit Dr. Martin Luther King, Jr. and other civil rights leaders; the clandestine surveillance and harassment of Vietnam War protestors; and the "black bag" burglary of Democratic Party campaign strategies by White House "plumbers" are but a few of the episodes which served to undermine public trust in the government and elucidate the need for reform.[8]

Concurrently, the Supreme Court limited the President's national security exception for the first time when it handed down its decision in *United States v. United States District Court* ("*Keith*").[9] In *Keith*, the Court was required to determine whether the President had the power "to

---

Surveillance Act of 1978 (50 U.S.C.A. §§ 1801 et seq.) Authorizing Electronic Surveillance of Foreign Powers and Their Agents, 190 A.L.R. FED. 385, 395 (Supp. 2005).

4. *See* Ellen S. Podger & John Wesley Hall, *Government Surveillance of Attorney-Client Communications: Invoked in the Name of Fighting Terrorism*, 17 GEO. J. LEGAL ETHICS 145, 150 (2003). *See also* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, codified at 18 U.S.C. §§ 2510 et seq. (2000).

5. 18 U.S.C. § 2518.

6. Pub. L. No. 90-351, 82 Stat. 214 (1968).

7. *See* Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1317–19 (2004).

8. *See id*.

9. 407 U.S. 297 (1972). The case is named after Damon Keith, the District Court judge who initially ordered the government to disclose information it obtained via electronic surveillance.

authorize electronic surveillance in internal security matters without prior judicial approval."[10] Despite a longstanding history of such surveillance, the Court determined that the President did not have this authority.[11] In the majority opinion, Justice Powell reasoned that "[t]he Fourth Amendment contemplates a prior judicial judgment,"[12] and although the task of ensuring national security presented special circumstances, "[t]he circumstances described do not justify complete exemption of domestic security surveillance from prior judicial scrutiny."[13] The *Keith* decision, combined with the widespread domestic unrest generated by Watergate and related government scandals, prompted Congress to form the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities. The subcommittee was chaired by Idaho Senator Frank Church and is commonly referred to as the "Church Committee."[14] The Church Committee was tasked with investigating the alleged intelligence abuses by the FBI and other agencies and furnishing its report and recommendations to Congress.[15] In its report to Congress, the Church Committee concluded that:

> [I]ntelligence activity in the past decades has, all too often, exceeded the restraints on the exercise of governmental power which are imposed by our country's Constitution, laws, and traditions. . . .[16] Too many people have been spied upon by too many Government agencies and [too] much information has [been] collected. The Government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on behalf of a hostile foreign power.[17]

According to the Committee, a necessary step towards curtailment of unconstitutional surveillance practices was to require that the government agencies which conduct surveillance do so in either the foreign or domestic realm.[18] The Committee's recommendations reflected the Supreme Court's language in *Keith*, in which the Court predicted that divergent statutory requirements for foreign and domestic surveillance may be necessary under

10. *Id*. at 299.
11. *Id*. at 320.
12. *Id*. at 317.
13. *Id*. at 320.
14. Solove, *supra* note 2, at 1276.
15. *See* The Assassination Archives and Research Center, http://www.aarclibrary.org/publib/church/reports/contents.htm (last visited Feb. 15, 2007).
16. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES OF THE U.S. SENATE, BOOK II: INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94-755, at 2 (1976), *available at* http://www.aarclibrary.org/publib/church/reports/book2/html/ChurchB2_0001a.htm.
17. *Id.* at 5.
18. *Id*. at 293–94.

the Fourth Amendment.[19] It was Congress' acceptance of this conclusion that prompted them to enact the Foreign Intelligence Surveillance Act in 1978.[20]

B. FISA

The legislative purpose in enacting FISA was to create, in the eyes of the law, distinct and mutually exclusive foreign and domestic spheres of surveillance and to provide a statutory framework for government conduct in the foreign sphere.[21] FISA, as amended by the USA PATRIOT Act,[22] remains in place today and provides authorization for the government to conduct surveillance of a "foreign power" and an "agent of a foreign power" for the purpose of gathering "foreign intelligence information."[23] Originally limited to electronic eavesdropping and wiretapping, its scope was later expanded in 1994 to permit covert physical intrusions with what have been dubbed "sneak and peek" warrants.[24] The combined scope of FISA and Title III theoretically addresses every instance in which the government may lawfully conduct electronic surveillance of any kind.[25]

In order to obtain a FISA warrant, the Attorney General must submit an application to the Foreign Intelligence Surveillance Court ("FISC"), an Article III special court created under the FISA statute.[26] The request must detail: (1) the identity of the target; (2) a certification that the target is a "foreign power" or an "agent of a foreign power"; (3) the type of surveillance to be used; and (4) certification that the information sought is

---

19. For instance, the Court commented, "There is no reason to believe that federal judges will be insensitive to or uncomprehending of the issues involved in domestic security cases. Certainly courts can recognize that domestic security surveillance involves different considerations from the surveillance of 'ordinary crime.'" *Keith*, 407 U.S. at 320.

20. 50 U.S.C. §§ 1801–11 (2000).

21. *See* Nathan C. Henderson, *The Patriot Act's Impact on the Government's Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications*, 52 DUKE L.J. 179, 190 (2002).

22. USA PATRIOT Act is an acronym for the Act's full title: The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections throughout 18 U.S.C.).

23. *See* 50 U.S.C. §§ 1805(a)(1), 1805(a)(3)(A).

24. *See*, *e.g.*, 50 U.S.C. § 1822.

25. Some commentators, including those in the Bush Administration, continue to argue that presidential authority to conduct surveillance for the purpose of national security is derived directly from the Constitution and is not limited by either Title III or FISA. Congress appears to have rejected this contention, asserting that FISA and the criminal warrant procedures constitute the "exclusive means" by which government may conduct surveillance. *See* 18 U.S.C. § 2511(2)(f) (Supp. III 2000).

26. 50 U.S.C. § 1803 (2000).

for the purposes of foreign intelligence.[27] In 2001, the USA PATRIOT Act amended FISA's foreign intelligence purpose requirement, lowering the standard from "primary purpose" to "significant purpose."[28]

In addition to court-ordered surveillance, FISA permits the President to authorize electronic surveillance without a court order for a period of up to one year, provided the Department of Justice ("DOJ") certifies that the surveillance is: (1) only for foreign intelligence information; (2) targets only foreign powers or their agents; and (3) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party.[29] In each of those cases, the Attorney General is required to certify compliance with those conditions to the FISC.[30] In addition, the Attorney General is required to provide a semiannual report on the use of surveillance under overall compliance to the House Permanent Select Committee on Intelligence as well as the Senate Select Committee on Intelligence detailing the extent of surveillance being conducted without a court order.[31]

Under the statute, a U.S. person can be classified as an "agent of a foreign power" upon a finding that he or she acts for a foreign power, is or may be involved in espionage for a foreign power, or is involved in international terrorism.[32] An important caveat to this definition is that no U.S. person can be classified as an agent of a foreign power based solely on his participation in activities protected by the First Amendment.[33]

In 1981, President Reagan issued Executive Order 12,333 as part of an effort to reorganize the U.S. intelligence regime and clarify its mission in response to emerging threats of terrorism.[34] The Order established the first procedures for conducting electronic surveillance outside of the U.S. and mandated that all intelligence collection must be done in a manner "consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded."[35] Specifically, this meant that federal agencies were not permitted to conduct foreign

27. *Id.* § 1804(a)(1)–(11).

28. Jennifer L. Sullivan, Note, *From "The Purpose" to "A Significant Purpose": Assessing the Constitutionality of the Foreign Intelligence Surveillance Act Under the Fourth Amendment*, 19 NOTRE DAME J.L ETHICS & PUB. POL'Y 379, 381 (2005). *See* USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 203(d)(1), 115 Stat. 272, 280 (2001) (codified as amended at 50 U.S.C. § 1804(a)(7)(B) (Supp. III 2000)).

29. 50 U.S.C. § 1802(a)(1) (2000).

30. *Id*. § 1802(a)(2).

31. *Id*. § 1808(a).

32. *See id*. § 1805(a)(3)(A).

33. *Id*.

34. *See* Exec. Order No. 12,333, 3 C.F.R. 200 (1981), *reprinted in* 50 U.S.C. § 401 (2000).

35. *Id.* at pt. 2.1.

intelligence operations for the purpose of collecting information about the domestic activities of U.S. persons.[36] In addition, the government would be required to use the least intrusive collection techniques available when conducting surveillance on U.S. persons abroad.[37]

Executive Order 12,333 was also the first directive to establish the National Security Agency ("NSA") as the primary agency responsible for collecting and disseminating signals intelligence information in support of U.S. military operations and foreign policy.[38] The Order permits the NSA to disseminate signals intelligence only to authorized government recipients, and it strictly forbids the sharing of foreign intelligence with private U.S. corporations.[39] Finally, President Reagan's Order prohibits the NSA from tasking foreign agencies or private entities to engage in activities forbidden by the Executive Order on its behalf.[40]

FISA and Executive Order 12,333 combine to create an extremely complex legal framework. The rules within this framework can vary widely depending on the identity of the target and the location of the surveillance. However (and at the risk of oversimplifying), the interaction of FISA and Executive Order 12,333 can be summarized as follows: (1) if the surveillance is occurring inside the U.S., FISA controls; (2) if the surveillance is occurring outside the U.S. and the target is a U.S. person, Executive Order 12,333 controls; and (3) if the surveillance is occurring outside of the U.S. and the target is not a U.S. person, there are no restrictions, and the agency is free to conduct surveillance as it wishes.[41]

C. FISC

Not surprisingly, the definitions provided in the FISA statute are a source of concern for civil libertarians. Section 1801(a) defines a "foreign power" first as "a foreign government or a component thereof, whether or not recognized by the United States;" and second as "a faction of a foreign nation or nations, not substantially composed of United States persons."[42] Here, there is a notable ambiguity as to exactly what "substantially" means and how many non-U.S. persons would need to be part of a particular group before the government is permitted to spy on it. Also included in the definition of foreign powers is any "entity that is directed and controlled by

36. *Id.* at pt. 2.3(b).
37. *Id.* at pt. 2.4.
38. *Id.* at pt. 1.12(b).
39. *Id.* at pt. 2.3.
40. *Id.* at pt. 2.4.
41. Technically, Executive Order 12,333 still controls, but it only requires that surveillance be conducted in accordance with the procedures established by the head of the agency.
42. 50 U.S.C. § 1801(a)(1)–(2) (2000).

a foreign government or governments."[43] This definition suffers from a similar ambiguity, leaving unclear how much control a foreign government must have over an "entity"—a foreign based corporation for example—before the NSA is permitted to gather intelligence on the group and its members or employees.

The FISC is the primary court charged with resolving such ambiguities in FISA. However, confusion over the meaning of much of FISA's language still remains after nearly thirty years, due largely to the fact that very little is known about how the FISC interprets the statute. In fact, very little is known about the court at all. However, the modest amount of information that is known about the FISC and its procedures has privacy advocates particularly concerned.

Although its membership is made public, the FISC's proceedings and judgments are highly classified.[44] It is known that the FISC meets in a "secret windowless courtroom, sealed from the public by cipher-locked doors on the top floor of the Department of Justice."[45] Proceedings are nonadversarial and entirely ex parte.[46] DOJ attorneys have exclusive access to the FISC judges to present evidence and argue for FISA warrants.[47] When reviewing a FISA application, the presiding judge is explicitly forbidden from second-guessing or otherwise scrutinizing any factual allegation made by the government.[48] If the warrant request is denied, the government can appeal to a three judge panel termed the Foreign Intelligence Surveillance Court of Review.[49] In reality, however, the government's option to appeal is essentially superfluous; in the time since its inception, the FISC has approved 20,605 surveillance applications and denied seven.[50] Conversely, no target of a FISA warrant, U.S. citizen or

---

43. *Id.* at § 1801(a)(6).

44. Patrick S. Poole, *Inside America's Secret Court: The Foreign Intelligence Surveillance Court*, Jan. 22, 2005, http://www.apfn.net/Messageboard/01-24-05/discussion.cgi.54.html. *See also* Jeremy D. Mayer, *9-11 and the Secret FISA Court: From Watchdog To Lapdog?*, 34 CASE W. RES. J. INT'L L. 249, 251 (2002).

45. *See* Poole, *supra* note 44.

46. Lawrence D. Sloan, *Echelon and the Legal Restraints on Signals Intelligence: A Need for Reevaluation*, 50 DUKE L.J. 1467, 1496 (2001).

47. *See* Poole, *supra* note 44.

48. *See* United States v. Duggan, 743 F.2d 59, 77 (2d Cir. 1984). The court explained:

> The FISA Judge, in reviewing the application, is not to second-guess the executive branch official's certification . . . . Further, Congress intended that, when a person affected by a FISA surveillance challenges the FISA Court's order, a reviewing court is to have no greater authority to second-guess the executive branch's certifications than has the FISA Judge.

Id.

49. *See* Poole, *supra* note 44; Sloan, *supra* note 46, at 1496.

50. Under FISA, the Attorney General is required to submit an annual report to Congress listing the number of FISA warrants requested, along with the number granted and

otherwise, is allowed to appeal any order of the FISC.[51]

D. Ambiguities and Loopholes

In order to outline what seems to be a major flaw in the way FISA was drafted, it is worthwhile to begin by making what may be a self-evident observation: FISA only applies to acts of government surveillance. That is to say, a prerequisite to trigger FISA's applicability to any particular instance of government observation is that the observation must fit FISA's definition of surveillance. If it does not, FISA is not implicated and the government is free to listen as it wishes.[52] With the NSA's increased use of data-mining technology, pattern-based inquiries, and National Security Letters, FISA's definition of surveillance may be antiquated to the point that it could render the entire statute irrelevant.

The definition of surveillance, in pertinent form, is the acquisition of a communication either sent or received by a "particular, known United States person who is in the United States," if the communication was acquired by "intentionally targeting" that person, and if the circumstances are such that they have a reasonable expectation of privacy.[53] Alternatively, "surveillance" also means the acquisition of any communication to or from someone located in the United States, if the acquisition occurs within the United States.[54]

It is clear from both FISA and Supreme Court precedent that an individual must have a reasonable expectation of privacy for "surveillance" to occur. In *United States v. Miller*, the Supreme Court held that individuals have no expectation of privacy in information held by a third party.[55] Through the use of National Security Letters, the FBI and the NSA routinely exploit this rule of law to acquire vast amounts of personal information on U.S. citizens from private corporations, such as phone companies and Internet service providers.[56] Because FISA's definition of surveillance fails to account for this practice, the government is not required to get a warrant or make any certification of probable cause. Considering how much the technological capacity of the private sector for gathering and retaining personal information has increased in recent years, the privacy implications of government access to this data are huge.

---

the number denied. These reports are available at http://www.fas.org/irp/agency/doj/fisa/.

51. 50 U.S.C. § 1803(b) (2000) (granting the Court of Review "jurisdiction to review the denial of [an application]; omits "granting of").

52. This is true provided that it complies with Title III and the Fourth Amendment.

53. 50 U.S.C. § 1801(f) (2000).

54. 50 U.S.C. § 1801(f)(2) (Supp. III 2000).

55. *See* 425 U.S. 435, 440, 442 (1976).

56. *See* Fred Cate, *Government Data Mining and Access to Personal Information*, *available at* 829 PLI/PAT 467, 480 (2005).

Recent "E-911" legislation, which requires all new cell phones in the U.S. to be fitted with devices that continuously transmit the phone's location, is an apt example.[57] In the wake of this law, those who regularly carry a cell phone now leave a digital trace everywhere they travel within a matter of feet. If cellular carriers were to share their customer's data with the NSA, CIA, or FBI, as has been widely alleged, those agencies could easily tell not only to whom those customers talk, but with whom they spend their time (assuming they have a cell phone as well), where they spend their time, how long they are there, etc. All of this can potentially be accomplished without doing any actual "surveillance."

Apart from the issue of private corporations gathering and sharing intelligence, FISA's surveillance definition is antiquated due to the distinction it makes between data acquired inside or outside of the U.S. Again, government observation only qualifies as surveillance if the data is acquired inside the U.S. or if one or more of the parties is a known U.S. person, inside the U.S., who the government is targeting intentionally. In other words, unrestrained and indiscriminate eavesdropping by the NSA is allowed under FISA as long as the communication is not physically intercepted within the U.S., and the target is either: (1) someone known to be a non-U.S. person, (2) someone who is intentionally targeted but whose identity is unknown, or (3) anyone else in the world who is not intentionally being targeted.

Today, the requirement that the interception of electronic communications takes place outside U.S. borders is hardly an obstacle to intelligence agencies. The proliferation of the Internet and other global communication networks has made physical distance and political borders a nonfactor in the realm of communications. To increase efficiency, Internet traffic is often routed through the least congested server regardless of the server's physical location.[58] For instance, two neighbors in Nebraska chatting on an instant messenger program might have their communications routed through servers in Hong Kong and back, despite being only 30 feet apart.

The third caveat discussed above, the predicate requirement that an individual be intentionally targeted in order to satisfy the definition of surveillance, is likely to be the NSA's most useful loophole in the FISA statute. As computing power has increased over the past 25 years, the U.S. intelligence community has become capable of capturing and analyzing huge amounts of data, beginning with no particular target of surveillance. These "pattern based" searches rely on sophisticated models of criminal

57. 47 C.F.R. § 20.18(g)(1)(iv) (2005) (establishing the E-911 program).

58. *See* Overview of Cyberspace, http://faculty.frostburg.edu/cosc/htracy/cosc100/c&n;ooc/ooc100.htm (last visited Feb. 15, 2007); Sloan, *supra* note 46, at 1477–78.

behavior with which to compare the captured data.[59]

III. THE ECHELON INTERCEPTION SYSTEM

A. Overview and Capabilities

Project Echelon is the offspring of a classified pact known as "UKUSA" between the United States, Great Britain, Canada, Australia, and New Zealand.[60] The pact was originally a post-World War II intelligence sharing effort to counter Soviet aggression in Europe. While the United States and Great Britain have refused to acknowledge its existence, the pact was referred to in a U.K. parliamentary monitoring body report and has been recognized by the Prime Minister of New Zealand and the former Director of the Australian Defense Signals Directorate ("DSD"), who admitted that the DSD "does cooperate with counterpart signals intelligence organisations overseas under the UKUSA relationship."[61]

Since its inception, the treaty's signatories have worked together to intercept, analyze, and share signals intelligence gathered from all of the world's communication channels.[62] After the fall of the Soviet Union, UKUSA member agencies quickly discovered that the cooperative nature of their intelligence sharing pact was the most effective means of combating modern global threats to national security.[63] Since September 11, 2001, international terrorism has unquestionably become the primary focus of UKUSA's operations, and signals intelligence is considered to be an invaluable tool in that effort.[64] Former Deputy Director of the CIA and Director of the NSA, General Marshall S. Carter, commented that signals

---

59. *See* Cate, *supra* note 56, at 484.

60. UKUSA is an acronym for United Kingdom-United States Security Agreement. Kevin J. Lawner, *Post-Sept. 11th International Surveillance Activity – A Failure of Intelligence: The* Echelon *Interception System & the Fundamental Right to Privacy in Europe*, 14 PACE INT'L L. REV. 435, 444 (2002).

61. Letter from Martin Brady, Director, Defence Signals Directorate, to Ross Coulthart, Reporter, Nine Network Australia Pty Ltd. 2 (Mar. 16, 1999), *available at* http://sunday.ninemsn.com.au/sunday/images/cover/DSD_page2.gif. *See also* GERHARD SCHMID, REPORT ON THE EXISTENCE OF A GLOBAL SYSTEM FOR THE INTERCEPTION OF PRIVATE AND COMMERCIAL COMMUNICATIONS (ECHELON INTERCEPTION SYSTEM), EUR. PARL. DOC. (A5-0264/2001) 62/194 (2001), *available at* http://www.fas.org/irp/program/process/rapport_echelon_en.pdf (citing to Martin Brady's letter as one evidentiary item that confirms the existence of the ECHELON interception system) [hereinafter PARLIAMENT REPORT ON ECHELON].

62. *See* Lawner, *supra* note 60, at 444 (citing Duncan Campbell, *Paper 1: Echelon and its Role in COMINT*, TELEPOLIS, May 27, 2001, paras. 15–17, *available at* http://www.heise.de/tp/deutsch/special/ech/7747/1.html).

63. *See id.* at 445–46 (citing Duncan Campbell, *Paper 2: COMINT Impact on International Trade*, TELEPOLIS, May 27, 2001, para. 3, *available at* http://www.heise.de/tp/deutsch/special/ech/7752/1.html).

64. *See id.* at 446.

intelligence has supplanted human intelligence in its value to policy makers:

> [Human Intelligence] is subject to all of the mental aberrations of the source as well as the interpreter of the source . . . [Signals Intelligence] has technical aberrations which give it away almost immediately if it . . . is not legitimate. A good analyst can tell very, very quickly whether this is an attempt at disinformation, at confusion. . . . You can't do that from [Human Intelligence]. . .[65]

UKUSA member nations currently gather and share intelligence under the treaty through a surveillance network known as Project Echelon. Put simply, Echelon is understood to be the most powerful communications surveillance project in history. It is in essence a global eavesdropping system that targets key communications satellites and grounded networks that convey phone calls, Internet, email, faxes, and telexes.[66] The system is capable of intercepting all radio and microwave communications as well.[67] It is believed that the NSA operates Project Echelon either in conjunction with, or on behalf of, the remaining UKUSA signatories.[68] As is the case with the UKUSA agreement itself, the United States has never publicly acknowledged the existence of Echelon, despite overwhelming evidence that it exists.[69]

What has been published on the project derives from congressional and media investigations, Freedom of Information Act requests, the testimony of former NSA employees, and a report published in July 2001 by the European Parliament.[70] A 1996 book by New Zealand investigative journalist Nicky Hager was the first to uncover New Zealand's involvement in the UKUSA pact and provided the first comprehensive details of Echelon.[71] Although there is evidence to suggest "Echelon" was at one time a code word used to describe a network of computers that processed communications after they were intercepted, today "Echelon" is used generically and describes the entire network of computers, satellites, cables, and other hardware that the UKUSA member nations use to

---

65. Sloan, *supra* note 46, at 1474 (citation omitted).

66. *See id.* at 1472 ("This worldwide network of COMINT programs is believed to intercept all forms of global communication . . . ."); Erin L. Brown, *ECHELON: The National Security Agency's Compliance With Applicable Legal Guidelines in Light of the Need for Tighter National Security*, 11 COMMLAW CONSPECTUS 185, 187 (2003).

67. *See* Brown, *supra* note 66, at 187.

68. *See* Lawner, *supra* note 60, at 452 (citation omitted).

69. *See id*. at 452–53.

70. *See* PARLIAMENT REPORT ON ECHELON, *supra* note 61.

71. *See* Duncan Campbell, *Making History: The Original Source for the 1988 First Echelon Report Steps Forward*, CRYPTOME, Feb. 25, 2000, http://cryptome.org/echelon-mndc.htm.

intercept and share signals intelligence.[72]

Because it is highly classified, the exact scope of Echelon's capabilities is unknown. However, based on what is known about the computing power of a similar system used by the FBI,[73] and in consideration of the budget allotted to the NSA,[74] the conclusion that Echelon is an enormously powerful system seems to be inevitably correct. After leading a congressional inquiry into the use of Echelon, Senator Church (whose influence on the legal landscape is discussed *supra*, Part II.A), warned:

> [Its] capability at any time could be turned around on the American people and no American would have any privacy left, such [is] the capability to monitor everything. . . it doesn't matter. There would be no place to hide. [T]he technological capacity that the intelligence community has given the government could enable it to impose total tyranny. . . . Such is the capability of this technology.[75]

Senator Church issued that statement in 1975, and it can only be assumed that the technology he spoke of has evolved considerably in the past thirty years.

Today, the common belief among researchers is that Echelon intercepts and analyzes nearly three billion communications per day.[76] Some, however, believe that Echelon's capabilities go even further.

---

72. *See* Sloan, *supra* note 46, at 1470–71 (citing Elizabeth Becker, *Long History of Intercepting Key Words*, N.Y. TIMES, Feb. 24, 2000, at A6 ("It [the Echelon system] links computers in at least seven sites around the world to receive, analyze, and sort information captured from satellite communications, newly declassified information shows.")).

73. The FBI uses a similar signals interception system codenamed "Carnivore." For an overview of the system and its capabilities, see IIT RESEARCH INSTITUTE, INDEPENDENT TECHNICAL REVIEW OF THE CARNIVORE SYSTEM (2000), *available at* http://www.usdoj.gov/archive/jmd/carnivore_draft_1.pdf.

74. While the actual budget and size of the NSA are classified, the agency admits that if it were considered a private corporation, it would rank in the top ten percent of Fortune 500 Companies in terms of dollars spent, floor space occupied, and personnel employed. *See* Frequently Asked Questions - About National Security Agency, http://www.nsa.gov/about/about00018.cfm#7 (last visited Feb. 15, 2007). Moreover, the NSA is the world's largest employer of Ph.D mathematicians, as well as the world's largest owner of supercomputers. The average electrical bill for NSA Headquarters in Maryland is estimated at twenty-one million dollars. *See* Susan Page, *NSA secret database report triggers fierce debate in Washington*, USA TODAY, May 11, 2006, *available at* http://www.usatoday.com/news/washington/2006-05-11-nsa-reax_x.htm.

75. Sloan, *supra* note 46, at 1467 (citation omitted).

76. *See* NSA Watch: Answers to Frequently Asked Questions About Echelon, http://www.nsawatch.org/echelonfaq.html (last visited Feb. 15, 2007) [hereinafter Echelon FAQ]; Brown, *supra* note 66, at 187; Echelon Watch, http://www.echelonwatch.org/ (last visited Feb. 15, 2007) ("ECHELON attempts to capture staggering volumes of satellite, microwave, cellular and fiber-optic traffic, including communications to and from North America."). *See also* Echelon at AllExperts, http://experts.about.com/e/e/ec/echelon.htm (last visited Feb. 15, 2007).

Former Georgia Congressman Bob Barr investigated the NSA while he was a senior member of the House Judiciary Committee and Vice-Chairman of the House Government Reform Committee.[77] Barr is an outspoken critic of the NSA and has commented that he believes that by now, Echelon has attained the capability to intercept numerous electronic communications in many countries around the world, no matter the point of origin or destination.[78]

The Echelon system connects supercomputers stationed at approximately twenty bases throughout the world, all of which channel intelligence through the project's headquarters at Fort Meade, Maryland.[79] The stations are said to operate "'giant golf balls,'" called "radomes," which communicate with orbiting satellites to coordinate the interception of communications all over the globe.[80] The largest station in the network is located in Menwith Hill, England, which is rumored to regularly intercept enormous amounts of email, telephone, and fax communications going into and out of Europe.[81] As recently as 2002, communications giant British Telecom publicly announced that it had wired three major domestic fiber-optic trunk lines (each capable of simultaneously carrying over 100,000 calls) directly through Menwith Hill, "allow[ing] the N.S.A. . . . [free access] to the heart of the British Telecomm network."[82]

All signals intelligence intercepted by Echelon is automatically routed through a series of computers before it is disseminated to UKUSA's intelligence agencies. Each member nation provides its own "dictionary," which is essentially a list of terms to form the basis of Echelon's search.[83] The "terms" are not limited to spoken or written words, but can consist of any number of permutations of words, phrases, pictures, voices, addresses, phone numbers, etc.[84] Each country maintains an independent dictionary, and intelligence "hits" are sent directly to the respective agency without

77. *See generally* Bob Barr, http://www.bobbarr.org/ (last visited Feb. 15, 2007) (describing the politician's political and nonpolitical achievements and undertakings).

78. *See* Bob Barr, *A Tyrant's Toolbox: Technology and Privacy in America*, 26 J. LEGIS. 71, 78 (2000) (stating that the scope of Echelon's interception abilities is unknown, but that reports by the European Parliament suggest the system is capable of intercepting numerous communications in Europe and other countries).

79. *See* Lawner, *supra* note 60, at 453 (citation omitted). *See also* PARLIAMENT REPORT ON ECHELON, *supra* note 61.

80. *See* Lawner, *supra* note 60, at 453 (citation omitted). *See also* PARLIAMENT REPORT ON ECHELON, *supra* note 61.

81. *See* Lawner, *supra* note 60, at 453 (citation omitted).

82. *See id*.

83. *See* Sloan, *supra* note 46, at 1480–81 (citation omitted); Douglas C. McNabb & Mathew R. McNabb, *Of Bugs, The President, And The NSA: National Security Agency Intercepts Within The United States*, THE CHAMPION, Mar. 2006, at 15.

84. *See* Echelon FAQ, *supra* note 76.

being seen by any of the other agencies.[85] The membership will then share intelligence at its discretion and in accordance with its own laws.

B. Interaction with Foreign Intelligence Legal Regime

1. Shared and Incidentally Obtained Information

Executive Order 12,333 authorizes the NSA to collect and disseminate any "[i]ncidentally obtained information that may indicate involvement in activities that may violate federal, state, local, or foreign laws . . . ."[86] This license is another example of the fundamental conflict that has resulted from Congress' attempts to control the NSA's new generation of unfocused and automated data mining programs using a statute that was designed to regulate traditional, target-specific surveillance.

Although the concept of using incidentally acquired information is not intuitively problematic, the sheer enormity of Echelon's surveillance capacity means the exception could potentially swallow the entire rule. A system that is essentially capable of intercepting every communication in the world could conceivably allow the government to thereby "incidentally acquire" all of those communications. If and when the government attains such a capability, FISA and the Fourth Amendment will be circumvented, and Americans will no longer have any statutory or constitutional protection of their privacy in the sphere of foreign intelligence surveillance.

Another issue arises from the fact that Executive Order 12,333 allows U.S. government agencies to accept intelligence about U.S. citizens acquired by foreign governments, regardless of how the information was obtained. Given the secrecy and collaboration that takes place in the UKUSA security agreement, the concern is that the NSA is side-stepping FISA by simply allowing a foreign government to spy on U.S. citizens and then freely sharing in the resulting intelligence. Although Executive Order 12,333 forbids the NSA from actively soliciting a foreign agency to conduct surveillance that the NSA could not conduct on its own,[87] there is evidence that the rule enjoys very little fidelity. Even assuming that the NSA strictly adheres to Executive Order 12,333 and accepts and shares intelligence only in good faith, the synergistic nature of the UKUSA pact may make the practice of intelligence sharing within the pact unconstitutional. A more detailed analysis of this idea is provided in the next section.

---

85. *See id.*
86. Exec. Order No. 12,333, *supra* note 34, at pt. 2.3(i).
87. *Id.* at pt. 2.12.

A noteworthy example of the potential for abuse in UKUSA came from former Canadian Intelligence Agent Mike Frost, who admitted to the BBC that he utilized Echelon to spy on two British Cabinet members at the behest of former Prime Minister Margaret Thatcher.[88] He claimed she ordered the surveillance because she suspected the cabinet members "weren't onside."[89] Frost clarified that the use of the term "onside" meant that the targets disagreed with her on policy matters but were not under suspicion of espionage.[90] In a reference to the UKUSA pact, Frost commented, "The British Parliament [had] total deniability. . . They didn't do anything . . . we did it for them."[91] Frost claimed that all five member nations used Echelon and the UKUSA pact to skirt domestic privacy laws.[92]

In a later interview with CBS News, Frost commented, "I was trained by you guys [the NSA]". And although admitting that widespread surveillance was necessary, Frost added, "My concern is no accountability and nothing, no safety net in place for the innocent people who fall through the cracks."[93] For example, Frost recalled an incident where a Canadian housewife was put on a terrorist watch list after she mentioned in a phone call that her son had "'bombed' in the play last night."[94]

Several ex-NSA employees claim that Echelon is often used to spy on civilian organizations such as Amnesty International and Greenpeace.[95] According to the Senate Select Committee on Intelligence, the NSA was involved in "clandestine service applications" including surveillance and "surreptitious entry" into the homes of journalists who attempted to investigate Echelon.[96] Also, an ex-analyst at Echelon's Menwith Hill station admits to eavesdropping on the phone calls of ex-Senator Strom Thurmond.[97]

Perhaps even more disturbing than allegations of the U.S. government spying on its own citizens is the fact that Echelon's dissemination

88. *Thatcher 'spied on ministers'*, BBCNEWS, Feb. 25, 2000, http://news.bbc.co.uk/1/hi/uk_politics/ 655996.stm.

89. *Id.*

90. *Id.*

91. *Ex-Snoop Confirms Echelon Network* , CBS NEWS, Mar. 1, 2000, *available at* http://www.cbsnews.com/stories/2000/02/24/60minutes/main164651.shtml.

92. *Id.*

93. *Id.*

94. *Id.*

95. Lawner, *supra* note 60, at 455; PARLIAMENT REPORT ON ECHELON, *supra* note 61, at 71.

96. Plaintiff's Complaint at 44, ACLU v. NSA and CSS, (E.D. Mich. 2006), *available at* http://www.aclu.org/safefree/nsaspying/23491lgl20060117.html.

97. PARLIAMENTARY REPORT ON ECHELON, *supra* note 61, at 71.

procedure creates the bizarre possibility that foreign intelligence agencies are using NSA technology and resources to spy on American citizens, and the NSA (at least in theory) has no immediate access to the information or control over its distribution to foreign intelligence agencies.

2. Information Sharing and the Fourth Amendment

U.S. Constitutional law has always recognized a distinction between intelligence gathering and intelligence sharing. The central difference between the two is that intelligence gathering (the central thesis of this Note notwithstanding) is typically limited by statutory and constitutional requirements, where intelligence sharing typically is not. If a foreign intelligence agency wishes to provide the U.S. government with information, the government is generally free to accept it. The only limitation is that the foreign agency must have been acting on its own accord and not at the behest of the U.S. government. The following is a brief overview of the exclusionary rule and an argument of why it should apply to information freely handed to the U.S. government by foreign intelligence agencies.

It is a well established canon of constitutional law that when a state acts as the agent of the federal government, or as part of a joint venture with the federal government, the actions of the state will be attributed to the federal government for constitutional analysis.[98] This doctrine does not apply to foreign governments. Under current law, information furnished to American officials by foreign intelligence agencies is not subject to the exclusionary rule, even in those cases where the surveillance was done in violation of the U.S. Constitution.[99]

The Supreme Court's decision in *Lustig v. United States*, in which Justice Frankfurter first articulated what would become known as the "silver platter" doctrine, set forth the initial precedent in this area.[100] Under the doctrine, the question of whether the government has participated in intelligence gathering or intelligence sharing is fact specific and turns not on the constitutionality of the search itself, but rather to the extent of the government's involvement. According to Frankfurter, "[t]he crux of that doctrine is that a search is a search by a federal official if he had a hand in it; it is not a search by a federal official if evidence secured by state

98. *See* Gambino v. United States, 275 U.S. 310, 316–17 (1927) (holding that in making a search and seizure, state officers were acting solely on behalf of the United States, and evidence thus obtained is inadmissible in a prosecution in a federal court if the circumstances of the search and seizure were such as to render it lawful).

99. *See* United States v. Hensel, 699 F.2d 18, 25 (1st Cir. 1983) (holding exclusionary rule does not require suppression of evidence seized by foreign police agents).

100. *See* Lustig v. United States, 338 U.S. 74 (1949).

authorities is turned over to the federal authorities on a silver platter."[101]

Justice Frankfurter's plurality opinion in *Lustig* was heavily criticized and would eventually be explicitly rejected by the Supreme Court in its decision in *Elkins v. United States*.[102] The *Elkins* Court held for the first time that evidence obtained in violation of the Fourth Amendment was inadmissible in federal courts regardless of whether the offending officer was a state or federal employee. Later, the Court's ruling in *Mapp v. Ohio* destroyed the remainder of the silver platter doctrine by establishing the rule that constitutionally tainted evidence will consistently be excluded in both state and federal courts.[103]

Although *Mapp* did not involve electronic surveillance and did not contemplate actions of foreign governments, its commentary on the scope of the Fourth Amendment is pertinent. The clear holding of *Mapp* is that evidence illegally obtained by the U.S. government should not be admissible in any American court. The reason for the exclusion of such evidence is to deter government officials from conduct which violates the Constitution.

With that in mind, the logical retort to the suggestion that the exclusionary rule should apply to evidence obtained by foreign governments is that a foreign government is not under the purview of the U.S. Constitution, so it cannot be deterred. Many courts agree with this logic. In *Brulay v. United States*, the Ninth Circuit ruled that neither the Fourth nor the Fourteenth Amendment would apply to exclude evidence seized by Mexican officials who were not "acting at instigation of United States customs or narcotic officials," because "[n]either the Fourth nor the Fourteenth Amendments are directed at Mexican officials and no prophylactic purpose is served by applying an exclusionary rule here since what we do will not alter the search policies of the sovereign Nation of Mexico."[104]

Although the Ninth Circuit's ruling in and of itself is not necessarily at odds with the thesis of this Note, its essential reasoning assuredly is. Because Brulay was arrested in Mexico, he was not under the umbrella of the Constitution at the time his privacy was invaded, and any expectation of privacy he had would rightfully have been diminished. This is not the case when foreign intelligence agencies acquire signals intelligence from U.S. citizens inside the U.S. and subsequently share it with the FBI or NSA. In

101. *Id.* at 78–79.

102. 364 U.S. 206 (1960).

103. *See* Mapp v. Ohio, 367 U.S. 643, 643 (1961) (holding all evidence obtained by searches and seizures in violation of the Federal Constitution is inadmissible in a criminal trial in a state court).

104. Brulay v. United States, 383 F.2d 345, 348 (9th Cir. 1967).

consideration of this, analysis of the *Brulay* decision is provided not for its significance in the field of privacy law, but rather as an anecdote highlighting a fundamental misconception about the exclusionary rule, particularly as it applies to the Fourth Amendment.

The interpretation of the exclusionary rule followed by the Ninth Circuit in *Brulay* is misguided in both its substantive understanding of the law and its assumptions about the exclusionary rule's real-world deterrent effect. To begin, the *Brulay* Court incorrectly concludes that the primary goal of the exclusionary rule is deterrence of U.S. official misconduct. While the function of the exclusionary rule may be to deter police from violating the Fourth Amendment, logically that function is only useful to the extent that it protects a liberty that society values. Put differently, the exclusionary rule exists because Americans value privacy, not because Americans value the Fourth Amendment. According to Justice Silas Clark, "were it otherwise. . . the [Fourth Amendment] would be a 'form of words,' valueless and undeserving of mention in a perpetual charter of inestimable human liberties. . . neatly severed from its conceptual nexus with [] freedom . . ."[105]

In addition, the *Brulay* Court's characterization of the practical effect of the exclusionary rule is flawed. The Court assumes that the investigation techniques used by foreign officials are guided solely by the sovereign authority of their respective nations. In other words, our law does not govern them, so they have no incentive to follow it. This assumption ignores considerations of efficiency and the end-goals of surveillance.

Admittedly, foreign officials do not operate under the threat of consequences for violating U.S. laws as U.S. officials do. Nevertheless, the threat of repercussions is not the sole, or even primary, reason U.S. law enforcement agents respect the Constitution. The exclusionary rule deters U.S. officials not because it is "the law" in the abstract, but rather because officials know that if they violate the Fourth Amendment, their work will be wasted and the suspect will go free. In that sense, there is no reason to think the exclusionary rule would not have the same deterrent effect on a foreign official as it does on an agent of the U.S.

A foreign agency conducting electronic surveillance on an American citizen, for the purposes of sharing intelligence with the U.S. government, would have precisely the same motivation to ensure that the evidence it gathers is admissible in a U.S. court. Even if the foreign government has no actual interest in the investigation, the logic would translate assuming that intelligence sharing is a reciprocal act among nations that is intended to aid in prosecution.

---

105. *Mapp*, 367 U.S. at 655.

IV. CONCLUSION

The Echelon Interception System has been described as an effort to do away with formal borders in the intelligence community.[106] If FISA and the Fourth Amendment are to provide meaningful protection to Americans in this new community, their application (to the extent possible) must also become global. To that end, the government's practice of accepting and utilizing intelligence provided by foreign agencies against Americans must be subject to the common law exclusionary rule. When the government accepts the surveillance product of foreign intelligence agencies, regardless of whether the Fourth Amendment is implicated, it is tacitly (if not overtly) encouraging a foreign government to violate the privacy rights of Americans. In the context of Echelon and the UKUSA intelligence sharing pact, the failure to apply the exclusionary rule to shared evidence is tantamount to recognizing a conceptual right to privacy, but in reality withholding the freedom and enjoyment it provides.

In the statutory realm, the fact that the FISC is essentially immune from meaningful scrutiny makes the current version of FISA uniquely threatening to the privacy rights of Americans. If the interests of national security require that the judgment of FISA warrant applications be done outside of the public eye, then the process should at least be adversarial. Congress may wish to consider appointing a special advocate, with the highest security clearance, whose job it would be to represent the privacy interests of potential FISA surveillance targets. Having a third voice in the room, even if it does not affect a single decision of the court, would help alleviate the public anxiety that naturally arises with the existence of secret courts, sealed decisions, and unexpressed law.

Unfortunately, the United States' current use of Echelon and the UKUSA pact to circumvent its own laws is both distressing and anti-democratic. While the marginalization of privacy rights in a post-September 11th America may have been inevitable, the same should not be said about the rule of law. The agencies charged with ensuring the security of America must be allowed to zealously fight terrorism with all of the tools and techniques at their disposal. However, if privacy is a luxury Americans can no longer afford, its death knell should be legislated and documented in a manner consistent with open government. And if the U.S. is to remain committed to open government, our laws must reflect the line that our elected leaders draw between the interests of liberty and security, regardless of where they choose to draw it.

---

106. McNabb & McNabb, *supra* note 83, at 15.