

CRS Report for Congress

Received through the CRS Web

Project Echelon: U.S. Electronic Surveillance Efforts

Richard A. Best, Jr.
Specialist in National Defense
Foreign Affairs, Defense, and Trade Division

Summary

Last year Congress passed legislation (P.L. 106-120, Section 309) requiring that the Executive Branch report on the legal standards for electronic surveillance by U.S. intelligence agencies. This action followed press reports and European Parliament studies claiming that the National Security Agency (NSA) has established a world-wide signals collection effort, known as Project Echelon, that jeopardizes the privacy rights of individuals and unfairly provides commercial advantage to U.S. firms. There has been no official U.S. confirmation of the existence of Project Echelon, but the responsibilities of the National Security Agency (NSA) for signals intelligence (sigint) are widely known and reflected in statutory law and executive orders. Although there is no evidence that NSA has undertaken illegal sigint operations, some observers, in the U.S. as well as abroad, argue that electronic surveillance efforts, even if sanctioned by domestic laws, undercut universally guaranteed human rights. Others counter that a robust signals intelligence is essential to protect the Nation and its allies against hostile foreign governments, terrorists, and narcotics traffickers. This report will be updated as additional information becomes available.

Background

In recent months there have been a number of media reports that the National Security Agency (NSA) is involved in a worldwide effort, known as Project Echelon, designed to collect civilian communications throughout the world.¹ Working in agreement with sister intelligence agencies in the United Kingdom and other countries, NSA is said to have the capability to intercept and report virtually all communications—telephone, facsimile, and email—that might be of interest to federal agencies. A working document prepared for the Directorate General for Research of the European Parliament stated that

¹ See, for instance, Vernon Loeb, "Critics Questioning NSA Reading Habits," *Washington Post*, November 13, 1999, p. A3; James Bamford, "Loud and Clear: the most secret of secret agencies operates under outdated laws," *Washington Post*, November 14, 1999, p. B1; Jeffrey Richelson, "Desperately Seeking Signals," *Bulletin of Atomic Scientists*, March 2000.

“Within Europe, all email, telephone and fax communications are routinely intercepted by the United States National Security Agency, transferring all target information from the European mainland via the strategic hub of London then by Satellite to Fort Meade in Maryland via the crucial hub at Menwith Hill in the North York Moors of the UK.” The report referred to a “Project known as ECHELON” that “works by indiscriminately intercepting very large quantities of communications and then siphoning out what is valuable using artificial aids ... to find key words.”² Subsequent reports provide a more extensive technical discussion of NSA’s supposed capabilities.³ The reports cite various journalistic accounts as sources for their information.

It is worth noting that such European Parliament studies, known as Scientific and Technological Options Assessments (STOA), are prepared by outside specialists commissioned because of prior publications and expertise. The authors, who are not civil servants, do not have official access to the classified information of the member states. Moreover, the Parliament itself has not taken an official position on Echelon.

The various charges relating to Echelon are difficult to assess, given the sensitivities involved in intelligence programs generally and in regard to the work of NSA in particular. To a far greater extent than the Central Intelligence Agency (CIA), NSA is publicly reticent about its operations. Indeed, specific statutory restrictions apply to the disclosure of information regarding cryptanalytic processes.⁴ Nevertheless, government efforts to gather intelligence about foreign countries and hostile groups through signals intelligence efforts are widely known.

Statutory Authorities

NSA, which was established in 1952 by Presidential directive, has statutory responsibilities for signal designated in the National Security Act and an executive order (E.O. 12333) signed by President Reagan in 1981.⁵ A major employer in the state of Maryland, NSA currently has a much higher profile than was true in the past and its post-Cold War missions are widely discussed, albeit usually not publicly by responsible Government officials. NSA’s operations in the U.S. are covered by the Foreign Intelligence Surveillance Act (FISA) (P.L. 95-511) that was enacted in 1978, in part as a result of concern about electronic surveillance of U.S. persons undertaken by intelligence agencies without court authorization. (Law enforcement agencies regularly conduct wiretaps and other surveillance activities, but under different statutory authorities.) FISA

² European Parliament, Directorate General for Research, Scientific and Technological Options Assessment, *An Appraisal of Technologies of Political Control*, Working document, January 6, 1998, PE 166 499, p. 19. Links to the reports have been published on a private web-site, <http://cryptome.org/dst-1.htm>.

³ European Parliament, Directorate General for Research, Scientific and Technological Options Assessment, *Development of Surveillance Technology and Risk of Abuse of Economic Information*, Working document, April 1999, PE 168.184/Part3/4: *Intelligence Capabilities 2000*, by Duncan Campbell.

⁴ 47 USC 605; 18 USC 952.

⁵ 50 USC 403-5(b)(1); E.O.12333, Section 1.12(b). Administrative authorities for NSA are established in the National Security Agency Act of 1959 (P.L. 86-36).

establishes procedures by which electronic surveillance can be undertaken in the U.S. for foreign intelligence (as opposed to law enforcement) purposes. The Act includes specific provisions designed to preclude the improper use of electronic surveillance against U.S. persons. Some critics have suggested that such provisions could be evaded by requesting foreign intelligence agencies to provide information on U.S. persons; the NSA has, however, officially denied that such practice occurs, noting that it has been prohibited since 1978.⁶

Observers of intelligence efforts acknowledge that sophisticated capabilities exist to gather electronic transmissions of different types. They suggest, however, that any claims that every one of the many millions of daily telephone calls, facsimile transmissions, and emails can be intercepted, translated and analyzed are not credible. Further, the technical ability of intelligence agencies to sift out all words or identify speakers which might be of significance is distinctly limited. For inevitable reasons, intelligence agencies are unwilling to disclose the extent of their electronic surveillance capabilities and their accomplishments—a factor that inhibits the useful forms of public cost-benefit analyses.

Although discounting media claims regarding the universality of the U.S. surveillance effort, observers of the Intelligence Community argue that sigint provides an extremely valuable, and often unique, source of information in an international environment that contains dangerous elements fully capable of undermining democratic institutions in this country and throughout the world. In particular, observers cite its value in obtaining information on terrorist groups planning attacks on U.S. facilities, on smugglers attempting to transport illegal narcotics into the U.S., or on hostile countries capable of attacking the U.S. or its allies. For certain targets, unapproachable by human agents or indistinguishable by overhead imagery, sigint is said to provide unique information.

It is known that electronic surveillance efforts have faced new technological challenges in recent years. People throughout the world are communicating more—through regular telephones, cellular telephones, facsimile, email, and through the Internet. Furthermore, the increasing use of fiber optic lines rather than microwave transmission presents challenges not readily overcome. The spread of sophisticated, but inexpensive, encryption systems has also complicated electronic surveillance efforts.⁷ Indeed, the House Intelligence Committee has reported that NSA needs radical surgery to adapt to the post-Cold War environment and has concluded that “NSA is in serious trouble.”⁸

Apprehension about NSA is found among European observers who suspect that U.S. intelligence agencies might be supporting U.S. corporations competing for international business—a suspicion not shared by most U.S. observers because of the complications that would be involved in transferring government intelligence to corporations in a highly

⁶ Robert L. Dietz [General Counsel of NSA], Letter to the Editor, *Washington Post*, December 7, 1999, p. A30.

⁷ On encryption, see Richard Nunno, *Encryption Technology: Congressional Issues*, CRS Issue Brief IB96039.

⁸ U.S. Congress, House of Representatives, 106th Congress, 1st session, Permanent Select Committee on Intelligence, *Intelligence Authorization Act for Fiscal Year 2000*, H. Rept. 106-130, Part 1, May 7, 1999, p. 12. See also, Seymour M. Hersh, “The Intelligence Gap,” *New Yorker* December 6, 1999.

competitive environment. Many major U.S. corporations are not wholly U.S.-owned and in those cases there would be no way to provide sensitive intelligence without revealing it to non-U.S. persons. U.S. intelligence agencies do, however, collect economic intelligence based on an established requirement to provide information to senior U.S. policymakers regarding unfair or illegal activities of foreign governments and corporations.

An underlying problem related to current concerns about electronic surveillance for intelligence purposes is the increasing overlap between foreign intelligence and law enforcement concerns.⁹ As a result of international banking scandals in the late 1980s, procedures were worked out between U.S. intelligence and law enforcement agencies to use information derived from intelligence sources in judicial proceedings. In addition, terrorism and narcotics trafficking, formerly considered law enforcement matters, have been elevated to national security concerns, thus justifying the employment of intelligence resources. Such use has required that information be collected and disseminated in accordance with specific laws and regulations that are designed to ensure that defendants' rights are protected. Seeking to clarify statutory authorities, the FY1997 Intelligence Authorization Act (P.L. 104-293) authorized intelligence agencies, including NSA, to collect information outside the U.S. about individuals who are not U.S. persons at the request of U.S. law enforcement agencies.¹⁰ Despite strict regulations, however, some observers—and some within intelligence agencies—question whether it will ultimately be advisable to introduce into the judicial system information that has been gathered by procedures designed for collection of foreign intelligence information.¹¹

International Cooperation

An issue for many critics has been secret international cooperation in sigint collection and reporting. The United States has cooperative intelligence collection arrangements with a number of foreign countries. The closest are those that emerged during World War II with the British, Canadians, and other Commonwealth countries. There have been numerous references to a formal agreement signed in 1948 regarding sigint cooperation between the United States and the United Kingdom although no text has been made public.¹² Given the extensive political and military ties between the two countries, the advantages of agreement would include the allocation of tasks and thus considerable savings in expenditures. The United States, Britain, Canada, Australia, and New Zealand shared common security policies in the Cold War and continue to cooperate in opposing

⁹ See Richard A. Best, Jr., *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.*, CRS Report RL30252, July 2, 1999.

¹⁰ Previously, such information was to be collected incidentally to foreign intelligence collection efforts, not for law enforcement purposes or even at the request of law enforcement agencies. Section 814 of P.L. 104-293 states, however, that intelligence agencies “may collect such information notwithstanding that the law enforcement agency intends to use the information collected for purposes of a law enforcement investigation or counterintelligence investigation.”

¹¹ See Stewart Baker [a former General Counsel of NSA], “Should Spies Be Cops?,” *Foreign Policy*, Winter 1994-1995.

¹² See, for instance, Christopher Andrew, “Intelligence and International Relations in the Early Cold War,” *Review of International Studies*, July 1998; also, Jeffrey T. Richelson and Desmond Ball, *The Ties that Bind*, 2nd ed. (Boston: Unwin Hyman, 1990).

rogue states, terrorist groups, and narcotics smugglers. (However, even close allies do not have identical interests throughout the world and do not share sensitive intelligence across the board.)

Congressional Reaction

Responding to concerns expressed about the propriety of NSA's operations, including Echelon, in May 1999 the House of Representatives adopted an amendment offered by Representative Barr to the FY2000 Intelligence Authorization bill (H.R.1555; subsequently enacted as P.L. 106-120), requiring a report from the Executive Branch (in both classified and unclassified forms) detailing legal standards for:

- The interception of communications when such interception may result in the acquisition of information from a communication to or from U.S. persons;
- Intentional targeting of communications to or from U.S. persons;
- Receipt from non-U.S. sources of information pertaining to communications to or from U.S. persons;
- Dissemination of information acquired through interception of communications to or from U.S. persons.¹³

The resulting report, the unclassified version of which was made available in late February 2000, reviews legal protections of communications of U.S. persons. It notes that in order to conduct electronic surveillance against a U.S. person located in the United States, statutes require that a U.S. intelligence agency must have a court order; if a U.S. person is abroad, E.O. 12333 requires approval by the Attorney General. The report further notes that, while FISA provides the statutory basis for conducting electronic surveillance within the U.S., E.O. 12333 establishes the overall framework for intelligence activities, including electronic surveillance, worldwide. A key principle of the E.O., it notes, is protecting the rights of U.S. persons; another is a prohibition on U.S. agencies requesting other, (*i.e.*, non-U.S.) parties to undertake activities that are forbidden by the E.O. Various procedures have been established to minimize or limit dissemination of information relating to U.S. persons that might be acquired incidentally in otherwise authorized surveillance [for instance, communications between foreign agents describing activities of a U.S. person]. The report describes, but does not enclose, various agency regulations that implement FISA and E.O. 12333.

In evaluating the report, Congress may choose to go beyond the question of whether current laws and regulations are being followed. Some foreign observers regard any U.S. surveillance efforts with suspicion, fearing that intelligence products will be used against their national interests, the privacy rights of their citizens, or to advance the interests of U.S. firms in competition for international business. This view is held even though it is

¹³ During floor consideration of the conference report on the intelligence bill, Representative Goss, Chairman of the Permanent Select Committee on Intelligence stated: "I can report, notwithstanding this provision [Section 309], that the committee has substantial insight into the action of the NSA and the guidance of its legal staff. I have thus far no reason to believe that the NSA is not scrupulous in following the Constitution and the laws concerning its SIGINT mission." *Congressional Record*, November 9, 1999, p. H11756.

well-known that many countries have long undertaken similar efforts. Nonetheless, some argue that electronic surveillance, except in a narrow, court-approved, law enforcement context, should not be undertaken by democratic governments.

Responding to media discussions of Echelon, Director of Central Intelligence George Tenet in a March 2000 press interview with Reuters News Service denied that U.S. intelligence agencies spy on foreign firms to give American companies competitive advantage. “We do not spy on foreign companies for the economic gain of American companies. We don’t do this. It’s our policy, it’s our regulation, we do not do this.” On the other hand, Tenet noted, “...if we find that an American company is being robbed, cheated and stolen or somebody is bribing and disenfranchising an American company, we will go to the Secretary of State or the Secretary of Commerce and say ‘we have this information, you figure out how to deal with it.’”¹⁴

Most observers tend to believe that some electronic surveillance for intelligence collection purposes will be found necessary for national security and law enforcement purposes. They argue that, in any event, laws and regulations involving signals intelligence are based on a balance between, on one hand, perceived requirements for collecting information on important security concerns with, on the other, the recognized importance of protecting individual privacy and fairness to individuals, groups, and enterprises. In the context of domestic law enforcement such a balance exists and is met in large measure through court-supervised legal procedures for undertaking wiretaps and other forms of electronic surveillance. Observers argue that such protections cannot be readily extended to efforts beyond U.S. borders that affect non-U.S. persons; few would support involving the courts in routine and ongoing signals intelligence operations.

Observers supportive of NSA argue that legitimate concerns about the intrusion of electronic surveillance into the communications of U.S. persons, as well as the proper use of sigint, can be addressed in a number of ways—by laws and regulations, by public hearings, and by Executive Branch and congressional oversight. They note that the authority to task intelligence agencies rests ultimately with the National Security Council, that appropriate congressional committees are kept “fully and currently informed” of collection activities, and that Congress must authorize and appropriate funds on an annual basis. The major issue with regard to sigint, they suggest, is broader—namely, that the widespread dissemination of sophisticated intelligence and expansion of communications are creating a signals environment from which warning of armed attacks, terrorist activities, or narcotics smuggling can be gleaned only with enormous difficulty and greater costs. A number of observers believe that NSA, in particular, must be radically restructured if it is to continue to support national security objectives—an effort that will take years and require a substantial increase in budgetary authority.

¹⁴ Tabassum Zakaria, *Interview-CAI Chief says US doesn’t spy for firms*, Reuters, March 1, 2000.

EveryCRSReport.com

The Congressional Research Service (CRS) is a federal legislative branch agency, housed inside the Library of Congress, charged with providing the United States Congress non-partisan advice on issues that may come before Congress.

EveryCRSReport.com republishes CRS reports that are available to all Congressional staff. The reports are not classified, and Members of Congress routinely make individual reports available to the public.

Prior to our republication, we redacted names, phone numbers and email addresses of analysts who produced the reports. We also added this page to the report. We have not intentionally made any other changes to any report published on EveryCRSReport.com.

CRS reports, as a work of the United States government, are not subject to copyright protection in the United States. Any CRS report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS report may include copyrighted images or material from a third party, you may need to obtain permission of the copyright holder if you wish to copy or otherwise use copyrighted material.

Information in a CRS report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to members of Congress in connection with CRS' institutional role.

EveryCRSReport.com is not a government website and is not affiliated with CRS. We do not claim copyright on any CRS report we have republished.