ECHELON AND THE LEGAL RESTRAINTS ON SIGNALS INTELLIGENCE: A NEED FOR REEVALUATION

LAWRENCE D. SLOAN

> [The] 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: telephone conversations, telegrams, 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. . . . I know the capacity that is there to make tyranny total in America, and we must see to it that this agency and all agencies that possess this technology operate within the law and under proper supervision, so that we never cross over that abyss. That is the abyss from which there is no return.
>
> Senator Frank Church, August 17, 1975[1]

INTRODUCTION

Senator Church provided this powerful warning to the American people in 1975 after overseeing a congressional investigation into abuses by the National Security Agency (NSA) and other components of the intelligence community. The concerns that he expressed twenty-five years ago have resurfaced recently in connection with an American intelligence-gathering program referred to as ECHELON, which has been the subject of much controversy of late. While the full extent of the intelligence community's current capabilities is not entirely known, systems such as ECHELON are certainly far more effective than the systems that aroused such great fear in Senator Church. ECHELON is a code word that has been used to refer to the

1. *Meet the Press* (NBC television broadcast, Aug. 17, 1975), *quoted in* JAMES BAMFORD, THE PUZZLE PALACE 379 (1982).

worldwide effort on the part of the United States and its allies to intercept communications intelligence (COMINT).[2] ECHELON is believed to be a joint initiative led by the National Security Agency in conjunction with its counterparts in the United Kingdom, Canada, Australia, and New Zealand. It is believed to intercept all forms of global communication, from telephone conversations to satellite data transmission. The various allegations surrounding ECHELON can be roughly grouped into two categories. The first set of allegations, coming primarily from Europe, concerns the use of the ECHELON system to conduct economic espionage on behalf of American companies.[3] The second set of allegations involves the illegal use of ECHELON to collect intelligence about American citizens. This second set of allegations will be the focus of this Note. In a society such as ours, which considers privacy and freedom from intrusive government to be fundamental values,[4] the prospect of the American government spying on its citizens is extremely troubling. These allegations raise questions about the sufficiency of the legal restrictions placed on the collection and use of signals intelligence. The use of national intelligence assets to conduct industrial espionage for the benefit of American companies over their foreign competitors is controversial,[5] but that issue turns primarily upon matters of policy rather than law. This Note will focus on the legal restrictions on signals intelligence (SIGINT) activities and, thus, will set aside the primarily

2. COMINT is defined by the NSA as "technical and intelligence information derived from foreign communications by other than their intended recipient" and is a major component of signals intelligence (SIGINT), which also includes the collection of noncommunication signals such as radar emissions. Duncan Campbell, Interception Capabilities 2000 (Apr. 1999) (volume two in the five-volume report "Development of Surveillance Technology and Risk of Political Abuse of Economic Information," a working document for the Scientific and Technological Options Assessment Panel of the European Commission), http://www.iptvreports.mcmail.com/interception_capabilities_2000.htm (working document, on file with the *Duke Law Journal*). ECHELON is alleged to be primarily a COMINT program, but because the legal regime that surrounds it applies more broadly to SIGINT, these terms will both appear in this Note.

3. Suzanne Daley, *French Prosecutor Investigates U.S. Global Listening System*, N.Y. TIMES, July 5, 2000, at A9 [hereinafter Daley, *French Prosecutor*]; Suzanne Daley, *Is U.S. a Global Snoop? No, Europe Is Told*, N.Y. TIMES, Feb. 24, 2000, at A1.

4. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J. dissenting) ("They [the Framers of the Constitution] conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.").

5. Former Director of Central Intelligence James Woolsey was quoted in 1993 as saying that economic espionage has become "in some ways the hottest current topic in intelligence policy issues." Jim Mann, *Woolsey Cites Dangers in Economic Espionage*, L.A. TIMES, Feb. 3, 1993, at A10.

policy-driven question of using national intelligence assets to conduct economic espionage.[6]

Part I of this Note begins by surveying the origins of the ECHELON program and the various means by which COMINT is collected. It outlines how the public has become aware of ECHELON and what action has been taken in response to the various allegations leveled against the NSA. Part II of this Note provides an overview of the legal regime that has been put in place to protect innocent Americans from unconstitutional use of the powerful electronic surveillance technology possessed by the United States intelligence community. After discussing the interconnected concerns of the Fourth Amendment, federal legislation, executive orders, and agency regulations that make up this legal regime, Part III argues that this legal regime has not kept pace with recent fundamental changes in the field of communications technology and SIGINT. This part will highlight examples of how the concepts embodied in the legal regime are no longer viable given the recent evolution of communications technology. The author does not propose to provide specific revisions to the legal regime surrounding SIGINT collection, as this would be a nearly impossible task given the shortage of reliable, publicly available information. This Note instead attempts to use some specific examples to highlight what is likely a larger problem and convince the reader of the need for a thorough reevaluation of the legal regime that regulates SIGINT collection. Developing this legal regime presents the formidable task of balancing national security against individual liberties.[7] It is the responsibility of the President and our elected representatives in Congress to determine how this balance should be struck.

---

6. For more on the involvement of the intelligence community in economic espionage, see generally Michael T. Clark, *Economic Espionage: The Role of the United States Intelligence Community*, 3 J. INT'L LEGAL STUD. 253 (1997).

7. President Carter recognized this delicate balance when he stated that "one of the most difficult tasks in a free society like our own is the correlation between adequate intelligence to guarantee our nation's security on the one hand, and the preservation of basic human rights on the other." Robert A. Dawson, *Foreign Intelligence Surveillance Act: Shifting the Balance: The D.C. Circuit and the Foreign Intelligence Surveillance Act of 1978*, 61 GEO. WASH. L. REV. 1380, 1380 (1993). The drafters of our Constitution recognized the need to sacrifice personal freedom in the name of national security when they voted at the outset of the Constitutional Convention to restrict the content of the debates until after the drafters had produced an acceptable document. *Id.* at 1381 n.4. For more historical examples of the clash between national security and civil liberties, see MORTON H. HALPERIN & DANIEL N. HOFFMAN, FREEDOM VS. NATIONAL SECURITY: SECRECY AND SURVEILLANCE ix-xi (1977).

I. WHAT IS ECHELON?

A. Overview

The government has never specifically acknowledged the existence of a program with the code name ECHELON. The closest a representative of the United States intelligence community has come to publicly confirming the existence of ECHELON was when the Director of Central Intelligence, George Tenet, referred to the "so-called ECHELON program of the National Security Agency" in congressional testimony on signals intelligence activities in April 2000.[8] What has been published about the ECHELON system can be attributed to whistle-blowing former employees, internal leaks, freedom of information requests, and surely a healthy amount of speculation.[9] ECHELON is alleged to be the code word for a worldwide signals intelligence collection effort that is believed to intercept all forms of global communications, including telephone, facsimile, e-mail, and data transmission.[10] People writing about and discussing this subject have used the term ECHELON very broadly, and it currently refers to almost every element of communications intelligence operations carried out by the United States and its close allies.[11] There is evidence to suggest, however, that ECHELON was a code word used to refer to a network of computers that was used to process intercepted

8. *Hearing Before the House Permanent Select Comm. on Intelligence*, 106th Cong. (Apr. 12, 2000) (statement of George J. Tenet, Director of Central Intelligence), http://www.cia.gov/cia/public_affairs/speeches/archives/2000/dci_speech_041200.html (on file with the *Duke Law Journal*) [hereinafter Tenet Statement]. Tenet did not discuss ECHELON any further in his statement that dealt with the policies and legal restraints that govern signals intelligence operations. *Id.*

9. For a good description of how one goes about researching a top-secret subject, such as ECHELON, see generally Nicky Hager, *Researching Echelon*, TELEPOLIS, Apr. 11, 2000 (describing how New Zealand author Nicky Hager obtained classified information for his book, *Secret Power*, which describes New Zealand's role in the UK/USA global alliance), http://www.heise.de/tp/english/inhalt/co/5993/1.html (on file with the *Duke Law Journal*).

10. Tom Zeller, *Cloak, Dagger, Echelon*, N.Y. TIMES, July 16, 2000, at A16 ("At its core, ECHELON is a network of ground stations with dishes aimed at the dozen or so satellites that now shepherd much of the world's television, fax, Internet and voice data.").

11. Niall McKay, *Did EU Scuttle Echelon Debate?*, WIRED NEWS (Oct. 5, 1998) ("According to scores of reports online and in newspapers, Echelon can intercept, record, and translate any electronic communication—telephone, data, cellular, fax, email, telex—sent anywhere in the world."), *at* http://wired.com/news/politics/0,1283,15429,00.html (on file with the *Duke Law Journal*); Jeffrey Richelson, *Desperately Seeking Signals*, 56 BULL. ATOMIC SCIENTISTS 47 (Mar.-Apr. 2000) ("According to much of the press coverage, Echelon is the code word for the UKUSA 'global surveillance network.' But it is not, nor is there any code word for the overall U.S. or UKUSA SIGINT . . . apparatus."), *at* http://www.bullatomsci.org/issues/2000/ma00/ma00richelson.html (on file with the *Duke Law Journal*).

signals.[12] Even if ECHELON was once the code name for one aspect of the United States's COMINT effort, this code word likely has been abandoned as the intelligence community generally changes code words when they are compromised.[13] Since it is impossible from the available information to delineate the precise boundaries of ECHELON, the term will be used generically to refer to the American communications intelligence effort.

The ECHELON program is coordinated by the National Security Agency, the lead signals intelligence agency in the United States.[14] Although the United States plays the lead role in administering ECHELON, the program is a global effort that fully integrates the NSA's counterparts in the United Kingdom (Government Communications Headquarters—GCHQ), Canada (Canadian Communications Security Establishment—CSE), Australia (Defense Signals Directorate—DSD), and New Zealand (Government Communications Security Bureau—GCSB).[15] The basis of this cooperation dates back to the World War II–era BRUSA COMINT alliance. This communications intelligence cooperation agreement between the United States and Britain was ratified on May 17, 1943.[16] After World War II, in 1946-47, the United Kingdom formed the Commonwealth SIGINT Organization, which incorporated Canada, Australia, and New Zealand.[17] The United States and the United Kingdom, on behalf of its Commonwealth SIGINT partners, entered into the post-war UKUSA

12. 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.").

13. *See* JEFFREY T. RICHELSON, THE U.S. INTELLIGENCE COMMUNITY 173 (1989) (describing how "in accordance with standard security practice," the National Reconnaissance Office changed the code name of the RHYOLITE satellite to AQUACADE when it was learned that two contractors working on the satellite sold details of the program to the KGB). Richelson also describes how a satellite program "[o]riginally code-named CHALET. . .was renamed VORTEX after its original code name was revealed in the press." *Id.* at 174.

14. The National Security Agency (NSA) was established to serve as the primary COMINT organization in the United States by President Truman. Memorandum from President Harry S. Truman to Secretaries of State and Defense (Oct. 24, 1952) (entitled "Communications Intelligence Activities"), http://www.nsa.gov/docs/efoia/released/truman/truman.tif (on file with the *Duke Law Journal*). For a complete discussion of the history and operations of the NSA, see generally BAMFORD, *supra* note 1.

15. *Accord* PATRICK S. POOLE, ECHELON: AMERICA'S SECRET GLOBAL SURVEILLANCE NETWORK (1999), http://fly.hiwaay.net/%7Epspoole/echelon.html (on file with the *Duke Law Journal*).

16. DESMOND BALL & JEFFREY RICHELSON, THE TIES THAT BIND: INTELLIGENCE COOPERATION BETWEEN THE UKUSA COUNTRIES 138 (1985).

17. *Id.* at 142-43.

agreement in 1947. This agreement is believed to have established procedures through which the SIGINT organizations in the five countries cooperate, but its details are still a secret.[18] The Australian government was the first to publicly acknowledge the UKUSA agreement in March 1999 when the Director of the Defense Signals Directorate (DSD) stated that DSD "does co-operate with counterpart signals intelligence organisations overseas under the UKUSA relationship."[19] No other government has officially acknowledged the UKUSA agreement.[20] These relationships have been solidified with detailed bilateral agreements between the parties.[21] It is believed that the result of these agreements is that the five nations cooperate very closely in all aspects of the collection and processing of signals and share the final product. Working closely with its allies allows the United States to achieve global coverage and also to defer some of the costs associated with this undertaking.[22]

This worldwide network of COMINT programs is believed to intercept all forms of global communication, including land-line and cellular telephone calls, satellite communications, electronic mail, facsimiles, and various forms of radio transmission. Historically, the traditional COMINT targets have been military and diplomatic communications,[23] but these communications often travel over the same

---

18. POOLE, *supra* note 15.

19. *The Sunday Programme* (Channel 9 television broadcast (Australia), Apr. 11, 1999) (reporting a statement by Martin Brody, Director of DSD, on March 16, 1999).

20. In response to a 1982 Freedom of Information Act request submitted to NSA requesting "all documents from 1947 outlining United States-United Kingdom-Australia-Canadian-New Zealand cooperation in Signals Intelligence," the NSA responded, "We have determined that the fact of existence or nonexistence of the materials you request is in itself a currently and properly classified matter." BALL & RICHELSON, *supra* note 16, at 1 (providing a photocopy of a letter sent to Richelson from Eugene Y. Yeates, Director of Policy, National Security Agency, dated December 7, 1982).

21. POOLE, *supra* note 15 (noting that "direct agreements between the U.S. and these [foreign] agencies also define the intricate relationship" between parties to the UKUSA agreement).

22. RICHELSON, *supra* note 13, at 268. The result of this close working relationship is a complex division of responsibility:

> Under the present division of responsibilities the United States is responsible for Latin America, most of Asia, Asiatic Russia and northern China. Australia's area of responsibility includes its neighbors (such as Indonesia), southern China, and the nations of Indochina. Britain is responsible for the Soviet Union (west of the Urals) and Africa. The polar regions of the Soviet Union are Canada's responsibility, New Zealand's areas of responsibility was the western Pacific.

Id. For a complete discussion of the history and mechanics of the UKUSA arrangement, see BALL & RICHELSON, *supra* note 16, at 135-44.

23. RICHELSON, *supra* note 13, at 167-68. Richelson gives an extensive description of COMINT targets:

media as commercial and private communications.[24] During the Cold War, this system focused primarily upon the Soviet Union and its allies.[25] In the wake of the Cold War, the COMINT establishment has necessarily shifted its focus to transnational threats such as narcotics trafficking, weapons of mass destruction, terrorism, and organized crime.[26]

Ever since electronic communication systems first came into general use in the mid-1800s, the United States has been using electronic surveillance to collect intelligence information.[27] Interception of communications has not always been a high priority for the United States. In fact, in 1929 Secretary of State Henry L. Stimson angrily ordered the dismemberment of the United States's only code-breaking unit, because he believed that "[g]entlemen do not read each other's mail."[28] Secretary Stimson later recognized that this statement was overly idealistic given the exigencies of the modern world.[29] Effective intelligence has proven to be invaluable to the protection of United States national security interests, and SIGINT is especially valuable to policymakers, because its authenticity is more easily determined than other forms of intelligence. According to Lieutenant General Marshall S. Carter, former deputy director of the CIA and former director of the NSA,

---

> The most traditional COMINT target is diplomatic communications—the communications from each nation's capital to its diplomatic establishments around the world. . . . The United States also targets the communications between different components of a large number of governments. . . . More specifically, the United States intercepts communications between the Soviet Ministry of Defense and Military District headquarters, and between Military District headquarters and units in the field.

Id.

24. *Id.* (quoting an observer as saying, "With modern communications, 'target' messages travel not simply over individually tappable wires like those that connect the ordinary telephone, but as part of entire message streams, which can contain up to 970 individual message circuits, and have voice, telegram, telex and high speed data bunched together").

25. The large proportion of the discussion of SIGINT that focuses on systems targeted at the Soviet Union is indicative of the importance of this target at the time the book was written in 1989. *See id.* at 167-97.

26. Tenet Statement, *supra* note 8 ("SIGINT is critical to monitoring terrorist activities, arms control compliance, narcotics trafficking, and the development of chemical and biological weapons and weapons of mass destruction.").

27. William F. Brown & Americo R. Cinquegrana, *Warrantless Physical Searches for Foreign Intelligence Purposes: Executive Order 12,333 and the Fourth Amendment*, 35 CATH. U. L. REV. 97, 103 (1985) (noting that the executive branch has used "warrantless electronic surveillance" to collect intelligence information since at least the mid-1800s).

28. HENRY L. STIMSON & MCGEORGE BUNDY, ON ACTIVE SERVICE IN PEACE AND WAR 188 (1947).

29. Brown & Cinquegrana, *supra* note 27, at 102.

> HUMINT [Human Intelligence] is subject to all of the mental aberrations of the source as well as the interpreter of the source. . . . SIGINT has technical aberrations which give it away almost immediately if it does not have bona fides, if it is not legitimate. A good analyst can tell very, very quickly whether this is an attempt at disinformation, at confusion, from SIGINT. You can't do that from HUMINT; you don't have the bona fides—what are his sources? He may be the source, but what are *his* sources?[30]

General Carter similarly believes that SIGINT is more useful than photographic intelligence:

> Photo interpretation can in some cases be misinterpreted by the reader or intentionally confused by the maker in the first place—camouflage, this sort of thing. SIGINT is the one that is immediate right now. Photo interpretation, yes, to some extent, but you still have to say "Is that really a fake, have they confused it?"[31]

For these reasons, SIGINT has slowly supplanted HUMINT as the most important form of intelligence.

B. Collection of Signals

The process of producing COMINT can be broadly divided into two steps: the collection of signals and the processing of those signals.[32] The collection techniques depend on the medium being intercepted. It is alleged that ECHELON intercepts all major modes of signal transmission, including land-lines, high frequency radio, microwave radio relay, communications satellites, subsea cables, and the Internet.

---

30. BAMFORD, *supra* note 1, at 377-78.

31. *Id*. at 378; *see also id.* ("Where once America's chief source of raw intelligence was the clandestine agent with his or her Minox camera, today that source is the same worldwide blanket of microwave signals and rivers of satellite transmissions that gives us our telephone calls, our remote banking, telegrams and, soon, our mail.").

32. The collection and processing of signals is the focus of this section of this Note, but they are only two steps in what is referred to as the "intelligence cycle." Prior to collection or processing of signals, there must be a planning phase in which the consumers of intelligence, such as officials of the Departments of Defense and State, identify their intelligence requirements. Once requirements are established, the NSA must then task its assets to collect and process relevant signals. After the signals have been collected and processed, analysts must convert the numerous pieces of raw intelligence into a single, meaningful intelligence report. The finished product is then disseminated to consumers, the final step of the intelligence cycle. For two similar depictions of how the "intelligence cycle" operates, see COLONEL JOHN HUGHES-WILSON, MILITARY INTELLIGENCE BLUNDERS 6 (1999); and Campbell, *supra* note 2.

Before any signals can be collected or processed, the SIGINT agency must have a means of accessing the signals. The majority of signals are believed to be accessed illegally, but there have been cases where the owners of the communications facilities have cooperated with the intelligence agency. For example, from 1945 to 1975, the three major telegraphic information carriers in the United States allowed the NSA, in a project code-named SHAMROCK, to access all of their traffic.[33] In a modern twist on project SHAMROCK, it is alleged that there are currently three major British Telecomm fiber-optic telephone trunk lines (each capable of carrying 100,000 calls simultaneously) that run through Menwith Hill—an American military installation in North Yorkshire, England, that is believed to be the largest spy station in the world.[34] The existence of some form of access agreement between British Telecomm and the NSA is further supported by allegations that in 1975 British Telecomm provided a coaxial cable connection from Menwith Hill to a British Telecomm microwave facility four miles away.[35]

Various other forms of communication are accessed without the knowledge of their owners using a variety of techniques. High frequency (HF) radio systems were the most common means of international telecommunication prior to 1960. HF signals travel long distances by bouncing between the earth's surface and the ionosphere. This makes them susceptible to interception by large ground-based arrays.[36]

---

33. BAMFORD, *supra* note 1, at 238 ("[D]espite the fear of prosecution and the warnings of their legal advisers, all three companies began taking part in what, for security reasons, was given the name Operation Shamrock."). Project Shamrock came to an abrupt halt after concerns arose as to its possible public disclosure. *Id*. at 236 (noting that fear of "exposure by a persistent press and increasingly aggressive congressional committees" were reasons for the decision to terminate Operation Shamrock).

34. POOLE, *supra* note 15:

> In documents and testimony submitted by British Telecomm in the case [of two women appealing their convictions for trespassing at the facility], R.G. Morris, head of Emergency Planning for British Telecomm, revealed that at least three major domestic fiber-optic telephone trunk lines—each capable of carrying 100,000 calls simultaneously—were wired through Menwith Hill.

Ben Rooney, *Unless You Are a Celebrity, Privacy Is of Little Concern to You. But Snooping Is All Too Common in the Digital World*, THE DAILY TELEGRAPH (LONDON), Jan. 4, 2001, at 4 ("The world's largest National Security Agency station outside America, RAF Menwith Hill, is the cornerstone of this global routine surveillance.").

35. POOLE, *supra* note 15.

36. Campbell, *supra* note 2. Most of the information describing the alleged capabilities of the ECHELON system is taken from this source, because this author believes that it is the most credible product available. Its author, Duncan Campbell, wrote the first press report on ECHELON in 1988 and has continued to investigate ECHELON.

Microwave radio relay was introduced in the 1950s to provide high-capacity intercity communications for telephony, telegraphy, and later, television. These systems consist of small, low-power transmitters on hilltops that can relay their signals to stations thirty to fifty kilometers away.[37] Only a small portion of the signal is captured by each relay station, which results in the majority of the signal passing over the horizon and out into space. Beginning in 1968, this microwave spillover was exploited with the launch of CANYON, the first American COMINT satellite capable of collecting these errant signals.[38] There are believed to be four of the most recent versions of these satellites, code-named MERCURY, in orbit collecting microwave signals which pass over the horizon and into space.[39]

In addition to MERCURY, there are two other classes of COMINT collection satellites currently in use. The ORION-class satellites are believed to be controlled from Pine Gap, Australia, and they target VHF radio, cellular mobile phones, paging signals, and mobile data links.[40] TRUMPET-class satellites intercept the same signals as MERCURY and ORION but are positioned in elliptical near-polar orbits that allow them to remain over high northern latitudes for extended periods of time.[41] The United States National Reconnaissance Office (NRO), the Department of Defense (DoD) organization tasked with constructing and maintaining space-based intelligence systems, has announced plans to consolidate these three separate classes of COMINT satellites into what it refers to as an integrated overhead SIGINT architecture.[42]

Communication satellites (COMSATS) have become an increasingly common means of communication since their introduction in 1967. The current iterations of COMSATS permit various forms of communication, such as telephone, facsimile, television, and data to be transmitted simultaneously over the same satellite at a rate equivalent to 90,000 simultaneous telephone calls.[43] The data transmitted on these satellites is primarily intercepted by ground-based antennae. The major COMSAT interception facilities are alleged to be located in Morwenstow, England; Yakima, Washington; and Sugar

37. *Id*.
38. *Id*.
39. JEFFREY RICHELSON, THE U.S. INTELLIGENCE COMMUNITY 185 (4th ed. 1999).
40. *Id.*
41. Campbell, *supra* note 2.
42. *Id*.
43. *Id*.

Grove, West Virginia, with smaller facilities in Canada, Australia, and New Zealand.[44]

A sizeable portion of transoceanic communication occurs over subsea cables, which today consist primarily of fiber-optic cables.[45] These were believed to be an inherently secure means of communication until a United States submarine, the USS Halibut, successfully "tapped" an undersea Soviet military communication line in October 1971.[46] It is believed that a specially modified 1980s vintage submarine, the USS Parche, continues to conduct cable-tapping operations around the world.[47] Since fiber-optic cables do not "leak" signals, these undersea cables are most likely "tapped" by meddling with the opto-electronic repeaters that are used to boost optical signals transmitted over long distances.[48]

Given the wide-ranging activities of the ECHELON program and the fact that an estimated 1.4 billion e-mail messages change hands every day,[49] it is not surprising to learn that there have been allegations that ECHELON also intercepts Internet traffic.[50] Marc Rotenberg, Director of the Electronic Privacy Information Center, stated that his organization "had reason to believe that the NSA is engaged in the indiscriminate acquisition and interception of domestic communications taking place over the Internet."[51] The Internet would seem to present unique opportunities for the NSA. Because a large portion of the Internet capacity of the world is found in the United States, and because messages are often routed through the

---

44. *Id*.

45. *Id*.

46. SHERRY SONTAG & CHRISTOPHER DREW, BLIND MAN'S BLUFF: THE UNTOLD STORY OF AMERICAN SUBMARINE ESPIONAGE 171-72 (1998) (describing the USS Halibut mission).

47. Campbell, *supra* note 2.

48. *Id*.

49. Stephen Labaton & Matt Richtel, *Proposal Offers Surveillance Rules for the Internet*, N.Y. TIMES, July 18, 2000, at A1.

50. *Electronic Privacy Group Sues Security Agency*, N.Y. TIMES, Dec. 4, 1999, at A13 (describing a lawsuit demanding that the NSA release records concerning the use of ECHELON for Internet surveillance) [hereinafter *Electronic Privacy Group*]. The United States is certainly not the only country that has been accused of intercepting communications on the Internet for intelligence purposes. Russia has admitted that its intelligence services are capable of intercepting and monitoring all Russian Internet traffic. *Brits Launch Online Spy Network*, WIRED NEWS (May 2, 2000), *at* http://www.wired.com/news/business/0,1367,36031,00.html (on file with the *Duke Law Journal*). The British are reported to be developing a similar system that would require all of Britain's Internet service providers to be connected to the British intelligence agency, MI5. *Id*.

51. Jeri Clausing, *Privacy Group Sues for U.S. Files on Spying*, N.Y. TIMES ON THE WEB (Dec. 4, 1999), *at* http://www.nytimes.com/library/tech/99/12/cyber/articles/04spy.html (on file with the *Duke Law Journal*).

least congested servers[52] regardless of the geographic distance traveled, many foreign messages pass through the United States where they are easily accessed by the NSA.[53] A former NSA employee has alleged that by 1995 the NSA had already installed sniffer programs to collect Internet traffic at nine major Internet exchange points in the United States.[54] Such sniffer programs would allow the monitoring of all traffic passing through the system. Allegations that it only took the NSA eleven months to fill what was projected to be three years' worth of storage capacity for intercepted Internet traffic suggests the scope of this effort.[55]

Although little has been written about the details of the NSA's technical capability to intercept Internet traffic, the Federal Bureau of Investigation (FBI) has not been as successful keeping its Internet interception capability out of the press.[56] An FBI program referred to

---

52. ROBIN BURK ET AL., UNIX UNLEASHED, SYSTEM ADMINISTRATOR'S EDITION (n.d.), http://www.ctel.msk.ru/~ftp/EBooks/Vol_1/ch07.htm (last visited Jan. 31, 2001) (on file with the *Duke Law Journal*):

> When a mail message is sent over the Internet, it is sent as a stream of packets, each containing a portion of the message. Each packet also contains the IP address of the destination. The packets are sent over the Internet using the IP protocol. Specialized networking systems on the Internet, known as routers, examine the IP address in each packet, and route it to the appropriate host.

53. *Hungarian Radio Calls Echelon System Surveillance by "Big Brother" and Siblings*, BBC WORLDWIDE MONITORING, Mar. 26, 2000 ("A considerable proportion of the international Internet traffic goes through the large US servers.").

54. Campbell, *supra* note 2.

55. *Electronic Privacy Group*, *supra* note 50.

56. Many of the same privacy groups that have sounded the alarm concerning ECHELON have raised similar privacy concerns in connection with CARNIVORE, including the American Civil Liberties Union (ACLU) and the Electronic Privacy Information Center (EPIC). John Schwartz, *Wiretapping System Works on Internet, Review Finds*, N.Y. TIMES, Nov. 22, 2000, at A19 (providing criticism of CARNIVORE from both ACLU associate director Barry Steinhardt and EPIC general counsel David Sobel) [hereinafter Schwartz, *Wiretapping*]. In response to public outcry over CARNIVORE that prompted congressional criticism, the Department of Justice commissioned the Illinois Institute of Technology's (IIT) Research Institute to conduct an independent evaluation of CARNIVORE. *Id.*; John Schwartz, *Computer Security Experts Question Internet Wiretaps*, N.Y. TIMES, Dec. 5, 2000, at A16 [hereinafter Schwartz, *Computer Security*]. A draft of the report produced by IIT, entitled *Independent Technical Review of the Carnivore System*, is available at http://www.usdoj.gov/jmd/publications/carnivore_draft_1.pdf (last visited Feb. 26, 2001) (on file with the *Duke Law Journal*). The IIT report confirmed that CARNIVORE does exactly what the FBI claims, but that certain additional safeguards should be incorporated to ensure that CARNIVORE only collects the specific type of information authorized for a given case. Schwartz, *Wiretapping*, *supra.* The results of the review conducted by IIT do not seem to have satisfied privacy activists who claim that the review did not address key issues. Schwartz, *Computer Security*, *supra*:

> Despite winning a favorable review by an outside group, the F.B.I.'s Carnivore Internet wiretap system continues to raise strong concerns about privacy and the legal limits of government surveillance, a prominent panel of security experts said yesterday. . . . While lauding the Justice Department and [IIT] for a good-faith effort to ex-

as CARNIVORE,[57] which is designed to allow that organization to intercept information passing through the Internet, including e-mail, attached documents, and instant messages, has recently become the subject of intense public scrutiny.[58] CARNIVORE is a piece of hardware, described as a "small black box," and a piece of software, which are installed at the facility of an Internet service provider (ISP), such as America Online or Earthlink.[59] Once installed, the black box operates in conjunction with the software component to scan Internet traffic passing through the Internet service provider's network.[60] CARNIVORE can be programmed to intercept and collect specific messages that are of interest to the FBI, such as those sent from a particular network or e-mail account.[61] Prior to the use of technology such as CARNIVORE, the FBI must obtain judicial authorization in the form of a warrant identifying the nature of the subject matter to be intercepted.[62] Although there have been no allegations that

---

amine the Internet wiretap system, the computer experts said that that study was designed too narrowly to answer the most pressing questions.

57. It is reported that in February 2001 the FBI changed the name of this program from CARNIVORE to the less controversial DCS 1000. *Carnivore Gets a Name Change*, UNIX INSIDER, Feb. 2001 ("The government agency has confirmed it changed the name of the controversial, email sniffing software from Carnivore to DCS1000. . . . The name change is part of the government's attempts to allay fears about the digital monitoring program."). There are reports that the DCS in the new name stands for "digital collection system," although the FBI has not confirmed this. *Id.* The FBI has stated that the 1000 refers to the first version of the system and that DCS2000 will probably be released in the not-too-distant future. *Id*.

58. Labaton & Richtel, *supra* note 49 (reporting on CARNIVORE's capabilities and the surrounding controversy).

59. *Id.* (describing CARNIVORE as a "system").

60. Michael J. Sniffen, *U.S. Selects Unit of IIT to Analyze FBI's E-mail Surveillance System for Safeguards*, CHI. TRIB., Sept. 27, 2000, at 3 (noting that CARNIVORE "has software that scans Internet traffic"). CARNIVORE is essentially a modified "packet sniffer," a diagnostic tool used to monitor networks. Stephen P. Smith et al., *Independent Review of the Carnivore System—Draft Report* (Nov. 17, 2000), http://www.usdoj.gov/jmd/publications/carnivore_draft_1.pdf (on file with the *Duke Law Journal*). The draft provides a surprisingly detailed description of the technology and operation of CARNIVORE. *Id*.

61. Stephen Labaton, *Learning to Live with Big Brother*, N.Y. TIMES, July 23, 2000, § 4, at 3 ("Carnivore could, for instance, be programmed to pick up the e-mail from only one sender and a particular computer, while excluding such e-mail as messages to or from, say, the sender's lawyer or wife.").

62. It is important to note that law enforcement programs, such as CARNIVORE, are subject to greater judicial scrutiny and oversight than foreign intelligence programs, such as ECHELON. *See FBI Programs and Initiatives: Carnivore Diagnostic Tool* (describing the steps necessary for the FBI to obtain approval to employ CARNIVORE), http://www.fbi.gov/programs/carnivore/carnivore2.htm (last visited Jan. 25, 2001) (on file with the *Duke Law Journal*). All uses of CARNIVORE require the FBI to seek judicial authorization in the form of a warrant. *Id.* In contrast, the NSA has discretion to use programs like ECHELON without obtaining judicial authorization as long as the surveillance does not occur within the United States. For a more complete discussion of the legal regime regulating NSA

CARNIVORE is in any way connected with the NSA, the technology involved is likely to be similar to some of the tools used by the NSA to intercept Internet-based communications.

C. Processing of Signals

The sheer volume of information that likely is collected through the above techniques is unimaginably large. The vast majority of the information collected is of no interest to the intelligence agencies that collect it and must be systematically discarded. The essence and magnitude of this process was conveyed by former NSA Director William Studeman, who revealed that

> [o]ne [unmodified] intelligence collection system alone can generate a million inputs per half hour; filters throw away all but 6,500 inputs; only 1,000 inputs meet forwarding criteria; 10 inputs are normally selected by analysts and only one report is produced. These are routine statistics for a number of intelligence collection and analysis systems which collect technical intelligence.[63]

Various automated data-analysis techniques are believed to be used to filter this data before it is seen by a human analyst. The core tool used in the analysis of intercepted communication has been referred to as the "dictionary computer." These dictionary computers, which are located at various collection sites around the world, contain a large database of specified targets, including names, keywords of interest, addresses, and telephone numbers. Incoming messages are evaluated against these criteria in an attempt to have the computer automatically extrapolate interesting pieces of intelligence.[64] The dictionary computers dispersed around the world are allegedly all wired into one network, in a manner similar to a corporate intranet.[65] Each UKUSA member has access to this worldwide network and can inde-

---

operations, see *infra* notes 114-74 and accompanying text.

63. Vice Admiral William Studeman, Deputy Director of Central Intelligence, Address to the Symposium on National Security and National Competitiveness (Dec. 1, 1992), *quoted in* Campbell, *supra* note 2.

64. Campbell, *supra* note 2 ("Incoming messages are compared to these criteria; if a match is found, the raw intelligence is forwarded automatically.").

65. As one commentator recently noted:

> Before Echelon appeared in the 1970's, the agencies shared intelligence, but they usually processed and analyzed the intercepted communications. As a result, most exchanges involved finished reports rather than raw intercepts. Echelon, on the other hand, is an integrated network that allows the agencies to specify which intercepts are of interest and to receive them automatically via computer.

Richelson, *supra* note 11.

pendently add or modify targets on the various dictionary computers around the world. If the dictionary receives a message that meets the target criteria, it automatically forwards that piece of intelligence electronically to the agency that specifically requested it.[66] UKUSA members are also believed to have the ability to search the various dictionary computers from a remote location to find previous messages of interest.[67]

Telephone calls and other aural media are generally analyzed based on call-identifying information such as country of origin.[68] Contrary to popular belief, automated word-spotting software that would allow automated processing of verbal communication is not reported to be currently available.[69] This has not been for lack of effort, as former NSA Director Admiral Bobby Inman admitted, "I have wasted more U.S. taxpayer dollars trying to do that [word spotting in speech] than anything else in my intelligence career."[70] Voice-recognition software, however, which can identify the voice of a targeted speaker, is believed to have been in use since at least 1995.[71]

The analysis process described above can be complicated if the intercepted signals have been encrypted. Encryption converts a message into incomprehensible data that can only be read by a recipient with a proper key.[72] Both written and oral communication can be encrypted to disguise content from unauthorized recipients. Generally, encrypted signals that are collected by the NSA must be decrypted before they can be analyzed in a meaningful manner.[73] Depending on

66. Campbell, *supra* note 2.

67. *Id.* ("ECHELON . . . enable[s] remote intelligence customers to task computers at each collection site . . . .").

68. Richelson, *supra* note 11 ("[T]he phones of the parties involved in a call can be automatically identified and voice-prints can be used to identify who is speaking.").

69. Campbell, *supra* note 2.

70. Richelson, *supra* note 11.

71. Campbell, *supra* note 2.

72. Norman Andrew Crain, Note, Bernstein, Karn, *and* Junger*: Constitutional Challenges to Cryptographic Regulations*, 50 ALA. L. REV. 869, 871 (1999) (describing encryption and decryption). A more sophisticated description of how encryption works is certainly beyond the scope of this Note. For a comprehensive history of the use and development of encryption, see generally SIMON SINGH, THE CODE BOOK: THE EVOLUTION OF SECRECY FROM MARY, QUEEN OF SCOTS, TO QUANTUM CRYPTOGRAPHY (1999).

73. In certain circumstances it is possible for encrypted signals that have not been decrypted to be meaningfully analyzed. Targets can be subjected to traffic analysis that focuses on the parties to a communication and the volume of that communications as opposed to the content of those communications. SINGH, *supra* note 72, at 318 ("Codebreakers continue to use old-fashioned techniques like traffic analysis; if codebreakers cannot fathom the contents of a message, at least they might be able to find out who is sending it, and to whom it is being sent, which in itself can be telling.") For example, a large increase in the volume of communications ema-

the sophistication of the encryption and the resources dedicated to cracking that encryption, the decryption process can be quite time-consuming, and in some cases even impossible.[74] Encryption has historically been the exclusive tool of governments, but with increasing use of personal computer technology and concerns for personal privacy, a demand for encryption accessible to the general public has recently emerged.[75] The de facto standard for private encryption is a program called Pretty Good Privacy (PGP). PGP offers personal-computer users access to military-grade encryption that, when set to its highest level of encryption, is believed to be unbreakable by organizations such as the NSA.[76] Programs such as PGP have become increasingly user-friendly and are available on the Internet for free download. Because it threatens its ability to provide timely

nating from a Soviet submarine base could be used to infer that there might be some type of accident at the base, or that the base was preparing to launch a new type of submarine.

74. Encryption that uses a randomly generated "one-time pad" is the only type of encryption that can be said to be entirely unbreakable because there are no patterns in the code to assist the code breaker. *Weekend Edition—Saturday* (National Public Radio broadcast, Sept. 25, 1999) (interview with Scott Simon, author of *The Code Book*), http://search.npr.org/cf/cmn ("Now there is one type of code that is unbreakable. It's called a one-time pad, and the one-time pad is a random series of instructions; and if it's truly random, there are no patterns; and if there are no patterns, then there's nothing for the code breaker to latch onto.") (on file with the *Duke Law Journal*). Of course, encryption methods that are theoretically breakable may be in practice unbreakable; for example, a code that would require 1,000 years of computing power to decrypt is effectively unbreakable.

75. Ronald Stay, Note, *Cryptic Controversy: U.S. Government Restrictions on Cryptography Exports and the Plight of Philip Zimmermann*, 13 GA. ST. U. L. REV. 581, 582-83 (1997).

76. *Id.* at 584-85 (citing William M. Bulkeley, *Cipher Probe: Popularity Overseas of Encryption Code Has the U.S. Worried*, WALL ST. J., Apr. 28, 1994, at A1). Admiral William Crowell, former Deputy Director of the NSA, testified before the Senate in September 1996 that it would take a computer expert 100 quadrillion years to break a message encrypted in a 128-bit algorithm, a level of encryption available in PGP. *Security and Freedom Through Encryption (SAFE) Act: Hearing on H.R. 3011 Before the House Comm. on the Judiciary*, 105th Cong. 34-55 (1996) (statement of Admiral William P. Crowell, Deputy Director, National Security Agency). Of course, with the continuing increases in computing power, today's unbreakable encryption may become vulnerable in the future. Phillip Manchester, *Cracking the Code Is Just a Matter of Time: As Processing Power Proliferates, Today's "Unbreakable" Encryption Keys Could Become Inadequate Tomorrow*, FIN. TIMES, June 7, 2000, at 7 ("[W]ith Moore's famous law—computer power doubles every 18 months—still applicable for at least another decade, it is conceivable that today's 'unbreakable' encryption will be inadequate tomorrow.").

intelligence to its consumers,[77] the spread of sophisticated encryption is of great concern to the NSA.[78]

Although it is possible that there are additional capabilities that have not yet been revealed, it is more likely that a number of the NSA's capabilities with respect to COMINT collection and analysis have been exaggerated in the recent discussion of ECHELON.[79] As a government agency with finite resources, it is unlikely that the NSA is able to intercept every form of global communication, as has been alleged. Jeffrey Richelson, a senior fellow at the National Security Archive who has been following the ECHELON issue closely, expressed this view:

> I would be very skeptical that the N.S.A. could or even would try to process every bit of data out there. . . . It makes sense to question how information they do gather is used, but the hysterical idea that the N.S.A. really cares about the e-mail conversations of everyday citizens is bottom-line nonsense. What everyone is worried about doesn't really exist.[80]

An unnamed "U.S. government official with ties to the intelligence community" similarly dismissed some of the more extravagant rumors:

> I wish we had something like that which was that good. I mean, it would make my life so much easier, but it just isn't there. . . . I don't

77. Intelligence has little value unless it can be delivered in a timely manner. For example, on December 6, 1941, U.S. codebreaking groups were able to intercept a fourteen-part message from the Japanese government to its American ambassador in Washington. HUGHES-WILSON, *supra* note 32, at 84-85. The fourteenth piece of the message, which provided warning of the impending attack on Pearl Harbor, was not decrypted in time to be distributed with the other parts of the message, and consequently the intelligence agencies were unable to provide sufficient warning of the attack. *Id.* at 85-86 (noting that the fourteenth part of the message indicated Japanese intent to break off negotiations and was interpreted as also indicating that an attack on American forces in Hawaii was likely). Although there were other failures in the dissemination process, which ultimately caused the alarms not to be raised in time, if the fourteenth part had been disseminated earlier with the other parts of the message, the Pearl Harbor attack may have been averted or diminished.

78. *See* Joel C. Mandelman, *Lest We Walk into the Well: Guarding the Keys—Encrypting the Constitution: To Speak, Search & Seize in Cyberspace*, 8 ALB. L.J. SCI. & TECH. 227, 231-32 (1998) ("The National Security Agency has expressed concerns that if advanced encryption technology becomes widely available its most sensitive counter-intelligence and counter-terrorism operations will be seriously jeopardized.").

79. Among the more outrageous claims is that of an unidentified British website, which, according to the New York Times, "seeks to expose Echelon as a source of 'psychotronic attacks' and 'mind control experimentation.'" Zeller, *supra* note 10, at A16.

80. Zeller, *supra* note 10, at A16 (quoting Richelson).

> really expect a lot of people having a great time with these Echelon stories to believe what I tell you, but just go back and do the math.[81]

Observers have suggested that much of the hype surrounding ECHELON has been fueled by the movie industry.[82] In movies such as *Enemy of the State* and *Mercury Rising*, the NSA is portrayed as a lawless organization whose members will go to extreme lengths to advance or protect their personal or professional interests.[83] Movies such as these make the public more susceptible to accepting outrageous claims associated with ECHELON. In fact, a fair number of NSA-observers assert that the agency has done a poor job of keeping pace with the progress of technology.[84] Richelson specifically cites the ex-

---

81. Thomas C. Greene, *Echelon Spy System Wildly Exaggerated—Official* (Aug. 1, 2000), http://www.theregister.co.uk/content/6/12294.html (on file with the *Duke Law Journal*); *see also id.*:

> The unidentified government official urged, Get some of those articles that purport to describe the ability of the Echelon system to do marvellous things, and [think through] the engineering work. . . . Figure out how much processing power it would require, the types of collaboration one would need with people who build telecommunications systems, and the amount of government employees you would need to read all the stuff that gets scooped out. We just haven't got it.

Of course, the diehard ECHELON conspiracy theorists assert that statements such as these are merely part of a disinformation campaign designed to deflect attention from the true capabilities of the ECHELON system. *Cryptome Note*, *at* http://cryptome.org/echelon-wily.htm (last visited Feb. 24, 2001) (on file with the *Duke Law Journal*):

> For some months now there has been a series of news reports and congressional testimony dismissing the threat of Echelon coupled with declarations on the NSA's diminished capabilities to cope with technologies of the digital era. The essentials of these reports and testimony are almost identical, as with the report [referring to the *Register* story citing the unidentified U.S. government official]. Customarily, a charge is made that Echelon is a confabulation of journalism without credible bases, and that NSA could not perform the surveillance feats alleged. Cryptome first heard such dismissive accounts in 1998 . . . . We welcome for publication here reports on what could be seen as a sustained disinformation campaign about Echelon and NSA technological prowess.

82. SINGH, *supra* note 72, at 309 (describing the portrayal of the NSA in *Enemy of the State* and *Mercury Rising*); Richelson, *supra* note 11 ("It is possible that some of the reporting and oratory concerning Echelon may be as over-the-top as these films, in which NSA officials . . . casually authorize murder, even of small children.").

83. In *Enemy of the State* (Touchstone Pictures 1998), the NSA successfully plots to assassinate a politician who supports a bill in favor of strong encryption. SINGH, *supra* note 72, at 309. *Mercury Rising* (Universal Pictures 1998) is the story of the NSA's attempts to assassinate a nine-year-old autistic savant who inadvertently deciphered a supposedly unbreakable NSA cipher. *Id.*

84. Congressman Sanford Bishop Jr., a Democrat from Georgia, was quoted in 1999 as saying that although the NSA is facing "tremendous challenges coping with the explosive development of commercial communications and computer technology . . . [the NSA] has not demonstrated much prowess in coping with the challenge." Richelson, *supra* note 11. The House Permanent Select Committee on Intelligence (HPSCI) said that as a result of process and

panding use of fiber-optic cables,[85] the increased sophistication of encryption,[86] and the recent explosion in the volume in communications as the three factors that have severely impacted the NSA's ability to collect and analyze communications.[87] The difficulty that recent technological advancement poses to agencies such as the NSA was alluded to by John Millis, Staff Director of the House Permanent Select Committee on Intelligence (HPSCI), when he said in 1998 that "[s]ignals intelligence is in a crisis . . . . In the past four or five years technology has moved from being the friend to being the enemy of SIGINT."[88] All of this leaves the NSA in the awkward position of being accused of being both incompetent and omnipotent. NSA Director Lt. General Michael Hayden explained this difficulty when he griped in an interview, "One criticism is that we're omniscient and reading everybody's e-mail, and the other is that we're going blind and deaf. . . . It can't be both."[89]

D. The Controversy

The story of ECHELON first broke in August 1988, when Margaret Newsham, an NSA contract employee working at Menwith Hill, participated in an anonymous interview with English investigative reporter Duncan Campbell.[90] Ms. Newsham claimed to have managed a number of SIGINT databases, including the ground processing system for the MERCURY COMINT satellites, and was apparently disillusioned by what she perceived as corruption, fraud, and abuse in

---

management problems, "[t]he committee believes that NSA is in serious trouble." *Id.* For one of the more comprehensive criticisms of the current state of the NSA, see generally Seymour Hersh, *The Intelligence Gap*, THE NEW YORKER, Dec. 6, 1999.

85. It is harder to intercept signals transmitted over fiber-optic cable than it is to intercept those transmitted via satellite, microwave, or copper wire. Unlike the other forms of communication, fiber-optic cables do not "leak" signals which can be intercepted. *See* Campbell *supra* note 2 ("Optical fibre cables, however, do not leak radio frequency signals and cannot be tapped using inductive loops. NSA and other Comint agencies have spent a great deal of money on research into tapping optical fibres, reportedly with little success.").

86. For a discussion of the way encryption complicates COMINT collection, see *supra* notes 72-78 and accompanying text.

87. Richelson, *supra* note 11.

88. *Id.* (quoting comments delivered to a CIA Retirees Association on October 5, 1998).

89. Bryan Bender, *US National Security Agency Faces Data Deluge, Says Chief*, JANE'S DEFENCE WEEKLY, Mar. 22, 2000.

90. Duncan Campbell, *Making History: The Original Source for the 1988 First Echelon Report Steps Forward* (Feb. 25, 2000), *at* http://cryptome.org/echelon-mndc.htm (on file with the *Duke Law Journal*). This interview produced one of the first articles written about ECHELON, which was published in the British political weekly, *New Statesman*, on August 12, 1988. *Id.*

the operation of these systems.[91] Ms. Newsham's strangest claim is to have witnessed firsthand the real-time interception of a telephone call made by United States Senator Strom Thurmond.[92] In early 1988 she had passed this information on to the House Permanent Select Committee on Intelligence but no action was taken.[93] The media was apparently uninterested in Ms. Newsham's allegations as there was very limited coverage of the story.[94]

Throughout the 1990s Mr. Campbell and a few other reporters and academics continued to investigate the allegations made by Ms. Newsham. In January 1998, the ECHELON question was revived when the Scientific and Technological Options Assessment (STOA) committee of the European Parliament released the results of an independent investigation it commissioned that indicated that the United States routinely intercepts communication around the world but especially in the European Union.[95] This report prompted the European Parliament's Committee on Civil Liberties and Internal Affairs[96] to request that STOA prepare a follow-up study entitled *Development of Surveillance Technology and Risk of Political Abuse of Economic Information*. This study actually consists of five separate studies prepared by five different authors on subject matters related to electronic surveillance. One of these studies was prepared by ECHELON researcher Duncan Campbell and entitled *Intelligence Capabilities 2000*. This report provided a thorough overview of the technology used in UKUSA COMINT programs and alleged that the United States had been using this intelligence-gathering system to its benefit in trade negotiations and to assist American businesses competing for contracts with European firms.[97] These inflammatory accu-

---

91. *Id.*

92. *Id.*

93. *Id.*

94. *Id.* ("Back in 1988, however, the US and world press was uninterested in her reports, and did not cover Peg Newsham's revelations. ABC News interviewed her for television in 1992, but editors at that network chose not to broadcast the report.").

95. *An Appraisal of the Technologies of Political Control*, § 2.4.1 (1998), The Omega Foundation, http://www.europarl.eu.int/stoa/publi/166499/execsum_en.htm (on file with the *Duke Law Journal*).

96. In July 1999, the name of the committee was changed to the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs. Peggy Becker, Presentation and Analysis (Oct. 1999) (volume one in the five-volume report "Development of Surveillance Technology and Risk of Political Abuse of Economic Information," a working document for the Scientific and Technological Options Assessment Panel of the European Commission), European Parliament Scientific and Technological Options Assessment, http://216.167.120.50/dst-pa.htm (working document, on file with the *Duke Law Journal*).

97. *Id.*

sations propelled the ECHELON story onto the front pages of the European press.[98] The French government seemed particularly incensed that the United States might be using its national intelligence assets to further economic interests and launched an independent investigation into the ECHELON allegations.[99] In July of 2000, the European Parliament appointed a thirty-six-member committee that will spend a year investigating ECHELON further.[100]

This negative attention from Europe, and the allegations concerning the illegal interception of the communications of Americans, caught the attention of the United States. Representative Bob Barr and Representative Porter Goss, Chairman of HPSCI, began to investigate the allegations made in connection with ECHELON and became frustrated with the lack of information provided to them by the NSA and the CIA. As part of these investigations, HPSCI requested documents, including legal memoranda from the office of general counsel, concerning the NSA's operating restrictions on intelligence-gathering systems such as ECHELON that may intercept the communications of innocent Americans. In an unusual twist of events, NSA officials refused to disclose these documents to the congressional oversight committee on the grounds of attorney-client privilege.[101] The HPSCI Report on the Intelligence Authorization Act for Fiscal Year 2000 included the "additional views" of Chairman Goss. Goss expressed concern that the committee had been unsuccessful in obtaining, "legal memoranda, opinions rendered, and other docu-

---

98. David Ruppe, *Big Ears and Big Secrets*, *at* http://abcnews.go.com/sections/world/DailyNews/Echelon_990709.html (July 7, 1999) (on file with the *Duke Law Journal*).

99. Daley, *French Prosecutor*, *supra* note 3, at A9:

> [The] fear that America's vast surveillance system, developed in the cold war, is being used to further America's economic interests . . . continues to arouse passions [in Europe]. That is particularly true in France, where even Justice Minister Elisabeth Guigou contended in February that cold war spy systems had been converted to "economic espionage."

The French investigation, ordered by prosecutor Jean-Pierre Dintilhac, is apparently a preliminary investigation to determine if further legal action is warranted, although it is unclear what legal recourse a French prosecutor could have against the NSA. *Id.* Mr. Dintilhac has stated that he believes the ECHELON system should be dismantled or that Europe should have a hand in governing it. *Id.* Neither of these two options seems especially likely to occur. Ironically, the French government is alleged to operate its own ECHELON-like surveillance system to eavesdrop on private and public communications. *Id.* This program has been given the nickname "Frenchelon." *Id.*

100. Steve Kettmann, *U.S. Eyes Europe's Echelon Probe*, WIRED NEWS (July 6, 2000), *at* http://www.wired.com/news/politics/0,1283,37411,00.html (on file with the *Duke Law Journal*).

101. *United States Congressional Action*, *at* http://www.aclu.org/echelonwatch/congress.html (last visited Feb. 21, 2001) (on file with the *Duke Law Journal*).

ments in the General Counsel's Office" addressing the question of whether the "NSA was carrying out its signals intelligence mission in consonance with the law, relevant executive orders, guidelines, and policy directives."[102]

As a result of this apparent stonewalling, the House of Representatives added an amendment to the annual intelligence budget authorization bill that required the Director of the CIA, the Director of the NSA, and the Attorney General to provide a detailed explanation of the legal standards employed in monitoring the communications of American citizens.[103] The House amendment also required the agencies to provide the oversight committees with copies of all legal memoranda, opinions, and other documents prepared by their offices of general counsel that were relevant to the conduct of signals intelligence.[104] The final version of the amendment that emerged from conference and eventually became law required the presentation of a

---

102. H.R. REP. NO. 106-130, pt. 1, at 35 (1999).

103. House Version of Intelligence Authorization Act for Fiscal Year 2000, § 307, http://www.aclu.org/echelonwatch/hr1555h.htm (last visited Feb. 21, 2001) (on file with the *Duke Law Journal*). The amendment specifically requested:

> (a) REPORT—Not later than 60 days after the date of the enactment of this Act, the Director of Central Intelligence, the Director of the National Security Agency, and the Attorney General shall jointly prepare, and the Director of the National Security Agency shall submit to the appropriate congressional committees a report in classified and unclassified form describing the legal standards employed by elements of the intelligence community in conducting signals intelligence activities, including electronic surveillance.
>
> (b) MATTERS SPECIFICALLY ADDRESSED—The report shall specifically include a statement of each of the following legal standards:
>
> > (1) The legal standards for interception of communications when such interception may result in the acquisition of information from a communication to or from United States persons.
> >
> > (2) The legal standards for intentional targeting of the communications to or from United States persons.
> >
> > (3) The legal standards for receipt from non–United States sources of information pertaining to communications to or from United States persons.
> >
> > (4) The legal standards for dissemination of information acquired through the interception of the communications to or from United States persons.

Id.

104. The documents specifically requested were:

> (c) INCLUSION OF LEGAL MEMORANDA AND OPINIONS—The report under subsection (a) shall include a copy of all legal memoranda, opinions, and other related documents in unclassified, and if necessary, classified form with respect to the conduct of signals intelligence activities, including electronic surveillance by elements of the intelligence community, utilized by the Office of the General Counsel of the National Security Agency, by the Office of General Counsel of the Central Intelligence Agency, or by the Office of Intelligence Policy Review of the Department of Justice, in preparation of the report.

Id.

written report to the committee but dropped the requirement that the various legal documents used in the preparation of that document also be turned over to the committee.[105] The document prepared by the CIA, the NSA, and the Department of Justice, entitled *Legal Standards for the Intelligence Community in Conducting Electronic Surveillance*, was transmitted to Congress in February 2000.[106] This report did not specifically address ECHELON. The House Permanent Select Committee on Intelligence held hearings on this matter in April 2000 at which the Director of Central Intelligence, George Tenet, and the Director of the NSA, Michael Hayden, both staunchly denied the accusations raised in connection with ECHELON.[107] Following the hearings, Representative Barr said those statements created "more questions than answers" and left "[o]ur citizens . . . with a feeling of unease that is unhealthy both to our intelligence community as well as to our citizens themselves."[108] It remains to be seen whether additional hearings will be held and whether anything will come about as a result of them.

In addition to congressional efforts to investigate ECHELON, the Electronic Privacy Information Center (EPIC), a privacy advocacy group, began to pursue a Freedom of Information Act (FOIA) request in May 1999 centered on ECHELON and the alleged interception of Internet traffic. The NSA chose to ignore the request en-

---

105. Intelligence Authorization Act for Fiscal Year 2000, Pub. L. No. 106-120, § 309, 113 Stat. 1606, 1613. The final version contained the language quoted from the House version at *supra* note 103, but omitted the paragraph quoted at *supra* note 104.

106. *Legal Standards for the Intelligence Community in Conducting Electronic Surveillance* (Feb. 2000), Federation of American Scientists, http://www.fas.org/irp/nsa/standards.html (on file with the *Duke Law Journal*) [hereinafter *Legal Standards*].

107. Specifically, Mr. Tenet said:

> Mr. Chairman, I am here today to discuss allegations about SIGINT activities and the so-called Echelon program of the National Security Agency with a very specific objective: To assure this Committee, the Congress, and the American public that the United States Intelligence Community is unequivocally committed to conducting its activities in accordance with US law and due regard for the rights of Americans.

Tenet Statement, *supra* note 8; *see also Hearing Before the House Permanent Select Comm. on Intelligence*, 106th Cong. (Apr. 12, 2000) (statement of Michael V. Hayden, Lieutenant Director, National Security Agency), http://www.nsa.gov/releases/DIR_HPSCI_12APR.HTML (on file with the *Duke Law Journal*) [hereinafter Hayden Statement]:

> Recently, NSA has been the subject of media reports which suggest that NSA collects all electronic communications, spies on U.S. citizens, and provides intelligence information to U.S. companies. There also have been claims that NSA activities are not subject to regulation or oversight. All of these claims are false or misleading.

108. *ECHELON Hearing Leaves "More Questions Than Answers," at* http://www.aclu.org/echelonwatch/echwire3.htm (last visited Apr. 13, 2000) (on file with the *Duke Law Journal*).

tirely, as it sometimes does with especially sensitive issues, and allowed the twenty-day period in which it is statutorily required to respond to expire.[109] As permitted by FOIA, EPIC has continued to pursue the matter by filing a suit in the United States District Court for the District of Columbia in an attempt to compel the disclosure of the material.[110] EPIC has specifically requested "all 'legal memoranda, opinions rendered, and other documents in the General Counsel's Office' sought by the Select Committee and addressing the question of whether 'NSA was carrying out its signals intelligence mission in consonance with the law, relevant executive orders, guidelines, and policy directives.'"[111] In the fall of 2000, the NSA released over 100 documents to EPIC concerning the NSA's interpretation of the legal restraints on SIGINT activities.[112] In response to this action, EPIC voluntarily dismissed its suit.[113]

II. OVERVIEW OF LEGAL RESTRICTIONS

The successful collection of intelligence often requires violations of the law.[114] COMINT collection, in particular, frequently involves violating the target's privacy and trespassing on the systems that transmit information. While it is generally recognized that American intelligence activities must violate foreign laws to be effective, there is a clear distinction drawn between foreign and American laws; the former are frequently bent and broken, while the latter must be upheld at all costs.[115] It is these American laws, which all agree must be carefully followed, that will be surveyed in this part.

---

109. Electronic Privacy Info. Ctr. v. NSA, C.A. No. 99-3197 (D.D.C. Dec. 3, 1999), http://www.epic.org/open_gov/FOIA/nsa_comp.pdf (on file with the *Duke Law Journal*). The NSA actually provided an "initial response" to the EPIC request dated July 6, 1999, which stated that "[t]he material responsive to [the] request is not voluminous or complex" and that "[w]e anticipate providing a response to you by October 31, 1999." *Id.* at 3. No further communication was received from the NSA by EPIC. *Id.*

110. *Id.*

111. *Id*.

112. E-mail from David Sobel, General Counsel, Electronic Privacy Information Center, to Lawrence D. Sloan (Apr. 4, 2001) (on file with the *Duke Law Journal*). Some of these documents can be seen on EPIC's website at http://www.epic.org/privacy/nsa/documents.html. The author can be reached at lawrence.d.sloan.c98@alumni.upenn.edu.

113. E-mail from David Sobel, *supra* note 112.

114. Roger D. Scott, *Territorially Intrusive Intelligence Collection and International Law*, 46 A.F. L. REV. 217, 217-18 ("[S]urreptitious intelligence collection in another nation's territory probably violates the target nation's domestic law just as espionage against the United States violates United States domestic law.").

115. *Id.* at 218 ("However, the fact spying on other countries violates their law is far different from the assertion that the activity itself is illegal, as if some skulking shame of criminality

The American legal regime regulating COMINT activities is an interconnected series of constitutional provisions, federal statutes, executive orders, and agency guidelines that have been put into place in order to strike a compromise that adequately balances protection of our national interests and the protection of civil liberties.[116] This part will first address the Fourth Amendment of the Constitution, the most fundamental right implicated by COMINT collection activities. The evolving judicial attitude towards the relationship between electronic surveillance and the Fourth Amendment will be tracked. This discussion will then turn to the Foreign Intelligence Surveillance Act (FISA),[117] a statutory framework for ensuring that intelligence agencies follow procedures sufficient to protect the Fourth Amendment rights of the subjects of electronic surveillance conducted in the United States for national security purposes. FISA is a complicated statute, but an overview of its operation and salient features will be provided. This part will then turn to Executive Order 12,333,[118] promulgated by President Reagan in 1981. This executive order provides the general framework for the conduct of intelligence activities by agencies of the United States government. Of particular importance for this Note will be the specific provisions of Executive Order 12,333 that deal with electronic surveillance. To insure compliance with the dictates of the Fourth Amendment, FISA, and Executive Order 12,333, the agencies involved in SIGINT activities, primarily the Department of Defense (DoD), and the NSA, one of its constituent agencies, have implemented policies to provide their employees with guidance on how to conduct electronic surveillance activities. These will be briefly surveyed in this part.[119]

---

were attached to the enterprise. Our spies are patriots."). It is more than a coincidence that Executive Order 12,333, which provides overall guidelines for the conduct of intelligence-gathering activities, neglects to state that foreign laws should be obeyed in the collection of intelligence. Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 8, 1981) ("All means, consistent with applicable United States law and this Order, and with full consideration of the rights of United States persons, shall be used to develop intelligence information for the President and the National Security Council.").

116. For additional discussion of this balance between national security and personal liberty, see *supra* note 7 and accompanying text.

117. 50 U.S.C. §§ 1801-1811 (1994).

118. Exec. Order No. 12,333, 3 C.F.R. 200 (1982), *reprinted in* 50 U.S.C. § 401 (1994).

119. This Note does not address the separate issue of whether COMINT activities violate any provisions of international law. One observer has asserted that COMINT activities are consistent with international law. Scott, *supra* note 114, at 217:

> The United States is not a party to any treaty or agreement that prohibits surreptitious, nondestructive intelligence collection. Such intelligence collection also does not violate customary international law. In fact, customary international law has evolved

A. The Fourth Amendment

The Fourth Amendment of the Constitution is the most fundamental limitation on SIGINT activities that implicate United States persons. The Fourth Amendment 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.[120]

The Fourth Amendment applies to all searches by the federal government, including those conducted to obtain foreign intelligence.[121] Academics have parsed the Fourth Amendment into the Warrant Clause and the Reasonableness Clause.[122] Unlike the Reasonableness Clause, the Warrant Clause does not apply to all searches.[123] Courts have recognized judicially created exceptions to the Fourth Amendment's Warrant Clause.[124] Examples of these situations include searches incident to arrest,[125] searches of people entering and leaving the country,[126] and searches of closed containers in automobiles that have been lawfully stopped.[127] The executive branch has consistently taken the position that foreign intelligence searches constitute another exception to the warrant requirement.[128] Courts have generally accepted this exception in cases involving electronic surveillance.[129]

---

such that spying has become the long-standing practice of nations. Indeed, while the surreptitious penetration of another nation's territory to collect intelligence in peacetime potentially conflicts with the customary principle of territorial integrity, international law does not specifically prohibit espionage.

120. U.S. CONST. amend. IV.

121. Brown & Cinquegrana, *supra* note 27, at 107.

122. *Id.* at 107.

123. *Id.*

124. *Id.*

125. United States v. Robinson, 414 U.S. 218, 235 (1973).

126. United States v. Ramsey, 431 U.S. 606, 616-17 (1977).

127. United States v. Ross, 456 U.S. 798, 823-24 (1982).

128. Brown & Cinquegrana, *supra* note 27, at 108.

129. It is less clear whether the exception applies to physical searches for national security purposes. *Id.* (arguing that "there is no reasonable basis for excluding physical searches, as distinguished from electronic surveillance, from the scope of this [warrantless foreign intelligence] exception"); David S. Eggert, Note, *Executive Order 12,333: An Assessment of the Validity of Warrantless National Security Searches*, 1983 DUKE L.J. 611, 613 ("[S]uch an exception cannot be constitutionally justified. Alternatively . . . the legislative history of the Foreign Intelligence Surveillance Act and other congressional proceedings reveal that Congress has preempted any

The development of the national security exception from the Warrant Clause of the Fourth Amendment for electronic surveillance began with the 1928 case of *Olmstead v. United States*.[130] In *Olmstead*, the Supreme Court held that electronic surveillance was not covered by the Fourth Amendment, concluding that the Fourth Amendment only protects against trespassory searches and seizures.[131] This was far broader than the national security exception that would be developed later, as it exempted all forms of nontrespassory electronic surveillance from the warrant requirement, not just surveillance to further national security interests. Anticipating the power of electronic surveillance, Justice Brandeis entered a powerful dissent urging that the personal rights of security and privacy protected by the Fourth Amendment were implicated by electronic surveillance and therefore restrictions on such surveillance should be included in the Fourth Amendment.[132]

In 1967, in *Katz v. United States*,[133] the Supreme Court reversed its previous position and held that the Fourth Amendment was applicable to nontrespassory electronic surveillance.[134] According to the Court, the protections of the Fourth Amendment not only applied to specific places but also to people and their reasonable expectations of privacy.[135] The *Katz* Court, however, specifically reserved judgment on whether a warrant should be required to conduct electronic surveillance for national security purposes.[136]

The unresolved question of warrantless electronic surveillance for national security purposes was addressed in the 1972 case of *United States v. United States District Court*,[137] generally referred to as the *Keith* case. *Keith* specifically held that prior judicial approval was required before the conduct of electronic surveillance in a domestic terrorism case.[138] More importantly, the Court invited Congress to

claimed presidential prerogative to conduct warrantless foreign intelligence surveillance.").

130. 277 U.S. 438 (1928).

131. *Id.* at 464-66.

132. *Id.* at 474-75 (Brandeis, J., dissenting) ("[E]very unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.").

133. 389 U.S. 347 (1967).

134. *Id.* at 347.

135. *Id.* at 351.

136. *Id.* at 358 n.23 ("Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case.").

137. 407 U.S. 297 (1972).

138. *Id.* at 324.

pass legislation establishing "reasonable standards" for the conduct of electronic surveillance in national security cases.[139]

B. The Foreign Intelligence Surveillance Act

Congress responded five years after *Keith* by passing the Foreign Intelligence Surveillance Act of 1978 (FISA),[140] a statutory regime constructed to regulate electronic surveillance occurring in the United States for foreign intelligence purposes. Prior to the enactment of FISA, congressional regulation of electronic surveillance was limited to Title III of the Omnibus Crime Control and Safe Streets Act.[141] This legislation created a statutory framework under which judicial warrants were required for electronic surveillance used for criminal law enforcement purposes. When Title III was enacted, a decade before the passage of FISA, Congress specifically disclaimed any intention to infringe upon the authority of the executive branch to use warrantless electronic surveillance for foreign intelligence purposes.[142]

The executive branch has historically asserted that it has the inherent authority to conduct warrantless electronic surveillance to protect national security.[143] It is claimed that this inherent authority derives from the President's constitutional mandate found in Article II to "preserve, protect and defend the Constitution of the United

---

139. *Id.*

140. Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended at 18 U.S.C. §§ 2511, 2518-2520, 47 U.S.C. §§ 605-606, 50 U.S.C. §§ 1801-1811 (1994)).

141. Pub. L. No. 90-351, §§ 801-804, 82 Stat. 211-25 (1968) (codified as amended at 18 U.S.C. §§ 2510-2520, 47 U.S.C. § 605 (1994)).

142. Title III of the Omnibus Act specifically stated:

> Nothing in this chapter or in section 605 of the Communications Act of 1934 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 or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government. The contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial, hearing, or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power.

Id. § 802 (codified at 18 U.S.C. § 2511(3)), *repealed by* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 201(c), 92 Stat. 1783, 1797 (1978).

143. Franklin D. Roosevelt was the first President to use this inherent authority argument to justify warrantless surveillance. Dawson, *supra* note 7, at 1382 n.11.

States."[144] FISA, which represents a compromise between Congress and the executive branch, provides for oversight of foreign intelligence electronic surveillance by all three branches of the government.[145] FISA has been described as "a very complex and difficult statute that reflects a multitude of compromises between the Executive, the Congress, and the various interest groups that influenced its development."[146] The provisions of FISA prescribe the mechanism and the procedural requirements for obtaining permission from the judiciary branch or the Attorney General to conduct electronic surveillance.[147] The electronic surveillance that FISA is intended to regulate is defined to include

> the interception of international communications to a target who is a United States person in the United States, wiretapping in the United States, interception of the microwave portions of telephone communications in the United States, and microphone, closed-circuit television, or other forms of electronic monitoring of activities in the United States, for the purpose of collecting foreign intelligence.[148]

All such surveillance carried out in the United States requires prior approval of the Foreign Intelligence Surveillance Court (FISC),

---

144. U.S. CONST. art. II, § 1, cl. 8. For more on the possible sources of presidential authority to conduct electronic surveillance, see generally Kent A. Jordan, Note, *The Extent of Independent Presidential Authority to Conduct Foreign Intelligence Activities*, 72 GEO. L.J. 1855, 1868 (1984).

145. Dawson, *supra* note 7, at 1382-83.

146. Brown & Cinquegrana, *supra* note 27, at 157.

147. *Id.*

148. *Id.* The exact definition of "electronic surveillance" used in FISA is:

> (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
>
> (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States;
>
> (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or
>
> (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

50 U.S.C. § 1801(f)(1) (1994).

a court consisting of seven United States district court judges appointed by the Chief Justice of the Supreme Court.[149] FISC proceedings are conducted in secret in a room within the Department of Justice building in Washington, D.C.[150] The proceedings before FISC are nonadversarial, and only the representative from the Department of Justice Office of Intelligence Policy and Review appears before the court.[151] The specific agency seeking to conduct the surveillance, usually the NSA or the FBI, must coordinate with and seek approval from the Attorney General, and it is his representative who presents the application to FISC.[152] For obvious reasons, the target of the intended surveillance is not notified of the proceeding nor represented by counsel.[153] There is also a three-member appellate court that in theory allows the government to appeal a rejection of an application for electronic surveillance by FISC.[154] In practice, the government has little reason to resort to the appellate court: during the period of 1978 through 1999, FISC approved 11,883 applications and denied none.[155]

---

149. STEPHEN DYCUS ET AL., NATIONAL SECURITY LAW 662 (2d ed. 1997).

150. Gerald H. Robinson, *We're Listening! Electronic Eavesdropping, FISA, and the Secret Court*, 36 WILLAMETTE L. REV. 51, 61 (2000) ("They [FISC judges] sit in a cipher-locked, windowless, secure room on the top floor of the Department of Justice.").

151. *Id.* at 62; *see also Office of Intelligence Policy and Review*, http://www.usdoj.gov/oipr (last visited Jan. 31, 2001) (on file with the *Duke Law Journal*):

> The Office [of Intelligence Policy and Review] prepares and files all applications for electronic surveillance and physical search under the Foreign Intelligence Surveillance Act of 1978, assists Government agencies by providing legal advice on matters of national security law and policy . . . . The Office serves as adviser to the Attorney General and various client agencies, including the Central Intelligence Agency, the Federal Bureau of Investigation, and the Defense and State Departments, concerning questions of law, regulation, and guidelines as well as the legality of domestic and overseas intelligence operations.

152. Robinson, *supra* note 150, at 62.

153. *Id*.

154. *Id*. If this appellate court upholds the FISC denial of a warrant, the government may apply for a writ of certiorari to the Supreme Court. *Id.*

155. *Id.*; *1998 Annual Foreign Intelligence Surveillance Act* (n.d.) (reporting that 796 applications for orders or extensions of orders approving electronic surveillance were received and granted by FISC in 1998), http://www.usdoj.gov/04foia/readingrooms/98fisa_ltr.html (last visited Feb. 13, 2001) (on file with the *Duke Law Journal*); *1999 Annual Foreign Intelligence Surveillance Act* (n.d.) (reporting that 886 applications for orders or extensions of orders approving surveillance were received and granted by FISC in 1999), http://www.usdoj.gov/04foia/readingrooms/99fisa-ltr.html (last visited Feb. 13, 2001) (on file with the *Duke Law Journal*). Critics of FISC often cite the former statistic as support for their allegation that FISC serves only as a rubber stamp for the government to add legitimacy to its surveillance activity. *See generally* Philip Colangelo, *The Secret FISA Court: Rubber Stamping on Rights*, COVERT ACTION Q., Jan. 23, 2001, http://mediafilter.org/caq/Caq53.court.html (on file with the *Duke Law Journal*). Those less inclined to see government conspiracies respond to this by arguing that the low rejection rate can be attributed to the Department of Justice being aware of the standards FISC will apply and eliminating those applications which do not meet the required guidelines.

The burden of proof that must be met by agencies submitting an application for surveillance to FISC varies depending on the nature of the subject of the surveillance.[156] All applications must certify that there is probable cause that the target of the proposed surveillance is either a foreign power[157] or an agent of a foreign power,[158] as those terms are defined by FISA. For non–"United States persons"[159] it

156. *Legal Standards*, *supra* note 106.

157. FISA defines "foreign power" to mean:

> (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 therefor;
>
> (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.

50 U.S.C. § 1801(a) (1994).

158. FISA defines "agent of a foreign power" to mean:

> (1) any person other than a United States person, who—
>
> > (A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section;
> >
> > (B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or
>
> (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 statues 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 power; or
> >
> > (E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

50 U.S.C. § 1801(b) (1994 & Supp. 2000).

159. "United States person" is defined in FISA as "a citizen of the United States, 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 perma-

must be shown that the information "to be acquired is merely *related* to the national defense or security of the United States o[r] the conduct of foreign affairs."[160] When a United States person is the intended subject of the surveillance, a higher standard is imposed, and the application must show that "the acquisition of such information is *necessary* to national defense or security or the conduct of foreign affairs."[161] The FISA procedures are only to be used in cases involving foreign intelligence information and are completely independent of the procedures adopted by Congress to regulate the use of electronic surveillance in all other criminal matters.

C. Executive Order 12,333

The next significant development in the law governing electronic surveillance in support of intelligence activities was Executive Order 12,333, issued by President Ronald Reagan in 1981. Executive Order 12,333 was designed to clarify the overall framework under which United States intelligence agencies should conduct foreign intelligence activities. Executive Order 12,333 outlines each member of the intelligence community's responsibilities and sets out rules governing the means by which these duties are to be fulfilled. This executive order places responsibility for signals intelligence solely with the NSA.[162] It provides:

> Collection of . . . information [about the capabilities, intentions and activities of foreign powers, organizations, or persons and their agents] is a priority objective and will be pursued in a vigorous, innovative and responsible manner that is consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded."[163]

The executive order was intended to provide the framework for an intelligence-gathering apparatus that "achieve[s] the proper balance between the acquisition of essential information and protection of individual interests."[164]

---

nent residence, or a corporation which is incorporated in the United States." *Id.* § 1801(i).

160. *Legal Standards*, *supra* note 106.

161. *Id*.

162. Exec. Order No. 12,333 § 1.12(b), 3 C.F.R. 200 (1982), *reprinted in* 50 U.S.C. § 401 (1994) ("No other department or agency [other than NSA] may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense.").

163. *Id.* § 2.1.

164. *Id.* § 2.2.

With respect to electronic surveillance, Executive Order 12,333 provides limited specific guidance. Section 2.4, which addresses collection techniques, provides:

> Agencies within the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Agencies are not authorized to use such techniques as electronic surveillance . . . unless they are in accordance with procedures established by the head of the agency concerned and approved by the Attorney General.[165]

In addition to approving the procedures to be implemented by the various agencies, the Attorney General is delegated the power to approve surveillance directed against United States persons abroad. The Attorney General is directed by Executive Order 12,333 to only approve such surveillance if he has determined that there is probable cause to believe that the target is acting as a foreign power or an agent of a foreign power.[166] FISA is explicitly recognized by Executive Order 12,333, which states that "[e]lectronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978, shall be conducted in accordance with that Act, as well as this Order."[167] Because FISA imposes more comprehensive restrictions than Executive Order 12,333, when the surveillance is to occur in the United States, compliance with FISA is the primary concern.

---

165. *Id.* § 2.4. Executive Order 12,333 defines "United States person" as

> a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

Id. § 3.4(i). This definition is identical to the definition of U.S. person quoted from FISA. *See supra* note 159.

166. Exec. Order No. 12,333 § 2.5, 3 C.F.R. 200 (1982).

> The Attorney General hereby is delegated the power to approve the use for intelligence purposes . . . against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probably cause to believe that the technique is directed against a foreign power or an agent of a foreign power.

The terms "foreign power" and "agent of a foreign power" are not defined in Executive Order 12,333. It is safe to assume that the Attorney General considers the definitions of these terms found in FISA when determining if the dictates of Executive Order 12,333 have been met. For FISA's definition of these terms, see *supra* notes 157-58.

167. *Id.*

D. Agency Guidelines

Executive Order 12,333 binds executive agencies by prohibiting the collection, retention, or dissemination of information about United States persons except in accordance with procedures promulgated by the agency head and approved by the Attorney General.[168] All of the intelligence agencies have produced such procedures, which have been approved by the Attorney General, and it is these procedures that form the final piece of the legal regime surrounding signals intelligence collection.[169] Department of Defense Directive 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons*, dated December 1982, governs all DoD components, including the NSA. These guidelines provide guidance concerning all forms of surveillance, including physical and electronic surveillance. There is a classified appendix to this document that is particularized for the NSA, nominally a component of the Department of Defense.[170] The NSA also has an internal directive, United States Signal Intelligence Directive (USSID) 18, which provides specific operational guidelines to that agency.[171] USSID 18 was previously classified SECRET, and, although a majority of it has been declassified, significant amounts have been redacted.[172] These documents provide instructions on how employees of NSA can collect, process, store, and disseminate the communications of United States citizens while conforming their activities to the restrictions imposed by the Constitution, Executive Order 12,333 and FISA. Much of the language in these instructions is similar to that found in Executive Order 12,333, and FISA.

The overall result of the interaction between the Fourth Amendment, FISA, Executive Order 12,333, and the agency guidelines is that the procedures to be followed when conducting electronic surveillance vary depending upon the identity of the target and his geographic location. All electronic surveillance that takes place in the

168. *Legal Standards*, *supra* note 106.

169. *Id.*

170. *Id.* For obvious reasons, the author did not have access to this document.

171. *United States Signal Intelligence Directive (USSID) 18* (Oct. 20, 1980), http://cryptome.org/nsa-ussid18.htm (on file with the *Duke Law Journal*) [hereinafter *USSID 18*].

172. Twelve lines of text were redacted from the section addressing collection; fifty-eight lines from the section addressing processing of signals; sixteen lines from the section addressing storage of information; twenty-five lines addressing the dissemination of information collected; and 105 lines addressing the responsibilities of various parties tasked with ensuring compliance with USSID 18. *Id.*

United States must be conducted in accordance with FISA, whose primary requirement is prior judicial authorization from FISC. However, when the surveillance occurs outside of the United States, FISA is not applicable, and there is no requirement of prior judicial authorization. In these cases, Executive Order 12,333 is the primary source of regulation. Executive Order 12,333 specifies different procedures to be followed depending on whether the subject is a United States person or not. If the subject is a United States person, as that term is defined in Executive Order 12,333, then the Attorney General, upon a finding that there is probable cause to believe that the target is a foreign power or an agent of a foreign power, has the power to authorize the collection.[173] If, however, the surveillance is to occur outside of the United States, and there are no United States persons implicated, then no prior approval from FISC or the Attorney General is necessary. In these situations, Executive Order 12,333 requires only that the surveillance be conducted in accordance with procedures established by the head of the agency concerned.[174]

III. PROBLEMS WITH THE CURRENT LEGAL REGIME

Though there seems to be a comprehensive set of regulations governing SIGINT activities, these regulations have not been updated sufficiently to account for the technological changes that have fundamentally altered the nature of the SIGINT-gathering business.[175] As alluded to previously, Congress has created different legal regimes to regulate electronic surveillance used in ordinary criminal and foreign intelligence cases. The criminal wiretap laws were updated in the 1980s with the Electronic Communications Privacy Act of 1986[176] and in the 1990s with the Communications Assistance for Law Enforcement Act,[177] but the laws and regulations governing foreign intelli-

173. Exec. Order No. 12,333 § 2.5, 3 C.F.R. 200 (1982), *reprinted in* 50 U.S.C. § 401 (1994).

174. *Id.* § 2.4.

175. The following discussion assumes that the description of the legal regime described *infra* Part II is complete and comprehensive. A possibility exists that other documents that are not yet publicly available provide further guidance to intelligence agencies on the conduct of electronic surveillance. This discussion is thus premised solely on the publicly available information.

176. 18 U.S.C. § 2510 (1994).

177. 47 U.S.C. § 1001 (1994). The legal regime concerning electronic surveillance in connection with criminal investigations is by no means perfect. For example, the Cable Act of 1984 sets a more difficult burden for government agents to satisfy when monitoring computers using cable modems than for computers using telephone-line connections. Labaton & Richtel, *supra* note 49. Such a differentiation is inexplicable as telephone and cable lines are capable of carrying the same high-speed Internet traffic. In the final days of its term, the Clinton administration pro-

gence surveillance have not been kept similarly current. United States Signal Intelligence Directive 18 was promulgated in October 1980, while the Department of Defense *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons* has not been modified since December 1982. Similarly, Executive Order 12,333 has not been updated or superceded since it was signed by President Reagan on December 4, 1981. FISA has been periodically updated to reflect minor changes, but its basic framework has remained unchanged since it was enacted in 1978.[178]

This part will consider three examples of concepts in the regulations that have become obsolete or inappropriate as a result of recent technological innovation. The first concept discussed will be "incidentally acquired information," which allows the intelligence community to retain and distribute information about United States persons who it might otherwise be prohibited from collecting against, provided that the information was collected incidentally to legally authorized collection activities. The increased capability of the SIGINT community to collect and analyze signals creates the possibility that a large amount of intelligence about United States persons will be collected incidentally, thereby threatening to swallow the rule prohibiting collection against United States persons without strictly adhering to certain procedures. The second concept that will be discussed is minimization, which requires that SIGINT collection activities be conducted in the manner least likely to inadvertently collect information about United States persons. If the allegations concerning the volume of signals collected by the intelligence community are accurate, then the concept of minimization has become irrelevant. The third aspect of the legal regime that will be addressed is the requirement that the intelligence community ascertain whether the subject of collection is a United States person. This threshold determination must be made early in the process because it determines what action the intelligence community is permitted to take with respect to the information. The interconnectedness of various forms of communication and the greater anonymity conferred by modern technologies such as the

posed legislation that "'would harmonize the legal standards that apply to law enforcement's access to e-mails, telephone calls and cable services.'" *Id.* (quoting White House Chief of Staff John D. Podesta).

178. The most recent amendments to FISA occurred in late 1998, when it was amended to allow the use of "roving wiretaps," "pen registers," and "trap and trace" devices. Intelligence Authorization Act for 1999, Pub. L. No. 105-272, 112 Stat. 2396 (codified at 50 U.S.C. §§ 404I, 1841-1846, 1861-1863 (1994 & Supp. 2000)).

Internet make this determination more difficult, if not impossible, to make. These three areas are certainly not the only areas of the law that pose difficulties. However, they serve to highlight the nature of the problem, demonstrating that these laws and regulations need to be reevaluated to insure that they continue to effectively balance the civil liberties of the American people against the national security interests of the United States.

A. Incidentally Acquired Information

The concept of "incidentally obtained information" is one element of the legal regime that may no longer be appropriate in light of recent technological advances. Information incidentally obtained by the United States SIGINT community will be discussed first, followed by a discussion of the problems raised by the use of information incidentally obtained by our foreign partners. Section 2.3(i) of Executive Order 12,333 specifically authorizes the collection, retention, and dissemination of "incidentally obtained information that may indicate involvement in activities that may violate federal, state, local or foreign laws."[179] The exact language quoted from section 2.3(i) is included as one of the four situations in which the DoD procedures permit the retention of "information about United States persons collected incidentally to authorized collection."[180] This exception was originally designed as a means of ensuring that valuable information accidentally obtained in the course of legally authorized collection need not be disregarded. When viewed from this perspective, the exception seems perfectly logical. However, because the ECHELON system is believed to collect nearly all signals, almost every piece of communication will be "incidentally acquired" by the United States or one of its allies. The modern generation of communication satellites is reportedly capable of simultaneously transmitting 90,000 telephone calls.[181] A large volume of information flowing through the

179. Exec. Order No. 12,333 § 1.12(b), 3 C.F.R. 200 (1982), *reprinted in* 50 U.S.C. § 401 (1994).

180. Department of Defense, *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Person* (Dec. 1982), http://www.cryptome.org/dod5240-1.htm (on file with the *Duke Law Journal*). The other three situations in which incidentally obtained information about United States persons is permitted to be retained are: (1) when such information could have been collected intentionally under Procedure 2; (2) when such information is necessary to understand or assess foreign intelligence or counterintelligence; (3) when the information is foreign intelligence or counterintelligence collected from electronic surveillance conducted in compliance with this regulation. *Id.*

181. Campbell, *supra* note 2.

same signal increases the likelihood that incidental information will be collected. In addition, the fact that many different types of communications flow over the same media results in increased incidental interceptions unrelated to the target of surveillance. Modern communication satellites are capable of carrying various forms of communication, including television, telephone, and data. Governmental communications often travel over the same signals as private communications, creating a situation in which an innocent man's telephone call to his wife can be transmitted over the same signal as a report from the Chinese embassy to Beijing. Given these developments in the field of COMINT collection and communication technology, this exception for incidentally acquired information threatens to swallow the entire rule.

The exception for incidentally obtained information also raises questions in connection with information obtained by the United States's SIGINT partners. The intelligence community has taken the position that it may accept "incidentally acquired information about U.S. persons from foreign governments."[182] This is relevant to the recent allegations that the NSA uses its partners in ECHELON to collect otherwise prohibited information on United States persons. Section 2.12 of Executive Order 12,333 specifically provides that "[n]o agency of the Intelligence Community shall participate in or request any person to undertake activities forbidden by this Order."[183] Even if one gives the NSA the benefit of the doubt and assumes that it would not blatantly violate the law by requesting that our allies conduct surveillance on a prohibited target, one can see how the "incidentally acquired" exception could be used for subtle circumvention of the limitations on domestic activities. For instance, in order to curry favor with the NSA, one of its foreign partners might, on its own initiative, undertake surveillance of United States persons in whom it knows that the NSA would have an interest. It could then pass this information along to the NSA, which would be legally permitted to accept it as "incidentally acquired" information. Given the close working relationships between these nations and the nature of the ECHELON system, each country is likely aware of the intelligence targets of interest to other parties.

Other than general allegations, there does not appear to be any specific evidence to support claims of such behavior on the part of the

182. *Legal Standards*, *supra* note 106.
183. Exec. Order 12,333, 3 C.F.R. 2000.

NSA. This is not the case, however, for some of the NSA's ECHELON partners. A former Canadian CSE officer has publicly claimed to have been involved in the execution of such a scheme on behalf of the British government.[184] Mike Frost, the former Canadian spy, alleges that British Prime Minister Margaret Thatcher requested in February 1983 that two ministers of her government, whom she suspected of disloyalty, be surveilled electronically. It is alleged that, instead of complying with the legal difficulties associated with spying on British citizens, the British GCHQ liaison in Ottawa requested that the CSE conduct the three-week-long surveillance mission on behalf of GCHQ.[185] This anecdote of improper use of information, which could be classified as incidentally obtained, suggests that the entire concept needs to be reevaluated to ensure that what was intended to be a limited exception does not unnecessarily bypass the restrictions placed on the collection of information concerning United States persons.

B. Minimization

The second concept discussed here is minimization. The legal regime surrounding SIGINT activities continually reinforces the position that SIGINT operations should be conducted in the least intrusive manner and that the amount of information collected about United States persons should be minimized.[186] Section 2.4 of Executive Order 12,333 dictates that "[a]gencies within the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad."[187] Annex A to USSID 18 specifically provides that, "[c]ollection personnel will monitor the collection of raw data at regular intervals to verify that the surveillance is not avoidably acquiring communications of U.S. persons outside the authorized scope of the surveillance or information concerning U.S. persons not related to the purpose of the surveillance."[188] These were acceptable limita-

184. MIKE FROST & MICHEL GRATON, SPYWORLD: INSIDE THE CANADIAN AND AMERICAN INTELLIGENCE ESTABLISHMENTS 35 (1994) (describing the beginning of the officer's involvement in the scheme).

185. *Id.* at 33-44, 238.

186. *Legal Standards*, *supra* note 106 ("[A]ll foreign intelligence electronic surveillance must be conducted in a manner that minimizes the acquisition, retention, and dissemination of information about unconsenting U.S. persons.").

187. Exec. Order No. 12,333, § 2.4, 3 C.F.R. 2000.

188. *USSID 18*, *supra* note 171, at ann. A.

tions in an era in which targets were carefully chosen. However, in the context of a system that intercepts everything, these rules seem outmoded and meaningless.

The concept of minimization is indicative of the general incongruity between the way SIGINT was conducted when the relevant legal rules were implemented and the way it is conducted today. The legislation and regulations that call for minimization seem to be well-suited to an era in which SIGINT was a narrowly focused activity. The assumption underlying the entire legal regime is that the nature of the intercepted material can be carefully controlled. In the past it seems that specific targets (such as certain geographic locations or specific radio frequencies) were identified for surveillance, thereby limiting the potential for overreaching by the agencies involved.

While the SIGINT agencies still undoubtedly focus their efforts on certain carefully chosen targets, the ECHELON system is believed to be more of a catch-all system: it has been analogized to a vacuum cleaner that ingests nearly every signal on or around the globe. In effect, the vacuum cleaner approach does not discriminate and makes it very difficult to limit what is collected. The availability of automated data processing makes the vacuum cleaner approach feasible today. If ECHELON is a vacuum cleaner, the previous era of SIGINT collection can be likened to a person bending over to pick up specific pieces of debris from the floor.[189]

Additionally, these minimization rules were implemented during the Cold War, a time when our enemy was clearly identified. The primary threat to our national security was the Soviet Union, and, therefore, the SIGINT agencies were able to primarily focus their attention on targets associated with that threat. Today, the geopolitical situation in the world has been altered dramatically, and the nature of the threats to United States national security is not as clearly defined. The dragon has been slain, and a multiheaded hydra has emerged in

189. A similar analogy has been presented by Phil Zimmerman, creator of PGP encryption software, who stated:

> In the past, if the government wanted to violate the privacy of ordinary citizens, it had to expend a certain amount of effort to intercept and steam open and read paper mail, or listen to and possibly transcribe spoken telephone conversations. This is analogous to catching fish with a hook and a line, one fish at a time. . . . [T]his kind of labor-intensive monitoring is not practical on a large scale. Today, electronic mail is gradually replacing conventional paper mail . . . . Unlike paper mail, e-mail messages are just too easy to intercept and scan for interesting keywords. This can be done easily, routinely, automatically, and undetectably on a grand scale. This is analogous to driftnet fishing . . . .

SINGH, *supra* note 72, at 296 (quoting Phil Zimmerman).

its place. Today, the United States finds itself threatened by terrorist groups, rogue nations, narcotics smugglers, and the proliferation of weapons of mass destruction. These threats have been shown to emanate from a wide variety of groups and geographic areas. Prudence therefore dictates that our SIGINT net be cast wider. SIGINT collectors must not only focus on determining the intentions of the enemy, but now must also attempt to determine who might emerge as the next enemy. The necessity of casting a wider net is difficult to reconcile with the requirements of minimization. Due to technological and geopolitical realities, it is time to reconsider whether the concept of minimization has lost too much of the protective value its creators intended for it to provide to American citizens.

C. United States v. Non–United States Persons

The difficulty experienced in trying to limit the reach of SIGINT activities and minimize their impact on United States persons is a manifestation of the increasing difficulty in determining the identity of the parties to a communication and their country of origin. The legal regime governing SIGINT collection is premised on fundamental distinctions between domestic and foreign activities and between United States persons and foreign persons.

These distinctions have always been problematic. As Frank Raven, the 1960s-era Chief of NSA Group G (collection against Third World countries) stated,

> [Y]ou cannot divide your problems neatly and cleanly into internal U.S. and external U.S. . . . . You have intelligence which is entirely foreign and you have intelligence which is entirely domestic. But then you have the third category which no one will recognize, which is intelligence which moves back and forth between them.[190]

USSID 18 includes guidance for operating in this gray area. It provides a set of default rules to guide NSA employees in determining whether to treat a subject as a United States person when the identity of the subject or his geographic location remains unknown. For instance, a person who is known to be in the United States, but whose identity is unknown, will be treated as a United States person unless that person can be positively identified as an alien or the circumstances indicate that he is not a United States person.[191] On the con-

190. BAMFORD, *supra* note 1, at 364.
191. *See USSID 18*, *supra* note 171.

trary, a person known to be outside the United States or whose location is unknown will not be treated as a United States person unless that person can be positively identified as a United States person or the circumstances of the communication create a reasonable belief that the subject is a United States person.[192]

Unfortunately, recent technological advances have served to further complicate the process of identifying the nationality and location of the subject of surveillance. In the context of Internet traffic, it would seem to be more difficult than ever to determine whether the parties to a communication are United States persons.

The Internet allows subjects to conceal their identities and communicate anonymously. There are a number of free e-mail services, such as Hotmail, that allow a user to establish an e-mail account without providing any verification of their identity. Further complicating matters is the fact that services like Hotmail allow the owner of the account to receive and send their messages from any computer in the world that has an Internet connection. Therefore, the physical location of the server on which the account actually resides does not provide any insight into the location of the subject.

There are tools currently available that allow the average personal computer user to send and receive e-mail or browse the World Wide Web in an entirely untraceable manner. Anonymous remailers are services that mask the origin of an e-mail address by stripping off all identifying information and replacing it with an anonymous code number.[193] All one has to do is send his e-mail message to a free anonymous remailer, such as the one at the Massachusetts Institute of Technology's Laboratory for Computer Science, which then strips off the identifying information and resends it anonymously.[194] Anyone trying to trace the e-mail back to the sender would be unable to get beyond the anonymous remailer as these services generally have a policy of destroying the logs of their operations.[195] There are similar

192. *Id.* § 3.31(c)(2).

193. Steve Lohr, *Privacy on Internet Poses Legal Puzzle*, N.Y. TIMES, Apr. 19, 1999, at C4.

194. *Id.*

195. *Id.* Most sophisticated remailers, such as the one at MIT, route messages through a number of different anonymous remailers. *Id.* Therefore, even if one of the remailers failed to adequately destroy its logs, the sender would still remain anonymous as long as one of the remailers in the chain observed this security practice.

services, such as Anonymizer,[196] that allow for similarly anonymous viewing of Internet web pages.[197]

The decentralized nature of the Internet causes difficulty in determining the identity and location of those sending messages. Because messages are often routed through a number of different servers that are frequently located in different countries, it is difficult to work backwards from an intercepted message to determine its source. Philip Reitenger, a senior counsel in the Justice Department's Computer Crimes and Intellectual Property Division, complained that trying to trace the path of a criminal communication often requires cooperation with authorities in eight to twenty different nations.[198]

The locations and nationalities of participants in a communication are threshold determinations that must be made under the present legal regime and have a significant bearing on what courses of action are available to the intelligence agency. The default guidelines on this matter established by the NSA in USSID 18 prove problematic on two fronts. First, they create the potential for the NSA to overstep its bounds by collecting more than it is legally permitted to collect against a United States person traveling abroad, who, at the time he makes his communication, cannot be identified as a United States person. Second, the default rules also threaten to unnecessarily hamper the NSA's effective monitoring of foreign subjects in the United States who are mistakenly assumed to be United States persons. Neither of these results is desirable. Any future revision of the legal regime surrounding COMINT activities must be crafted to account for the unique problems posed by emerging technology such as the Internet.

CONCLUSION

Given all of the above criticism of the current legal regime governing SIGINT activities, one might think that the author is firmly in favor of further restricting the capabilities of American SIGINT organizations. This is not the case. The services provided by these organizations are essential to the national security of this nation. Although the intelligence community, especially the segment involved

196. *Privacy Is Your Right*, *at* http://www.anonymizer.com (last visited Feb. 25, 2001) (on file with the *Duke Law Journal*).

197. For a discussion of a number of technologies being developed to facilitate anonymous Internet usage, see Peter H. Lewis, *Internet Hide and Seek*, N.Y. TIMES, Apr. 8, 1999, at G1.

198. Lohr, *supra* note 193.

in SIGINT, is necessarily hesitant to trumpet its successes, there can be little doubt that the information gathered via SIGINT operations has saved the lives of numerous Americans both in the United States and abroad.[199] Systems such as 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. It is understandable that this may involve some invasion of the privacy of American persons, but this is a balance that must be maintained. While the prospect of occasionally having innocent e-mail messages screened by a NSA computer is troublesome, the prospect of inhaling sarin gas on the New York City subway system is far more alarming. Given our democratic form of government, this balance must be dictated by our elected officials, namely Congress and the President.

The shortcomings that were identified in this Note are surely only a few of the many ways in which the outdated rules have fallen behind new technology. The author does not agree with General Hayden when he says that the legal regime surrounding SIGINT "is technology neutral and does not require amendment to accommodate new communications technologies."[200] Addressing the changing technology and the new adversaries faced by the NSA, General Hayden has recognized a fundamental shift: "This is about an agency that's grown up in one world, learned a way to succeed within that world and now finds itself in another world, and it's got to change if it hopes to succeed in that world."[201] As the NSA struggles to remake itself in this new world, this author believes that it is equally important to ensure that the legal regime surrounding SIGINT collection similarly adapts. Congress and the President must both take steps to reevaluate the procedures in place to ensure the appropriate balance between national security and civil liberties continues to be struck in the face of the fundamental changes in communications technology.

---

199. Brown & Cinquegrana, *supra* note 27, at 103:

> Electronic surveillance authorized under FISA, for example, allowed the United States to break up the Walker spy ring and to frustrate the plans of an international terrorist group, the Armenian Secret Army for the Liberation of Armenia, to construct and detonate an explosive device at an Air Canada facility in California.

200. Hayden Statement, *supra* note 107.

201. *NSA Head: Tech Weakness Makes U.S. Vulnerable*, *at* http://www.cnn.com/2001/TECH/internet/02/12/usa.security.reut/index.html (Feb. 12, 2001) (on file with the *Duke Law Journal*).