ECHELON: THE NATIONAL SECURITY AGENCY'S COMPLIANCE WITH APPLICABLE LEGAL GUIDELINES IN LIGHT OF THE NEED FOR TIGHTER NATIONAL SECURITY

Erin L. Brown

I. INTRODUCTION

Article II of the Constitution broadly states that the President has the fundamental duty to preserve, protect and defend the Constitution of the United States. In United States v. United States District Court, Justice Powell elaborated on Article II by stating, "Implicit in that duty is the power to protect our Government against those who would subvert or overthrow it by unlawful means." The United States is the most powerful country in the world, and it arguably has the most enemies. The National Security Agency ("NSA"), in upholding the provisions of Article II, operates intelligence gathering systems that protect our nation from its enemies. In carrying out this duty, the NSA must constantly monitor communications to and from the United States, while remaining cognizant of the constitutional protections granted to its citizens.

One of the most controversial tools at the NSA's disposal is ECHELON. ECHELON is a telecommunications spy network operated by the NSA in conjunction with four other countries. It intercepts telephone, fax and e-mail transmissions traveling to and from, and sometimes within, the United States. The key issue concerning ECHELON is whether this global communications interceptor infringes upon the Fourth Amendment's guarantees of protection from unreasonable search and seizure.

This issue now must be analyzed in light of the World Trade Center and Pentagon tragedies of September 11, 2001. These tragic events have led Americans to reevaluate the debate between privacy and national security in a new context. Gone are the days when "Big Brother" was the only concern that Americans had in regard to the government's use of electronic surveillance. Americans are now faced with questions that will substantially affect the manner in which they view their fundamental constitutional rights. Americans must ask if they will tolerate government surveillance through the use of technologies, such as ECHELON, used in the hopes of detecting, preventing and apprehending terrorist threats to the United States. Americans must also ask if they are willing to surrender some personal privacy in order to strengthen both national security and their knowledge that chances of another September 11th occurring during their lifetimes will be substantially reduced.

Citizens and inhabitants of the United States

1. U.S. CONST. art. II, § 1, cl. 8.
3. Id. at 310 (holding that the President may find it necessary to use electronic surveillance to obtain intelligence on those foreign agents who conspire to harm the United States government).
6. Id. (explaining the motivation and plan behind hackers' "Jam Echelon Day").
7. Jeffrey Richelson, Desperately Seeking Signals, BULLETIN

OF THE ATOMIC SCIENTISTS, available at http://bullatomsci.org/issues/2000/ma00/ma00richelson.html (Mar./Apr. 2000) [hereinafter Richelson] (raising the issue of "Big Brother" and government surveillance and the feeling of a lack of privacy that these surveillance techniques have instilled in the American people. This article also provides the historical and technical background of ECHELON and claims that the NSA has not been adequately able to keep up with evolving technological breakthroughs in its operation of intelligence gathering for national security purposes).
may not realize that systems such as ECHELON do not require them to make this sacrifice, because the NSA must strictly adhere to legal standards when conducting electronic surveillance activities. However, in the wake of the September 11, 2001 tragedies, it may be beneficial for the NSA to know that it has the support of those it seeks to protect and that the controversy surrounding ECHELON may subside for years to come. The more Americans realize that national security allows them to realize their rights and privileges, the more likely it is that they will tolerate the slim prospect that their privacy may be infringed upon in the operation of ECHELON.

This Comment seeks to lay forth the legal framework in which the NSA operates and to establish that the NSA is not permitted to conduct domestic surveillance on the general populace. Part I of this Comment provides the purposes and powers of the NSA. Part II goes into detail as to how the technological aspects of ECHELON operate. Part III explains the legal guidelines of the Foreign Intelligence Surveillance Act ("FISA"), Executive Order 12,333 and the Fourth Amendment of the Constitution, with which the NSA must comply in its operation of technological surveillance. Part IV discusses the main concerns surrounding the operation of ECHELON. This Comment focuses on allegations of domestic surveillance and invasion of privacy, but will not address the highly debated issue of economic espionage. Lastly, this Comment will analyze the technological aspects of ECHELON in the context of the established statutory and administrative guidelines governing its operation, and, in doing so, will seek to provide assurance that the NSA complies with applicable legal requirements in its maintenance and operation of ECHELON.

II. THE NATIONAL SECURITY AGENCY

The NSA was established by President Harry S. Truman’s directive in 1952 to provide both signals intelligence and communications security activities to the government. The present-day NSA has a twofold mission: to protect United States information systems and to produce foreign signals intelligence information. To achieve these objectives, the NSA works in conjunction with the Central Security Service and various other government organizations to gather intelligence information. The NSA claims that it strictly follows the laws and regulations designed to protect United States’ citizens’ Fourth Amendment rights and that it therefore performs signals intelligence operations only against foreign powers or agents of foreign powers, not against citizens or inhabitants of the United States.

There are judicial, statutory and administrative safeguards that regulate the NSA’s collection of signals intelligence. These safeguards are designed to balance the government’s need for foreign intelligence information with the privacy rights afforded to United States citizens under the Fourth Amendment. The NSA also has an internal process overseen by the Office of the Inspector General to ensure that the “CSS was established in 1972 to provide cryptologic activities within the military.” This article does not focus on the NSA’s information assurance mission.

9 See Michael Mosier, Note, Causes of Action for Foreign Victims of Economic Espionage Abroad by U.S. Intelligence, 11 Duke J. Comp. & Int’l L. 427, 427-29 (2001) (claiming that ECHELON is used for economic espionage purposes for which foreign individuals have no recourse).
10 NATIONAL SECURITY AGENCY, NSA AND THE INTELLIGENCE COMMUNITY 1, at http://www.nsa.gov/about_nsa/nasa_role.html (last visited Nov. 19, 2000) [hereinafter NSA AND THE INTELLIGENCE COMMUNITY] (providing information as to how the NSA was established and where it fits into the intelligence community).
11 NATIONAL SECURITY AGENCY, MISSION STATEMENT 1, at http://www.nsa.gov/about_nsa/faq_internet.html (last visited Nov. 19, 2000) [hereinafter MISSION STATEMENT] (stating that the Information Assurance mission provides "the solutions, products and services, and conducts defensive information operations, to achieve information assurance for information infrastructures critical to U.S. national security interests," whereas the signals intelligence mission "allows for an effective, unified organization and control of all the foreign signals collection and processing activities of the United States").
12 NSA AND THE INTELLIGENCE COMMUNITY, supra note 10, (stating that the “CSS was established in 1972 to provide cryptologic activities within the military.” This article does not focus on the NSA’s information assurance mission).
14 Id. (providing information on the guidelines and focus of the collection of signals intelligence).
15 Id. (stating that the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence ensure that the NSA adheres to applicable laws and regulations); but see generally Lawrence D. Sloan, Note, ECHELON and the Legal Restraints on Signals Intelligence: A Need for Reevaluation, 50 Duke L.J. 1467, 1505-05 (2001) (alleging that ECHELON’s ability to collect nearly all signals makes its
tor General ("OIG"), whose responsibility is to ensure that the NSA complies with Executive Order 12,333 and related implementing directives and regulations in its execution of intelligence-gathering operations.18 Executive Order 12,333 provides the NSA and the other members of the intelligence community with responsibilities and appropriate procedures to which to adhere in collecting intelligence and counterintelligence information.17

Now that the foundation for the powers and responsibilities of the NSA in its collection of intelligence and counterintelligence information has been laid, we will explore the technology behind ECHELON and its operation.

III. BACKGROUND OF ECHELON

A. General Framework

ECHELON is an automated global satellite-based interception and relay system operated by the intelligence agencies of five nations: the United States, Britain, New Zealand, Australia and Canada ("UKUSA countries").18 This telecommunications spy network intercepts all means of communications as part of the global signals intelligence ("SIGINT")24 operations of a direct violation of the statutory framework of the Foreign Intelligence Surveillance Act and the Fourth Amendment because it does not comply with the warrant and probable cause elements of the Fourth Amendment and that ECHELON is a device used to conduct domestic surveillance).16 NSA FREQUENTLY ASKED QUESTIONS, supra note 13.


17 See generally Legal Standards for the Intelligence Community in Conducting Electronic Surveillance, at http://www.fas.org/irp/nsa/standards.html [hereinafter Legal Standards] (establishing the legal basis and constitutionality of ECHELON's existence), but see generally Legal Standards for the Intelligence Community in Conducting Electronic Surveillance, at http://www.fas.org/irp/nsa/standards.html [hereinafter Legal Standards] (explaining the technical aspects of ECHELON, how it is operated, what kind of information it intercepts and what is done with the intercepted information. The article elaborates on the technical aspect of ECHELON by claiming that there is no governmental oversight in its operation); but see generally Legal Standards for the Intelligence Community in Conducting Electronic Surveillance, at http://www.fas.org/irp/nsa/standards.html [hereinafter Legal Standards] (explaining the technical aspects of ECHELON, how it is operated, what kind of information it intercepts and what is done with the intercepted information. The article elaborates on the technical aspect of ECHELON by claiming that there is no governmental oversight in its operation).

18 AMERICAN CIVIL LIBERTIES UNION, FREEDOM NETWORK, ANSWERS TO FREQUENTLY ASKED QUESTIONS (FAQ) ABOUT ECHELON, at http://www.aclu.org/echelonwatch/faq.html (last modified Oct. 15, 2001) [hereinafter FREQUENTLY ASKED QUESTIONS] (exposing the technology of ECHELON to the general public for the first time, Campbell explains ECHELON's capabilities and describes the technological forefathers of electronic surveillance). Campbell also determined the separate jurisdictions of which each government agency is in charge. GCHQ is the coordinating center for Europe, Africa and Russia. The NSA covers parts of Eastern Europe and most of North and South America. Australia coordinates the electronic monitoring of the South Pacific and South East Asia. Id.

19 Patrick S. Poole, ECHELON: America's Secret Global Surveillance Network at http://fly.hiwaay.net/~pスポール/echephon.html (last visited Nov. 19, 2001) [hereinafter ECHELON: America's Secret Global Surveillance Network] (discussing the UKUSA agreement between the United States, Australia, Canada, New Zealand and Britain. Poole states that Australia, Canada, New Zealand and Britain are considered the "Second Parties" to the agreement. There are also "Third Party Members" including Germany, Japan, Norway, South Korea and Turkey).

20 Id.

21 Duncan Campbell, Somebody's Listening, at http://www.gn.apc.org/duncan/echelon-dc.htm (last visited Nov. 19, 2001) [hereinafter Somebody's Listening] (exposing the technology of ECHELON to the general public for the first time, Campbell explains ECHELON's capabilities and describes the technological forefathers of electronic surveillance). Campbell also determined the separate jurisdictions of which each government agency is in charge. GCHQ is the coordinating center for Europe, Africa and Russia. The NSA covers parts of Eastern Europe and most of North and South America. Australia coordinates the electronic monitoring of the South Pacific and South East Asia. Id.

22 AMERICAN CIVIL LIBERTIES UNION, FREEDOM NETWORK, ACLU URGES CONGRESS TO INVESTIGATE ECHELON SURVEILLANCE SYSTEM, at http://www.aclu.org/congress/l040699a.html (last visited Nov. 19, 2001) [hereinafter ACLU LETTER] (claiming that the interception of these forms of communication is a direct violation of the rights of United States persons because the National Security Agency is allegedly conducting domestic surveillance).

23 AMERICAN CIVIL LIBERTIES UNION, FREEDOM NETWORK, ACLU URGES CONGRESS TO INVESTIGATE ECHELON SURVEILLANCE SYSTEM, at http://www.aclu.org/congress/l040699a.html (last visited Nov. 19, 2001) [hereinafter ACLU LETTER] (claiming that the interception of these forms of communication is a direct violation of the rights of United States persons because the National Security Agency is allegedly conducting domestic surveillance).

24 Duncan Campbell, Interception Capabilities 2000 6, at http://www.iptreports.mcnmail.com/ic2report.htm (last visited Nov. 19, 2001) [hereinafter Interception Capabilities] (explaining that communications intelligence deals with technical and intelligence information derived from foreign communications by those other than the intended recipient and is included in the broader category of signals intelligence which also includes the collection of non-communications signals such as radar emissions). This article was part of the Scientific and Technical Options Assessment report released by the British Parliament for the purpose of alerting the
partments of the five participating governments. The UKUSA agreement originally was enacted to protect against U.S.S.R.'s arms build-up during the Cold War. However, the countries decided to expand their signals and communications intelligence efforts by developing technologically advanced capabilities to ward off not only Russian enemies, but any threat to the safety of the UKUSA nations.

This is where ECHELON came in. ECHELON allegedly came into existence in the 1970's, but has only recently been acknowledged by any of the UKUSA nations. To this day, the United States denies the existence of ECHELON despite overwhelming evidence to the contrary.

ECHELON has a very complex, technological and precise method of gathering data. The interception process captures all data from e-mail transmissions, telephone calls and fax transmissions. Therefore, the communications that are captured consist of vocal conversations, as well as transmissions containing written data. These interceptions are designed to capture non-military communications of governments, private organizations, businesses and private individuals on behalf of these nations. The interception process is divided into three stages: the collection of intelligence, its analysis and contextualization and its redistribution.

B. Interception

One way in which ECHELON collects communication transmissions is via large satellite dishes located at various points around the world. These dishes are aimed at satellites orbiting the Earth that transmit telephone and fax communications between civilians. This information is in turn funneled through the ground dishes from these satellites.

The second source of ECHELON-gathered communications is the United States satellite network and its reception bases that are scattered throughout the United States, Canada, New Zealand, Britain and Australia. This network deals with signals intelligence rather than the aforementioned, and not as high-tech, interception of satellite communications. The United States'
satellite network is far more sweeping than the network of previously mentioned satellites because it gathers information from e-mail and cell phone transmissions, in addition to phone and fax transmissions. Internet and e-mail interceptions require the use of a complex technological device that is not required to parlay ordinary phone and fax signal interceptions to the NSA.

Even though the ECHELON listening stations are located on foreign soil, the NSA is primarily responsible for the American-owned downlink stations. The downlink, or reception stations, consist of radomes, which are enormous golf-ball-like structures that contain satellite dishes and other listening equipment. The radomes capture information that is then poured into memory buffers capable of storing five trillion pages of data at NSA’s headquarters.

C. Analysis and Dissemination

After the satellite dishes capture the signals, they are then sent to a large computer network for analysis. This network consists of many state-of-the-art computers that “decrypt, filter, examine and codify” the intercepted messages during the analysis process through the use of programs that have optical character recognition and voice recognition capabilities. The NSA and its UKUSA partners are mainly concerned with any form of communication that could pose a threat to their national security. The determination of whether the intercepted information will be removed from the network prior to analysis or remain in the system for further investigation depends on the contents of dictionaries supplied by the five nations.

The dictionaries can be found in computers supplied by each of the five UKUSA countries that contain a list of keywords whose appearance raises a red flag for its corresponding country. If an intercepted message is red-flagged, it then is automatically transcribed, assigned a four-digit code, recorded by the system and forwarded to the interested country’s computer. The agents at the receiving site then analyze the message further to determine whether it is a threat to national security. Often, the messages that are red-flagged are nothing more than innocent conversations and do not have substantial merit as threats to national security.

---

38 ECHELON: America’s Secret Global Surveillance Network, supra note 19, at 6.
39 FREQUENTLY ASKED QUESTIONS, supra note 18, at 2.
40 ECHELON: America’s Secret Global Surveillance Network, supra note 19.
41 David Ruppe, Big Ears and Big Secrets, ABCNEWS.COM, at http://www.abcnews.go.com/sections/world/DailyNews/ Echelon_990709.html (July 16, 2000) [hereinafter Ruppe] (stating that the radomes located at Menwith Hill in Yorkshire, England download information from various satellites that conduct surveillance of Europe, North Africa and western Asia. Ruppe also commented that the European Parliament’s STOA report put fear in all Europeans that the United States also engages in industrial espionage to defeat European competitors in major trade competitions).
43 ECHELON: America’s Secret Global Surveillance Network, supra note 19 (explaining the various technologies that work in conjunction with ECHELON to provide the NSA with intelligence information). SILKWORTH is the main computer system at the Menwith Hill facility that drives the keyword search programs. PATHFINDER is a tool that " sifts through large databases of text-based documents and messages looking for keywords and phrases based on complex algorithmic criteria.” VOICECAST is able to pinpoint an individual’s voice pattern so that every call that a person makes is transcribed and analyzed. Id.
44 See Richardson, supra note 7.
45 ECHELON: America’s Secret Global Surveillance Network, supra note 19 (stating that very few messages are actually transcribed and recorded by the system); but see Ex-Snoop Confirms Echelon Network, CBSNEWS.COM, at http://cbsnews.com (Feb. 12, 2001) [hereinafter Ex-Snoop Confirms Echelon Network] (concluding that ECHELON intercepts and analyzes all electronic communications, including those from the “good guys” in order to determine who the threats are to the nation’s security).
46 See id.
47 Id.
48 See Erin Zimmerman and Dale Hurd, Surveillance Society: Exposing Echelon, at http://www.christianity.com/CC/article/1.1183,PTID2546%7CCHIP%7CCHIP136183.00.html [hereinafter Zimmerman & Hurd] (stating that ECHELON intercepts over two million communications every hour); see also Ex-Snoop Confirms Echelon Network, supra note 45 (recalling a situation in which a woman’s communication was intercepted and red-flagged because she told a friend on the phone that her son had “bombed” in a school play. The system alerted the analysts to this communication, and therefore it was further analyzed to determine its propensity for alarm).
IV. THE CONTROVERSY SURROUNDING ECHELON

The debate over the legality and constitutionality of ECHELON’s existence and operation came to Congress’ attention in 1988, when a whistleblower stationed at the Menwith Hill Facility in England during the 1980s was interviewed by the Cleveland Plain Dealer. The whistleblower, Margaret Newsham, filed a lawsuit concerning corruption and misspending on United States government black projects, claiming that she overheard real-time intercepts of Senator Strom Thurmond’s telephone conversations. This lawsuit raised fears that the NSA conducted domestic surveillance of Americans, over which it had no jurisdiction.

In addition to Ms. Newsham’s lawsuit, the Scientific and Technical Options Assessment program office ("STOA") of the European Parliament released two reports, “An Appraisal of Technologies of Political Control” and “Interception Capabilities 2000,” that describe the capabilities of American surveillance and ECHELON. Both reports were prepared to provide the European Parliament with a guide to technological advancements, while developing policy recommendations for the operation and control of technologies such as ECHELON. The first report, released in 1998, suggested that ECHELON indiscriminately intercepts large amounts of communications, including economic intelligence, constituting malpractice and negligence. "Interception Capabilities 2000," written by British investigative journalist Duncan Campbell, contained accusations from the French government that the NSA uses ECHELON for industrial and commercial espionage. In response to this report, the French government issued a decree encouraging the public to use more powerful encryption to disable the interception capabilities of ECHELON.

The STOA reports prompted action from the American Civil Liberties Union, who brought it to Congress’ attention that the NSA and its electronic surveillance operations needed to be examined to ensure that Americans’ privacy rights were not being willfully invaded by the NSA. Congressman Bob Barr led the Congressional movement to force the NSA to account for the fact that United States citizens’ communications are intercepted by ECHELON in the name of national security. The NSA eventually submitted the legal standards to which it adheres in the interception of communications, but did so without ever acknowledging the existence of ECHELON.

49 Frequently Asked Questions, supra note 18 (stating that the dictionaries allow the system to work more efficiently because they provide ECHELON with key words, addresses, and the like that are to be flagged for inspection); see also Interception Capabilities, supra note 24, at 18 (explaining that the dictionary computers store a database of specified targets including names, topics, addresses, telephone numbers and the like).

50 See Richelson, supra note 7.

51 ECHELON: America’s Secret Global Surveillance Network, supra note 19.

52 See Somebody’s Listening, supra note 21.

53 See Zimmerman & Hurd, supra note 48 (claiming that the five-country partnership that runs ECHELON creates a legal loophole in which no country has to spy on its own citizens, but is able to receive intercepted information pertaining to their own citizens, from another UKUSA country).

54 Frequently Asked Questions, supra note 18 (stating that due to the STOA reports, the European Parliament formed a temporary committee of Enquiry to investigate ECHELON. In May 2001, committee members were scheduled to meet with NSA and CIA personnel to discuss ECHELON, but the meetings were never realized).

55 ACLU Letter, supra note 22.

56 Frequently Asked Questions, supra note 18 (claiming that domestic surveillance and economic espionage are an unacceptable and illegal use of ECHELON).

57 Id.

58 See Ruppe, supra note 41.

59 See ACLU Letter, supra note 22 (describing ECHELON to the House Committee on Government Reform. The letter also raised allegations of the role of ECHELON in domestic surveillance, and its violation of United States citizens’ civil liberties under the Fourth Amendment).

60 See Zimmerman & Hurd, supra note 48 (pointing out that Congressman Barr asked the NSA to supply the American people with basic information regarding the NSA’s legal basis for intercepting communications. Barr eventually pushed a bill through the House requiring the NSA, CIA and Attorney General to supply the House Select Committee on Intelligence with this information); see also American Civil Liberties Union, Freedom Network, ECHELONWatch: United States Congressional Action, at http://www.aclu.org/echelonwatch/congress.html (describing the process through which H.R. 1555 was passed).

61 See generally Legal Standards, supra note 18.
V. LEGAL GUIDELINES

ECHELON's astounding ability to intercept satellite-based communications leaves an impression on Americans that they are the objects of government surveillance. However, the NSA must adhere to strict rules in the operation of its electronic surveillance equipment. ECHELON is subject to the Fourth Amendment of the United States Constitution, which requires reasonableness and probable cause for searches and seizures. ECHELON is also subject to strict regulation by the Foreign Intelligence Surveillance Act of 1978, as well as Executive Order 12,333, which deal with intelligence gathering and surveillance in terms of national defense. Lastly, the NSA has provided Congress with its own set of legal guidelines that apply to its operation and use of ECHELON. These internal guidelines incorporate the standards of the Fourth Amendment, FISA and Executive Order 12,333.

A. Legal Standards for the Intelligence Community

ECHELON has recently come into the spotlight under a cloud of suspicion and fear, causing authorities to question the legality and constitutionality of its existence. Congressman Bob Barr initiated hearings to determine whether United States’ signals intelligence activities are violating the privacy rights of Americans. In April 2000, the House Intelligence Committee held a hearing to deal with these allegations and suspicions arising from ECHELON’s alleged existence and operation. The Committee hoped that the hearing would rebut the assumption that ECHELON circumvents the federal requirement that it is necessary to obtain a warrant prior to eavesdropping on communications involving United States "persons," a term which refers to both citizens and non-citizen inhabitants.

Congressman Porter Goss of Florida, the Republican Chair of the House Permanent Select Committee on Intelligence, requested that the NSA disclose its legal standards to the committee. The NSA invoked the attorney-client privilege and refused disclosure of the requested information. In response, Congressman Barr proposed a bill that would require the NSA to disclose to Congress the legal standards that apply to the operation of ECHELON.

Subsequently, the House of Representatives amended a bill authorizing funds for intelligence operations. The amendments required the Director of the Central Intelligence Agency, the Director of the NSA and the Attorney General to prepare a report disclosing the legal standards for gathering intelligence via electronic surveillance. The bill passed both houses of Congress, but the Senate version required only a report and did not require full disclosure of all signals intelligence activities.

President Clinton signed the Senate version into law as an intelligence community funding bill—the Intelligence Authorization Act for Fiscal Year 2000. This act required disclosure reports from the NSA, CIA and the Attorney General to include the legal standards for the interception

---

63 U.S. Const. amend. IV.
66 Legal Standards, supra note 18.
68 Richelson, supra note 7.
69 ACLU ALERT, supra note 67.
70 See Richelson, supra note 7.
71 FREQUENTLY ASKED QUESTIONS, supra note 18.
72 See Zimmerman & Hurd, supra note 48 (reciting the question that Bob Barr posed to the NSA:
73 There seems to be very credible evidence that this operation is taking place, and has been taking place for quite some time. At this point, all we’re asking for is the basic information telling us what do you at the NSA, the National Security Agency, believe is the legal basis for you to gather this information? That’s the starting point: What’s the basis that you believe you’re authorized to do this?).
74 American Civil Liberties Union, Freedom Network, United States Congressional Action, at http://www.aclu.org/echelonwatch/congress.html (providing the process of H.R. 1555 being passed by both the House and the Senate, and stating the requirements imposed on the NSA and CIA in response to the Bill).
of communications when such interception may result in the acquisition of information from a communication to or from United States persons; intentional targeting of the communications to or from United States persons; receipt from non-United States sources of information pertaining to communications to or from United States persons; and dissemination of information acquired through the interception of the communications to or from United States persons.\footnote{76} In the NSA’s report to Congress, titled “Legal Standards for the Intelligence Community in Conducting Electronic Surveillance,”\footnote{77} the NSA stated that its internal legal standards are governed by the Fourth Amendment,\footnote{78} FISA,\footnote{79} and by Executive Order 12,333.\footnote{80} Further, the NSA stated that it abides by the FISA requirements of prior judicial notice and probable cause in conducting electronic surveillance that either targets United States persons or may result in the acquisition of information involving them.\footnote{81} The NSA also reported that incidentally-acquired information about a United States person who is not an approved target may be retained and disseminated if the communication is in regard to foreign intelligence or counterintelligence.\footnote{82} The standards also posit that the requirements for obtaining and utilizing information regarding a United States person is governed by a much stricter set of rules than in a situation in which the parties are foreign.\footnote{83}

If an electronic interception may result in incidentally acquired information directed to or from a United States person, both FISA and Executive Order 12,333 apply, and the surveillance must be conducted in a reasonable manner to ensure that a minimum amount of information is acquired regarding the United States person. If the incidentally acquired information pertains to foreign intelligence, it may be disseminated.\footnote{84}

Lastly, in order for the NSA to conduct proper dissemination of information acquired about United States persons, it must comply with FISA and the minimization procedures therein. In order to disseminate personally identifiable information concerning a United States person, the information must be deemed necessary to understand foreign intelligence.\footnote{85}

In sum, the aforementioned legal standards for electronic surveillance are governed by both a statutory framework that governs foreign intelligence collection and the procedures and restrictions that apply to the interception of foreign communications, as well as Executive Order 12,333, which sets the guidelines for interception of information dealing with a United States person who is abroad at the time of surveillance. The NSA states that it also abides by the Fourth Amendment’s necessary requirements of reasonableness and probable cause in its surveillance and communication interception activities.\footnote{86} The following is a more detailed discussion of FISA, Executive Order 12,333 and the Fourth Amendment.

B. Foreign Intelligence Surveillance Act of 1978 (“FISA”)*

Congress enacted FISA in 1978 to further United States counterintelligence and to determine who has the authority to engage in activities that involve the interception of intelligence and gathering surveillance operations).

\footnote{87} Id. (stating that it is sufficient in the case of a non-U.S. person to show that the information to be acquired is merely related to the national defense or security of the United States or the conduct of foreign affairs; where a United States person is involved, the contents of the application must include a showing that the acquisition of such information is necessary to national defense or security or the conduct of foreign affairs).

\footnote{88} Id. (providing the legal standards for receipt from non-United States sources of information pertaining to communication to or from United States persons).

\footnote{85} Id.

\footnote{86} Id.

what restrictions should apply to those activities.\textsuperscript{88} This act also was aimed at lessening the competition between the Federal Bureau of Investigation ("FBI") and the Department of Justice on the one side and the CIA and other segments of the intelligence community on the other side.\textsuperscript{89} The intelligence community was viewed as a mysterious group that answered to no one, and this characterization made citizens nervous in regard to their perceived lack of privacy.\textsuperscript{90}

FISA allows the President, acting through the Attorney General, to acquire foreign intelligence information for periods up to one year, if the surveillance is directed at intercepting communications between or among foreign powers.\textsuperscript{91} FISA states that the surveillance must not operate with a substantial likelihood that the intercepted communications would involve any United States person.\textsuperscript{92} United States citizens' privacy rights are protected by this act. The method of electronic surveillance must be conducted in accordance with the certifications and the minimization procedures\textsuperscript{93} adopted by the Attorney General.\textsuperscript{94} These procedures allow the federal government to use intercepted communications involving a United States person only if they have complied with the minimization procedures set out in the act.\textsuperscript{95}

FISA has also established a specialized court, the Foreign Intelligence Surveillance Court ("FISC"), with the purposes of reviewing Department of Justice applications requesting the use of electronic surveillance and issuing secret warrants authorizing these activities.\textsuperscript{96} Applications to this court must adhere to a strict set of guidelines established by FISA before the Department of Justice can expect FISC to grant its application.\textsuperscript{97} The Chief Justice of the United States Supreme Court designates seven district court judges from seven of the judicial circuits whose purpose is to

\textsuperscript{88} Gerald H. Robinson, We're Listening! Electronic Eavesdropping, FISA, and the Secret Court, 36 WILLAMETTE L. REV. 51, 51-52 (2000) [hereinafter We're Listening!] (providing the background and inception of the Foreign Intelligence Surveillance Act and its court).
\textsuperscript{89} Id. at 52.
\textsuperscript{90} Id. (arguing that the FISA and its court are operated in a crippling shadow of secrecy that makes it nearly impossible for checks and balances to be brought against their operation in regard to ECHELON).
\textsuperscript{91} FISA defines "foreign power" as: (1) a foreign government or any component thereof whether or not recognized by the United States; (2) a faction of a foreign nation or nations, not substantially composed of United States persons; (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments; (4) a group engaged in international terrorism or activities in preparation therefore; (5) a foreign-based political organization, not substantially composed of United States persons; or (6) an entity that is directed and controlled by a foreign government or governments.
\textsuperscript{92} FISA defines an United States person as: an alien lawfully admitted for permanent residence, . . . 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, but does not include a corporation or an association which is a foreign power.
\textsuperscript{93} The minimization procedures with respect to electronic surveillance include: (1) specific procedures, which shall be adopted by the Attorney General that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information; (2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1), shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; (3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and (4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to 102(a) [50 U.S.C. § 1802(a)], procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than twenty-four hours unless a court order under section 105 [50 U.S.C. § 1805] is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.
\textsuperscript{94} 50 U.S.C. §1801(h) (1994).
\textsuperscript{96} We're Listening!, supra note 88, at 51 (providing statistics concerning the Foreign Intelligence Surveillance Court ("FISC").
\textsuperscript{97} See 50 U.S.C. §1804 (1994) (establishing the necessary showing of a detailed application to FISC in the gathering of intelligence information. This section makes it clear that the necessary showings are very stringent even when foreign powers are the proposed targets).
sit on the FISC bench and hear applications for, and grant orders approving, electronic surveillance for counterintelligence purposes. The FISC will grant the application if the government has adhered to the stated guidelines, compliance with which allows the court to make certain findings required pursuant to FISA before an application can be granted. The orders themselves also must adhere to established specifications, often including a description of the target of electronic surveillance, the nature and location of the targeted surveillance, the type of information sought and the allotted time to conduct the surveillance. However, if the target is solely comprised of foreign powers, certain information may be excluded from the order. Orders may also be granted on an emergency basis without all of the aforementioned formalities, while still utilizing the minimization procedures if the information sought indicates a threat of death or serious bodily harm to any person.

If the FISC denies an application, the government can move for review by a panel of three judges who are designated by the Chief Justice. If the court of review affirms the denial of the application, the government may petition for a writ of certiorari to the Supreme Court of the United States.

C. Executive Order 12,333

Executive Order 12,333 was issued in 1981 by President Reagan with the purpose of establishing the policies and procedures to which each participant in the intelligence community must adhere in the collection, retention and dissemination of intelligence information. The Order establishes the framework in which the government

\[\text{footnotes:}\]


99 To issue an order, the FISC must first make the necessary findings of:

1. the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information;
2. the application has been made by a Federal officer and approved by the Attorney General;
3. the basis of the facts submitted by the applicant is probable cause to believe that—
   A. the target of the electronic surveillance is a foreign power or agent of a foreign power or an agent of a foreign power solely upon the basis of activities protected by the First Amendment to the Constitution of the United States; and
   B. each of the facilities or places at which the electronic surveillance is directed is being used, or is abused, or is about to be used, by a foreign power or an agent of a foreign power;
4. the proposed minimization procedures meet the definition of minimization procedures under section 104; and
5. the application which has been filed contains all statements and certifications required by section 104.

50 U.S.C. §1804 and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 104(a)(7)(E) and any other information furnished under section 104(d).


100 50 U.S.C. §1805(c) (1994).


102 FISA authorizes emergency orders when the Attorney General reasonably determines that:

1. an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained; and
2. the factual basis for issuance of an order under this title to approve such surveillance exists; he may authorize the emergency employment of electronic surveillance if a judge having jurisdiction under section 103 is informed by the Attorney General of his designee at the time of such authorization that the decision has been made to employ emergency electronic surveillance and if an application in accordance with this title is made to that judge as soon as practicable, but no more than twenty-four hours after the Attorney General authorizes such surveillance. If the Attorney General authorizes such emergency employment of electronic surveillance, he shall require that the minimization procedures required by this title for the issuance of a judicial order be followed. In the absence of a judicial order, the surveillance shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of twenty-four hours from the time of authorization by the Attorney General, whichever is earliest. In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated and no order is issued approving the surveillance, no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court.


and its agencies are to gather foreign intelligence and counterrintelligence information and the manner in which the information collection will be conducted in the United States and abroad.\textsuperscript{106} The Order sought to strike a balance between the Fourth Amendment rights of United States persons with the need for an effective national security regime able to protect the United States from "international terrorist and international narcotics activities, and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents."\textsuperscript{107}

The Order's goal was to "enhance human and technical collection techniques, especially those undertaken abroad, and the acquisition of significant foreign intelligence, as well as the detection and countering of international terrorist activities and espionage conducted by foreign powers."\textsuperscript{108} The Order also stated that the collection of intelligence is a "priority objective and will be pursued in a vigorous, innovative and responsible manner that is consistent with the Constitution."\textsuperscript{109}

Executive Order 12,333 authorized the NSA to collect, retain and disseminate information pertaining to United States persons if the procedures are authorized by the Attorney General, and the information constitutes foreign intelligence or counterrintelligence not otherwise obtainable.\textsuperscript{110} Under this Order, the NSA may also collect information incidentally acquired that indicates involvement in activities that may violate federal, state, local or foreign laws.\textsuperscript{111}

The NSA must, in accordance with this Order, use the least intrusive means authorized by the Attorney General in the collection, retention and dissemination of intelligence information in the United States or directed at United States persons abroad.\textsuperscript{112} Executive Order 12,333 also states that the NSA may not conduct physical surveillance of a United States person abroad to collect foreign intelligence unless the information is significant and cannot be reasonably acquired by other available means.\textsuperscript{113}

Executive Order 12,333 gives the Attorney General power to approve the use of electronic surveillance within the United States or against a United States person abroad if it is determined that there is probable cause to believe that the "technique is directed against a foreign power or an agent of a foreign power."\textsuperscript{114} In authorizing electronic surveillance, the Attorney General must also comply with FISA. Since FISA pertains to electronic surveillance of United States persons as well as foreign countries, FISA is much more comprehensive than Executive Order 12,333, which only deals with United States persons located abroad and/or United States persons acting as foreign agents.\textsuperscript{115}

\textsuperscript{106} Id. at 62.

\textsuperscript{107} Exec. Order No. 12,333 §1.4 states:

The agencies within the Intelligence Community shall, in accordance with applicable United States law and with the other provisions of this Order, conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States, including:

(a) Collection of information needed by the President, the National Security Council, the Secretaries of State and Defense, and other Executive Branch officials for the performance of their duties and responsibilities;

(b) Production and dissemination of intelligence;

(c) Collection of information concerning, and the conduct of activities to protect against, intelligence activities directed against the United States, international terrorist and international narcotics activities, and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents;

(d) Special activities;

(e) Administrative and support activities within the United States and abroad necessary for the performance of authorized activities; and

(f) Such other intelligence activities as the President may direct from time to time.


\textsuperscript{108} The stated purpose of Executive Order 12,333 is: to enhance human and technical collection techniques, especially those undertaken abroad, and the acquisition of significant foreign intelligence, as well as the detection and countering of international terrorist activities and espionage conducted by foreign powers.

Exec. Order No. 12,333 §2.2 (1982).

\textsuperscript{109} Exec. Order No. 12,333 §2.1 (1982).

\textsuperscript{110} See Exec. Order No. 12,333 §2.3(b) (1982) (stating that foreign intelligence collection may not be undertaken for the purpose of spying on American citizens).

\textsuperscript{111} Exec. Order No. 12,333 §2.3(i) (1982).

\textsuperscript{112} Exec. Order No. 12,333 §2.4 provides:

Agencies are not authorized to use such techniques as electronic surveillance, unconsented physical search, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the agency concerned and approved by the Attorney General. Such procedures shall protect constitutional and other legal rights and limit the use of such information to lawful government purposes.


\textsuperscript{113} Exec. Order No. 12,333 §2.4(d) (1982).

\textsuperscript{114} Exec. Order No. 12,333 §2.5 (1982).

\textsuperscript{115} See Exec. Order No. 12,333 (1982).
D. The Fourth Amendment

The most prominent argument leveled against ECHelon is that the NSA, in its operation of ECHelon, violates American citizens’ civil liberties guaranteed by the Fourth Amendment of the Constitution, which provides:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.116

The government’s participation in electronic surveillance was first considered in light of the Fourth Amendment’s provisions in Olmstead v. United States.117 The issue in Olmstead was whether the use of private telephone conversations intercepted by means of wiretapping was in violation of the Fourth and Fifth Amendments.118 The defendant argued that wiretapping his phone lines to gain evidence of an alleged conspiracy, in violation of the National Prohibition Act, was a trespass upon his property and comparable to breaking and entering his home to steal letters.119 In contrast, the government contended that the case was more analogous to a situation in which a federal officer overheard a conversation on the street.120

Chief Justice Taft delivered the opinion of the Court, which examined past precedent for search and seizure cases. The Court’s opinion relied on Weeks v. United States121 in conjunction with the history of the Fourth Amendment.122 It held that the Founders would not have wanted the language of the Fourth Amendment to be stretched beyond the practical meaning of the words.123 Therefore, the Constitution was not violated unless there had been “an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house ‘or curtilage’ for the purpose of making a seizure.”124 The Olmstead court ultimately found that the government’s use of a wiretap on the defendant’s phone line did not amount to a search or seizure, and therefore did not violate the Fourth Amendment.125

Justice Brandeis entered a powerful dissent. He contended that the issue of privacy is an ever-evolving condition that the Founders took into account while drafting the Fourth Amendment.126 He argued that the Constitution must be able to evolve with changing circumstances and new technology.127 He also noted that more offensive means of invading the privacy of those protected by the Constitution are arising at an alarming rate, and the Constitution should evolve to protect Americans from these invasions.128

An example of such a case is Silverman v. United

116 U.S. Const. amend. IV.
117 277 U.S. 438 (1928).
118 Id. at 455.
119 Id. at 460-65 (comparing Olmstead’s situation to cases that have found that letters are protected from unreasonable search under the Fourth Amendment); see also Ex Parte Jackson, 96 U.S. 727, 733 (1877) (holding that “letters and sealed packages... in the mail are as fully guarded from surveillance as are letters in the hands of the parties forwarding them in their own domiciles”).
120 Olmstead, 277 U.S. at 464-65 (claiming that eavesdropping in public does not violate the Fourth Amendment because there is no invasion of one’s right to be secure in their persons, houses, papers or effects); see also Goldman v. United States, 316 U.S. 129, 133-34 (1942) (holding that the government’s use of a dictaphone (a high-tech microphone) to listen in on one’s conversation from an adjacent apartment did not violate the Fourth Amendment because it did not amount to an interception of the conversation).
121 292 U.S. 383, 398 (1914) (holding that it was unconstitutional for the police to intercept mail without a warrant because it amounted to an unreasonable search and seizure). The Court reasoned that:

if letters and private documents can thus be seized and held and used as evidence against a citizen accused of an offense, the protection of the Fourth Amendment declaring his right to be secure against such searches and seizures is of no value, and... might as well be stricken from the Constitution. Id.

122 Olmstead, 277 U.S. at 463 (stating that the Fourth Amendment's purpose was to do away with the destructive English practice of general warrants and writs of assistance); see also Boyd v. U.S., 116 U.S. at 625-26 (explaining general warrants and writs of assistance). Writs of assistance empowered the officers to search suspected places for smuggled goods at their own discretion. General warrants were issued for searching houses for the search and seizure of books and papers that might be used to convict their owner of the charge of libel. Id.
123 Olmstead, 277 U.S. at 465.
124 Id. at 466.
125 Id.
126 Id. at 472-73 (Brandeis, J., dissenting) (arguing “time works changes, brings into existence new conditions and purposes. Therefore a principle to be vital must be capable of wider application than the mischief which gave it birth.”).
127 See id. at 473 (Brandeis, J., dissenting).
128 See id. at 473-75 (Brandeis, J. dissenting) (citing Entick v. Carrington, 19 Howles State Trials, 1030, 1066).

It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty and private property,
States,129 in which the Supreme Court held that law enforcement officers' warrantless use of a microphone to eavesdrop on the defendant violated the Fourth Amendment because such a device constituted a physical intrusion into the defendant's premises.130 The officers stationed themselves in an adjacent row house and placed the microphone in the heating system of the defendant's home.131 Absent such a physical intrusion, the Supreme Court would have held that the defendant's Fourth Amendment protection against unreasonable search and seizure would not have been violated even without a warrant.132

Six years later in Katz v. United States,133 the Supreme Court conducted a major revision of the law regarding the government's use of electronic surveillance. The petitioner posed his issues to the Court in terms of constitutionally protected areas and privacy rights in general.134 However, in taking an alternate view, the Court rephrased the issue as whether the petitioner's Constitutional rights under the Fourth Amendment were violated when an electronic listening device was attached to a public telephone booth in which the defendant was using the telephone.135

The Court relied on the reasoning that petitioner had a reasonable expectation of privacy, and therefore the use of listening device was deemed an unconstitutional search and seizure.136 The Court held that although the Fourth Amendment protects people and not places, the petitioner sought to keep his conversation private despite the fact that he was in an area accessible to the public, and therefore, his conversation was constitutionally protected.137 Justice Harlan's concurring opinion provided an important test for a reasonable expectation of privacy in regard to Fourth Amendment protections.138 This reasonable expectation of privacy rule has remained in effect to this day.139

Justice Black delivered a powerful argument against the requirement of search warrants for wiretapping and other forms of electronic surveillance. He posited that the Fourth Amendment was framed to deter the practice of actual breaking and entering to gain evidence against a person to be used in a court of law140 and not to apply to intangible things such as spoken words.141 The very characteristics of conversation provide that this intangible concept cannot properly fit under the the Fourth Amendment because it is not a search or a seizure in the traditional sense.142

In the 1972 case of United States v. United States District Court,143 the Supreme Court elaborated on its Olmstead holding.144 The government argued that the Omnibus Crime Control Act imparts on the government the right to conduct warrantless electronic surveillance to thwart threats to the nation's security.145

The Court recognized the necessity to balance the citizens' needs for privacy and free expression with the government's efforts to "protect itself from acts of subversion and overthrow directed against it."146 The Court concluded that the use of wiretaps for domestic aspects of national security where that right has never been forfeited by its conviction of some public offense.

Id. at 353.
Id. at 351.
Id. at 361 (holding that in order for a person to have

Fourth Amendment protection, they must have an actual (subjective) expectation of privacy, and the expectation must be one that society is prepared to deem as reasonable).

See United States v. Charbonneau, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997) (stating that a person challenging the validity of a search and seizure may only assert a "reasonable subjective expectation of privacy." The Court held that the defendant did not have a reasonable and subjective expectation of privacy on the Internet because the openness of the chat room diminished his expectation of privacy incrementally).

Katz, 389 U.S. at 367.
Id. at 365-66.
Id. at 36-56.
407 U.S. at 297 (1972).
Olmstead, 277 U.S. at 466 (holding that the wiretapping did not amount to a search and seizure because there was no actual trespass committed against petitioner).
United States District Court, 407 U.S. at 503.
Id. at 315.

The question that must be asked is whether the needs of citizens for privacy and free expression may not be better protected by requiring a warrant before such a sur-
require prior judicial approval.\textsuperscript{147} The previous discussion’s goal was to aid the reader in understanding the legal regime that the NSA adheres to in its operation of electronic surveillance for intelligence gathering purposes. The following section is a discussion on the operation of ECHELON within the aforementioned legal framework.

VI. ECHELON’S OPERATION WITHIN ITS STATED LEGAL REGIME

Despite the recent terrorist attacks on the United States, Americans are not willing to surrender or loosen their hold on their fundamental right to privacy.\textsuperscript{148} The majority of Americans, if aware of the existence of ECHELON, would believe that the Fourth Amendment protections against unreasonable search and seizure are directly violated by the operation of this surveillance technology. However, this Comment asserts that the oversight in the legal framework for operating ECHELON adequately guarantees the steadfast protections warranted by the Fourth Amendment, while maintaining the national security of the United States.

A. Allegations of Domestic Surveillance

1. Non-United States Persons

The NSA is not permitted to spy on American citizens. The NSA’s main priority is to gather signals intelligence from foreign powers and individuals that pose a threat to the security of the United States.\textsuperscript{149} The NSA adheres to the strict guidelines established by FISA when it conducts surveillance on foreign powers. FISA requires the NSA to gain authorization from the Attorney General and abide by FISA’s minimization procedures if the electronic surveillance is directed at foreign powers, and there is no substantial likelihood that the surveillance will incidentally acquire information pertaining to a United States citizens’ communications.\textsuperscript{150} There is no need to obtain a warrant or court order to conduct this surveillance, because foreign powers are not granted the constitutional protections that are granted to the American people.\textsuperscript{151}

2. United States Persons

FISA requires the NSA to obtain a court order from the Foreign Intelligence Surveillance Court if a United States person is involved in electronic surveillance. If the United States person is located abroad, Executive Order 12,333 is the guiding authority, and the NSA must obtain permission from the Attorney General to conduct electronic surveillance.\textsuperscript{152} The only way a United States person would be the object of the NSA’s electronic surveillance would be if that individual is deemed an agent of a foreign power, in that he acts for, or on behalf of the foreign power by: knowingly engaging in intelligence gathering; knowingly engaging in sabotage or international terrorism; knowingly entering the United States under a false or fraudulent identity; or knowingly aiding or abetting any persons in the above-mentioned activities.\textsuperscript{153}

\textsuperscript{147} Id. at 321.
\textsuperscript{148} See Philip Shenon & Neil A. Lewis, Groups Fault to Listen, Search and Seize, NYTIMES.COM, at http://www.nytimes.com (Sept. 21, 2001) (claiming that the broader wiretapping authority granted by the Combating Terrorism Act 2001 is vehemently opposed by numerous United States organizations); but see Ariana Eunjung Cha & Jonathan Krim, Privacy Trade-Offs Reassessed, The Washington Post, Sep. 18, 2001, at E01 (providing testimony that Americans are much more tolerant of government surveillance in the wake of the terrorist attacks on the United States).
\textsuperscript{149} See Exec. Order No. 12,333 §1.12(b), 46 Fed. Reg. 59941 (Dec. 4, 1981) (establishing that the responsibilities of the NSA are to collect, process and disseminate signals intelligence for national foreign intelligence purposes).
\textsuperscript{151} Id.
\textsuperscript{152} Legal Standards, supra note 18.
\textsuperscript{153} FISA defines agent of a foreign power to include:
(2) any person who—
(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
(D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign
If gathered information concerns a United States person, the acquired information may be used in a criminal proceeding if the Attorney General provides advanced authorization, the aggrieved person is notified, and the FISA minimization procedures are followed. The acquisition of such information must be necessary for, and not merely related to, national defense, national security or the conduct of foreign affairs of the United States.

The operation of ECHELON adheres to the aforementioned legal standards because it does not conduct surveillance on its own citizens. The NSA, in its operation of ECHELON, intercepts communications that are sent abroad. If the communications are to and from United States persons and travel within the United States, the NSA will not target those communications. The NSA's objective is to intercept foreign intelligence, not domestic intelligence. However, it may appear that the NSA spies on its own citizens because the other UKUSA countries may intercept United States persons' communications and analyze them for threatening content. It is alleged that there are situations in which another UKUSA country intercepted American communications, analyzed them, and then determined that they were a threat to the national security of the United States and therefore notified the NSA of the situation. This is legal under the stated guidelines. If the intercepted information was mistakenly tagged as containing questionable information, the analyst would examine the data and then discard it from the system if she determined that the contents do not warrant concern.

ECHELON's operation also adheres to the minimization procedures established by FISA. The NSA intercepts a vast amount of telephone, fax and e-mail communications, but only a small fraction actually get analyzed by NSA employees. The majority of intercepts flow through the system without ever being seen or heard by a live person. If the communication does not get flagged for analysis, it simply gets kicked out of the system, and no one's privacy is violated. Simply stated, if people are not doing anything wrong or illegal, they have nothing to fear.

B. War and National Defense Legislation

Terrorism has not just recently become a threat to the United States—it was a threat to the United States long before September 11, 2001. However, the recent attacks on the United States brought the issue of terrorism to the forefront. The NSA was established in 1952 and has performed the functions of gathering intelligence and counterintelligence information since that time, attempting to prevent and detect acts of terror and war against the United States, so our nation's citizens may continue to realize their rights under the Constitution. President Reagan sought to strengthen this purpose with Executive Order 12,333, which was of great historical significance in the evolution of war and national defense legislation in the United States. The statutory provision in which Executive Order 12,333 was incorporated states:

In enacting this legislation, it is the intent of Congress to provide a comprehensive program for the future security of the United States; to provide for the establishment of integrated policies and procedures for the departments, agencies, and functions of the Government relating to the national security.

Congress' motivation in enacting this legislation was based on findings that "recent revolution-

---

161 See Richelson, supra note 7.
162 See NSA FREQUENTLY ASKED QUESTIONS, supra note 13 (stating that there is an internal review process within the NSA, the Office of the Inspector General, that oversees compliance with Executive Order 12,333).
163 See id.
164 See United Presbyterian Church in the U.S.A. v. Reagan, 557 F. Supp 61, 62 (D.D.C. 1982) (holding Executive Order 12,333 constitutional. Stating that the Order "establishes the framework in which our governmental and military agencies are to effectuate the process of gathering foreign intelligence and counterintelligence information, and the manner in which intelligence-gathering functions will be conducted at home and abroad).
ary world events require a fundamental reassessment of the defense and national security policies of the United States,"166 and "real and potential military threats to the United States and its allies will continue to exist for the foreseeable future from not just the Soviet Union but also from terrorism and from Third World nations."167 Congress, back in 1947, realized that the United States would have trouble maintaining its superpower status. It also determined that our nation’s ability to guard against subversive countries establishes the United States’ position as “mother hen” over those countries that cannot adequately protect themselves from opposing governments.168

The NSA must balance the aforementioned considerations with the privacy rights granted to all Americans. In doing so, the NSA has developed technological breakthroughs such as ECHELON that aid in the goals of preventing hostile governments and radical groups from destroying the security of the United States.169 At first glance, ECHELON may appear to tread upon forbidden soil, but further investigation reveals that adequate safeguards have been established to protect the civil liberties of all Americans.170 The NSA and its intelligence community partners will continue to fight an uphill battle against those who challenge their every move. With ever-evolving technological advances coming out of the woodwork, the government agencies and military factions in the intelligence community will have to justify the existence of such increased technology to their respective oversight boards and Congressional oversight committees.171 In some situations, the oversight committees may find that the encroachment on United States persons’ civil liberties is too broad, and the men and women that our people have elected to represent our best interests will be zealous advocates in a time of need.

However, if Congress finds that questionable technology is necessary to effectuate the purpose of a government agency, the military or the Constitution, it may determine that new legislation is necessary despite public opinion to the contrary. In response to the September 11th tragedy, for example, Congress enacted the Uniting and Strengthening America Act by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (“U.S.A. Patriot Act”).172 This bill provided the government with reduced judicial oversight for tapping phones, tracing e-mail, retrieving voice mail and tracking web surfing.173

VII. CONCLUSION

In light of the recent terrorist attacks on the United States, the evaluation of privacy matters must be conducted in a new context. The NSA is not asking Americans to put their privacy rights by the wayside, but it does hope to prove that its interception capabilities are not as broadly sweeping as one may imagine. The prospect that one’s private communications have a slim chance of interception by a government agency should be weighed against the benefit of the existence of technological surveillance such as ECHELON.174 For law-abiding citizens, the benefits of a secure nation far outweigh the infrequent risks to one’s individual expectation of private communications. Despite certain intrusions into United States citizens’ privacy rights, there are adequate judicial, statutory and administrative safeguards that protect Americans from an abuse of governmental power and secrecy. If the NSA is to continue to serve the nation by providing and protecting vital information, we must “embrace change and resume our place on the forward

---

167 Id.
168 Id. (stating that "emerging democracies around the world will require political, technical, and economic assistance, as well as military assistance, from the developed free nations in order to thrive and to become productive members of the world community").
169 See NSA FREQUENTLY ASKED QUESTIONS, supra note 13.
170 See Legal Standards, supra note 18.
171 See Bob Barr, Legislative Reform Commentaries: A Tyrant’s Toolbox: Technology and Privacy in America, 26 J. LEGIS. 71, 72-76 (2000) (discussing the various technological advancements and the need for an effective mechanism for protecting privacy in the information age).
174 Lawrence D. Sloan, Note, ECHELON and the Legal Restraints on Signals Intelligence: A Need for Reevaluation, 50 DUKE L.J. 1467, 1510 (2001) (stating that ECHELON must be “permitted to function in the most effective manner possible that does not unacceptably compromise the privacy and freedoms that are so important to Americans").
edge of technology."\(^{175}\)