Signals intelligence and human rights

– the ECHELON report -

Prepared by Duncan Campbell

for the

Electronic Privacy Information Center

epic.org

TABLE OF CONTENTS

Published by Electronic Privacy Information Center,
1718 Connecticut Avenue, Washington D.C. 20009

INTRODUCTION

No part of the U.S. government is more protected by secrecy than the National Security Agency (NSA). Founded in 1952 as the successor to wartime codebreaking agencies that attacked German, Japanese and other enemy communications, the NSA was – and remains – the largest component of the United States intelligence community.

Five years before NSA was formed, the U.S., British and British Commonwealth governments agreed to ally their peacetime signals intelligence (Sigint) agencies into a single unified global network with common procedures and standards. Over time other nations joined this network, on more limited terms than the original English-speaking participants. In the years of the cold war, this combined intelligence organization devoted the majority of its resources to seeking intelligence about the Soviet Union, China, and their allies. But the agencies, their budgets and equipment did not disappear when the cold war ended. Although there were reductions, they were redeployed and retargeted – and in some ways enlarged, to deal with new technologies.

As this report reveals, throughout the cold war, and even in the years of greatest east-west tension, the Soviet Union was far from the only focus of NSA and its allies. Part of this report is concerned with the ECHELON project. ECHELON is a system for intercepting civilian and commercial communications carried by satellite. Planning for ECHELON began as early as 1966, in an era when the communications satellites being targeted were run solely by the West[1] and carried no Soviet or Chinese military communications. Plans for the massive extension of the system were drawn up in the early 1980s, and put into effect in the 1990s. The system continues in existence. Although some commentators (responding in part to exaggerated accounts of its capabilities) have suggested that the system is an invention, this view became untenable when U.S. government documents released under the Freedom of Information Act confirmed the status of four U.S. Sigint stations as "Echelon Units" and identified the nature of their tasks.[2] ECHELON still predominantly intercepts ordinary commercial and private communications between friendly western nations.

No part of NSA's Sigint operations has ever been willingly made public. Incumbent NSA directors have testified about the legal aspects of its activities before Congress in open session on only two occasions in its 48 years of existence. The first, in the fall of 1975, was part of the post Watergate investigations of the misconduct of U.S. intelligence agencies.[3] The second occasion, in April 2000, followed an increasing wave of international media interest and public concern about the impact of systems such as ECHELON on constitutional rights.[4] At the time of writing, the Congressional Committee on Government Reform also proposes to hold hearings into Sigint, ECHELON and constitutional rights. This report is intended to assist such inquiries.

---

[1] The satellites were in fact controlled and managed from the United States, by the Intelsat consortium, whose headquarters are at 3400 International Drive NW, Washington DC.

[2] See page 32.

[3] Senate Select Committee to Study Government Operations with Respect to Intelligence Activities (Church), 94th Congress, First session, Volume 5 "National Security Agency and Fourth Amendment Rights", 29 October and 6 November 1975.

[4] House Permanent Select Committee on Intelligence, Hearing on the National Security Agency, 12 April 2000.

Opening his 1975 hearings, Senator Frank Church observed that "the danger [to constitutional rights lies in its ability to turn its awesome technology against domestic communications … the NSA could be turned inward and used against our own people." These observations are truer in the 21st century than before. Telecommunications and information technology have become the foundation of society. The technical boundaries of "domestic" and "international" communications have blurred, to the extent that it is not possible to know what country an Internet user is in, let alone what her or his nationality is. In a globalized, highly interconnected world, "foreign intelligence" can be found almost everywhere, not just in remote physical territories.

One remedy to intelligence agencies' intrusions into the rights of U.S. citizens was the Foreign Intelligence Surveillance Act (FISA) of 1978.[5] The Act introduced controls on the circumstances in which intelligence agencies could conduct electronic surveillance within the United States or deliberately target the private communications of U.S. citizens. But FISA has little impact on the type of NSA abuses exposed during the 1970s, which involved only international communications. Although changes were made to NSA's fundamental directives and mechanisms in the 1970s and later, these remain shrouded by complexity and heavy classification. NSA's activities, now as then, are authorized only by presidential directives and derivative instruments, of which many of the most critical portions affecting constitutional rights have been classified and withheld. As such, they are subject to amendment without notice. It is not apparent that, were another candidate like Richard Nixon to be elected to the Presidency, NSA would be restrained by current legislation or policy from performing the services it undertook from 1967 to 1973.

Early in 1999, the House Permanent Select Committee on Intelligence asked NSA to provide copies of legal memoranda concerning the collection and dissemination of the communications of U.S. citizens. NSA refused to comply, citing "attorney-client privilege" as its reason. After facing severe criticism, and after some delay, NSA changed its position and complied. The agency produced about one hundred documents, dated from 1993 to 1999. EPIC has obtained the same documents, following a FOIA action against the agency. Although heavily redacted, they provide a unique insight into NSA's operations and methods. They suggest that, although NSA is careful to comply strictly with FISA, the Act functions as a smokescreen, drawing attention away from important technical and constitutional issues. These include the obscure nature of the Agency's authority, the many classified exemptions which permit it to conduct warrantless electronic surveillance, and the lack of (visible) restrictions on what the agency does *internally* with a huge volume of "incidentally" intercepted and stored communications of U.S persons.

New communications systems, and the nature of today's communications have led NSA and its supporters to argue that it should indeed "turn inward" and be given more access and more power as the guardian of the nation's "critical infrastructure".[6]

This report argues that FISA places no effective restraint on NSA surveillance on the international communications of U.S. citizens, of all types and in every place. FISA and other restrictions operate to limit intelligence surveillance in the U.S. It affects information that *leaves* NSA, but not that which *enters* the agency's computers and

[5] 50 USC §§ 1801-1819.
[6] Wayne Madsen, Critical Infrastructure Protection and the Endangerment of Civil Liberties, EPIC, 1999.

storage systems, or those of its foreign allies. Critical questions about how the NSA can "minimize" extending intrusion in the era of the Internet have been asked many times, but never (publicly) answered. Advanced data processing systems and methods can conform to the rules of the 1970s, yet strip a person naked of privacy. The possible methods of conducting electronic search and seizure in the 21st century were not foreseen in the 1970s, far less two hundred years earlier.

Today's citizens face the search and seizure of private communications in ways never before imaginable. When the Bill of Rights was written, it was inconceivable that British redcoats who had been beaten back to their homeland could intrude on the privacy of an American household. Their successors are in a different position. In 2000, Britain's GCHQ[7] can intercept and process many forms of U.S. domestic communications at will, with or without NSA co-operation. Despite strong denials, there is substantial evidence that NSA and collaborating agencies like GCHQ have co-operated to pass questionable project to each other. Thanks to satellite communications, France and other European countries can and do extend the reach of their interception systems into the domestic and international communications of the Americas. Foreign corporations and multinationals, as well as governments, can also collect U.S. private communications. From a site near Havana, Cuba, both Russia and China operate facilities that intercept U.S. domestic communications.

The privacy of international communications remained badly protected in large part because NSA, GCHQ and their allies have long fought to keep them unprotected, in order to protect their own surveillance capacities.

This report argues for a comprehensive reconsideration of the right to privacy, internationally as well as nationally. It calls for the clarification of international arrangements affecting Sigint, and for the recognition and reinforcement of everyone's rights to international telecommunications privacy. It offers an agenda for legislators to consider.

Duncan Campbell

Washington DC, June 2000

[7] Government Communications Headquarters, the British Sigint agency and counterpart to NSA.

Acknowledgements

Any report in this difficult and recondite field has to stand on many years prior work by other international researchers and writers. I have collaborated with and drawn assistance in particular from Nicky Hager and Owen Wilkes in New Zealand, Ross Coulthart and Des Ball in Australia, Jeff Richelson, Bob Windrem, Steve Aftergood, Jim Bamford, Matthew Aid, John Pike, Bob Fink and John Young in the U.S., and Bill Robinson and Dominic Patten in Canada. Jean Guisnel has slotted the French role into the picture. Many researchers in this specialized area also benefited from the remarkable achievement of Cies Weibes in the Netherlands in putting together the first-ever unrestricted international Sigint conference in 1999, where for the first time ever a senior Sigint practitioner (the deputy director of the Dutch agency) talked openly about the methods and functioning of a modern Sigint organization.

I also thank colleagues in and around EPIC for guidance, advice and support; Marc Rotenberg, David Sobel, Wayne Madsen, and David Burnham of TREC, and also Barry Steinhardt and Greg Nojeim of ACLU, and Brad Alexander of the office of Congressman Bob Barr.

Most of those who have worked inside or with Sigint organizations and who have assisted this and earlier research must remain anonymous, but those who can be acknowledged include Fred Stock, Mike Frost, Margaret "Peg" Newsham, Jock Kane, Alex Laurie, Perry Fellwock, and John Berry.

Whit Diffie and Susan Landau, the authors of *Privacy on the Line*, first proposed this report. I am glad to be able to go forward and add to their comprehensive examination of the U.S. wiretapping scene[8].

The full details of Echelon would never have come to public attention but for six years of careful work by New Zealand writer Nicky Hager. His 1996 book *Secret Power*[9] is based on extensive interviews with and help from members of New Zealand's Sigint organization. It remains the best-informed account of how Echelon works. In 1998 and 1999, the intelligence specialist Dr Jeff Richelson of the Washington, DC National Security Archive used the Freedom of Information Act to obtain modern U.S. Navy and Air Force documents which confirmed the continued existence, scale and expansion of the Echelon system. Because of these workers, there is now no room for doubt about the substance of the 1988 revelations by Ms Newsham. I am grateful to her and others who must still stand in the shadows, perhaps in fear, while they blow the whistle in the public interest.

[8] Whitfield Diffie and Susan Landau, Privacy on the line – the politics of Wiretapping and Encryption, MIT Press, 1999.

[9] Craig Potton Publishing, Nelson, New Zealand, 1996.

THE GLOBAL SURVEILLANCE SYSTEM

Signals intelligence or "Sigint" is an industrial activity that involves the large-scale interception and processing of telecommunications of all types, at the rate of hundreds of millions of message a day. The nature of the work of Sigint agencies has been represented in contemporary Hollywood melodrama[10], and in historical accounts of wartime codebreakers forcing their way into Japanese, German or Soviet ciphers. Neither gives an accurate picture of today's intelligence organizations, which because of the growing dependence of society on electronic information, appear more than ever to have "the capacity … to make tyranny total in America."[11]

Today's global electronic surveillance system derives principally from the conflicts of the Second World War. But in a deeper sense, it results from the invention of radio and the fundamental nature of telecommunications. The creation of radio permitted governments and other communicators to pass messages to receivers over transcontinental distances. But there was a penalty – anyone else could listen in. Previously, written messages were physically secure (unless the courier carrying them was ambushed, or a spy compromised communications). The invention of radio thus created a new importance for cryptography, the art and science of making secret codes. And it led to the business of signals intelligence.

The power of Sigint organizations to use their knowledge is limited - by legal restrictions, resource constraints, developing technology and in particular by extraordinary security restrictions that they impose on their product, which can often all but nullify the use others make of the information they obtain.

During the 1970s, the Church and Pike committees documented abuses by U.S. intelligence agencies, including the NSA, directed against U.S. citizens. These investigations resulted in reforms in the conduct of U.S. intelligence and the institution of new oversight mechanisms, through the creation of the House and Senate Intelligence Committees.

In 2000, the concerns of Congressional oversight committees appear mainly to be focused on NSA's reported technical and managerial difficulties rather than the challenges its work poses to privacy and fundamental rights. In a current report, the Senate Intelligence Committee reported "failure to invest in the infrastructure and organizational changes required to keep pace with revolutionary developments in the global telecommunications arena … as a result, the NSA enters the 21st Century lacking the tools necessary to maintain the status quo, much less meet emerging challenges"[12].

If these assertions are correct, then it is also appropriate to debate whether Sigint agencies should keep their untrammeled right to surveil international communications – an activity which, like much else in intelligence, is unlawful and in breach of human

[10] Notably "Enemy of the State", released in 1999.

[11] Comment by the late Senator Frank Church, in 1975 : "I know the capacity that is there to make tyranny total in America, and we must see to it that this agency ... operate[s] within the law and under proper supervision, so that we never cross over that abyss".

[12] Senate Select Committee on Intelligence, report on S.2507, authorizing funds for fiscal year 2001 for intelligence programs and activities of the US, 4 May 2000.

rights. There is no *prima facie* reason why international communications should have less protection under the Fourth Amendment than domestic communications, or why U.S. citizens abroad should enjoy a lesser standard of protection - but that is the case. The same applies in Europe, where the European Union and European Parliament have been considering the issue in detail. Article 8 of the European Convention on Human Rights protects international as well as domestic communications but – like the Fourth Amendment – it has not been rigorously applied.

More than 30 nations operate substantial Sigint agencies, globally and regionally. The largest is NSA, which since its inception has been part of the global monitoring network known as UKUSA, after a 1947 agreement between the U.S. and Britain. The terms of the UKUSA pact remain secret, as do subsequent and supplementary agreements with British Commonwealth and other "Third Party" countries.

The National Security Agency's structure and operations are not and have never been controlled by legislation but derive from directives and Presidential Executive Orders. A National Security Intelligence Directive, NSCID 6, formally brought the agency into being on 4 November 1952. It replaced a predecessor, the Armed Forces Security Agency. In 1957, it moved to its present headquarters "campus" at Fort George G. Meade, adjacent to the Baltimore-Washington parkway.

Since that time, NSA has had sole control of U.S. Sigint activities. The current order prescribes its functions as the "establishment and operation of an effective unified organization for signals intelligence activities …", except for the delegation of operational control over certain operations that are conducted through other elements of the Intelligence Community. "No other department or agency may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense".[13] The agency is also instructed to "conduct … foreign cryptologic liaison relationships, with liaison for intelligence purposes … in accordance with policies formulated by the Director of Central Intelligence". It is required to administer security regulations for the handling of Sigint information and product. These regulations are agreed between the U.S. and its English-speaking allies.

The overall Sigint production system is known as the U.S. Sigint System (USSS). The USSS consists mainly of the Sigint missions of NSA and the Sigint components of the intelligence organizations of the four military services. Collectively, these are known as the Central Security Service (CSS). The Director of NSA is simultaneously the Chief of CSS. Inside the USSS, arrangements for handling the personal and protected information of U.S. citizens are different to those required of NSA's customers.

The U.S. Air Force Air Intelligence Agency (AIA) runs Sigint field stations overseas, and helps operate a Regional Sigint Operations Center (RSOC) at the Medina Annex of Kelly Air Force Base, San Antonio, TX. Each RSOC is responsible for support to a specific military command or commands. The Medina center is responsible for processing Sigint primarily for the U.S. Central and Southern commands command. Elements of AIA assist in operating ECHELON units at four U.S. sites – Sugar Grove, VA, Sabana Seca, PR, Yakima, WA and Guam. A fifth AIA unit operates a satellite communications interception site at Misawa, Japan. The Air Force also operates an Information Warfare Center at San Antonio.

[13] Executive Order 12333, Part 1.12(b); signed by President Reagan on 4 December 1981.

The U.S. Naval Security Group (NSG) operates a Regional Sigint Operations Center at Kunia, Hawaii, providing for military requirements in the Pacific Rim. It administers and operates field stations including Sugar Grove, VA, Guam and Sabana Seca, Puerto Rico. These stations' primary mission is the collection of civilian satellite communications signals as part of the ECHELON system. A naval Fleet Information Warfare center is located at Norfolk, VA.

The U.S. Army runs a third RSOC at Fort Gordon, GA, providing Sigint support to Central and European commands. During the 1990s, the Army also took over the administration of the NSA's two largest overseas Field Stations collecting Sigint data. Field Station F83 at Menwith Hill, Yorkshire, England is a primary center for operating and processing data from Sigint satellites. Its second major function, known as MOONPENNY, is to intercept data from other country's satellites, military or civil. Run in collaboration with the British agency GCHQ, Menwith Hill is the largest interception site in the world. NSA Field Station F81 at Bad Aibling, Bavaria, Germany operates the GARLICK system, which also intercepts satellite communications.

Besides NSA and the Sigint components of the military intelligence agencies, elements of the CIA also operate Sigint collection sites, often clandestinely. In Australia in 1968, the CIA established a receiving station at Pine Gap, close to Alice Springs, to receive data from the first Sigint satellite to be placed in a high geostationary orbit, RHYOLITE. Many interception sites are located within U.S. embassies or diplomatic premises abroad, and are run jointly by the CIA and NSA as the Special Collection Service (SCS). SCS operate from secure headquarters now located near Beltsville, MD. Its interception units deployed overseas to U.S. embassies and other sites are known as Special Collection Elements, or SCEs.

Intelligence requirements and collected data and signals flow round the world between field stations, the RSOCs, and NSA's National Sigint Operations Center (NSOC) located within its Fort Meade headquarters. U.S. field stations operate in a single integrated network with those of the UK, Canada, Australia and New Zealand. The collaborating organizations are Britain's GCHQ located at Cheltenham, England, the Australian Defence Signal Directorate (DSD) based in Canberra, Canada's Communications Security Establishment (CSE) in Ottawa, and the New Zealand organization, the Government Communications Security Bureau (GCSB), in Wellington.

In the fall of 1999, NSA director Lt-Gen Michael V. Hayden returned from a visit to the UK and told staff that GCHQ and NSA had renewed a long-standing commitment to work together. "We must go back to our roots with GCHQ," he said.[14]

Each allied station has a unique identifier within the integrated system, denoting the primary nationality and operating component at each site. For example, the U.S. Air Force site in Misawa, Japan is USA39, Canada's main interception site at Leitrim near Ottawa is CAF97, New Zealand's civilian run satellite interception station is NZC333, a British army Sigint unit in Cyprus is UKM253, and NSA's Menwith Hill Station is USD1000.

Not until 1999 did any of the participating governments make any direct public acknowledgement of their Sigint co-operation. In March 1999, the Australia government broke ranks and stated publicly that the Defence Signals Directorate (DSD) "does co-

[14] Loud and Clear - The most secret of secret agencies operates under outdated laws, James Bamford, *Washington Post*, 14 November 1999.

operate with counterpart signals intelligence organisations overseas under the UKUSA relationship".[15]

Besides integrating their stations, each country appoints senior officials to work as liaison staff at the others' headquarters. The United States operates a Special U.S. Liaison Office (SUSLO) in London and Cheltenham, while a SUKLO official from GCHQ has his own offices inside NSA headquarters at Fort Meade. Similar arrangements are made between each allied agency.

Under the UKUSA agreement, the five English-speaking countries took on responsibility for overseeing surveillance in different parts of the globe[16]. Britain's zone included Africa and Europe, east to the Ural Mountains of the former USSR; Canada covered northern latitudes and Polar regions; Australia covered Oceania. The agreements prescribed common procedures, targets, equipment and methods that the Sigint agencies would use. Other countries including Norway, Denmark, Germany and Turkey later signed Sigint agreements with the United States and became "Third Party" participants in the UKUSA network.

Although the world's largest surveillance network is run by UKUSA, it is far from alone. Russia, China, France and other nations operate substantial networks. For each of these countries, U.S. communications of every type are a primary target. Dozens of advanced nations use Sigint as a source of intelligence. Even smaller European nations such as Denmark, the Netherlands or Switzerland have recently constructed small, Echelon-like stations to obtain and process intelligence by eavesdropping on civil satellite communications.

In earlier years, the UKUSA network focused on the containment of the former Soviet Union. In the 1990s, citing threats of terrorism, narcotics trafficking and weapons proliferation, it set out to extend surveillance of the worlds' main communications arteries. One of the two main goals of NSA and its surveillance system, as noted by former NSA Director Vice Admiral William O. Studeman in 1992, is "global access".[17]

Access to communications

Signals intelligence activities break down into four sequential components – collection, processing, analysis and dissemination. Taking into account the assessment of

---

[15] Statement by Martin Brady, Director of DSD, 16 March 1999. Broadcast on the *Sunday Programme*, Channel 9 TV (Australia), 11 April 1999. Earlier, Canada had made a more cautious statement, when the Parliamentary Security and Intelligence committee stated "Canada collaborates with some of its closest and long-standing allies in the exchange of foreign intelligence... These countries and the responsible agencies in each are the (National Security Agency), the U.K. (Government Communications Headquarters), Australia (Defence Signals Directorate), and New Zealand (Government Communications Security Branch [sic])" (May 1995).

[16] The arrangements are sometimes called "TEXTA Authority". TEXTA stands for "Technical Extracts of Traffic Analysis" and is a voluminous listing of every communications source identified by each agency. It is catalogued and sorted by countries, users, networks, types of communications system and other features, such as cryptosystems in use.

[17] Valedictory letter to NSA staff, 8 April 1992. A copy is available on-line at www.gwu.edu/~nsaarchiv. The "business area" of "global access" was, Studeman said, one of "two, hopefully strong, legs upon which NSA must stand" in the next century. The other was Support to Military Operations, or SMO.

the quality and relevance of disseminated reports leads in turn to the re-specification of intelligence collection priorities, thereby completing the intelligence cycle.

Collection, the first stage, means finding, acquiring, and intercepting electronic signals. The essential prelude to collection is to have, or obtain, access to the signal path. The methods employed are as variable as can be imagined. They include more-or-less ordinary radio receivers, the unauthorised interception of commercial satellites, exotic wiretapping devices disguised as parts of trees, tapping into long distance communications from satellites in space, tapping undersea cables using submarines, or plugging into the heart of the Internet.

Within Sigint, the interception of international civilian communications forms a large and distinct target, readily distinguishable from many categories of exclusively or predominantly military interception systems. The targets of the Sigint civilian communications interception mission are international common carrier circuits of every type. Within Sigint, these are known as International Leased Carrier, or ILC.

Until the 1960s, the predominant means of international communications was high frequency (HF) radio. Radio interception is the simplest form of Sigint. Radio messages (including cell phones and other mobile radio systems) can be intercepted directly by techniques no more complex than erecting a wire antenna. However, many HIF interception systems for Sigint are elaborate affairs, typically involving large circular arrays of masts to pick up weak signals and simultaneously determine their direction of arrival.

During the 1960s, these messages could be civil or military. While some operators tracked the radio messages of Warsaw Pact air forces from USAF sites in Britain in the 1960s and 1970s, other colleagues covered “ILC” - commercially run radio links between major European cities. These networks could carry anything from birthday telegrams to detailed economic or commercial information exchanged by companies, to encrypted diplomatic messages. Around the world, thousands of analysts worked on these mostly unencrypted communications using NSA-supplied 'watch lists' - weekly key word lists of people, companies, and commodities of interest for analysts to single out in the 'clear' traffic. Coded messages were passed on immediately. In the 1960s and 70s, the names of rising Africa leaders were on the watch list. At a U.S. Naval Security Group site at Sidi Yahia, Morocco, analysts were given the name of Black Panther leader Eldridge Cleaver. As uncovered during Senate hearings in 1975, “watch lists” in use by 1970 included the names of actress Jane Fonda, Dr Benjamin Spock and hundreds of others put under surveillance because of their opposition to the war in Vietnam.

Until the 1970s, most long distance messages were written communications, either telegrams or telegraph. These systems were augmented by automatically switched telegraph systems, or telex. Within NSA, these non-aural messages were known as “record” communications. Between 1960 and 1980, the processing of the content of record communications became fully automated. In contrast, aural messages – normally telephone calls – could only be processed automatically by reference to their destinations. In setting up (automatically switched) telephone calls, this information is necessarily passed (in digital form) to the distant switch(es). Conveniently for Sigint operations, the signaling systems used for international telephony were modified during the 1980s so that the originating as well as destination telephone numbers were transmitted in the setup phase of each call. This made it possible for collection systems to target the origination of

any call, as well as the destination. But only human analysts could process the speech content of the call.

Cables laid on land afford no easy access, since the signals they carry can only be intercepted by interfering with the cable or its termination equipment. Some cables can be tapped *inductively* without causing damage to equipment. Generally, this can be done without the cable user being able to detect that monitoring is taking place. Placing a wiretap of this sort however entails a high degree of risk, particularly on hostile territory. There are also ancillary problems, including how the intercepted material is to be relayed to analysts. One solution is to collect and replace recording tapes. A second method is to relay intercepts to a satellite. Both have been used by U.S. intelligence. The intelligence museum of the former KGB (now SVR) in Moscow displays a range of captured U.S. equipment to do this. One is a false tree stump into which is built a satellite communications antenna. Miniaturised inductive taps recorders have also been used to intercept underground cables.[18] CIA agents tapped a coaxial cable running from Moscow to a nearby scientific establishment, by connecting an inductive tap and associated recorders. The convicted CIA spy, Aldrich Ames, allegedly revealed this operation.

But both methods are far from satisfactory, as these instances demonstrate. The problems become dramatically worse with wide bandwidth links. Intercepting higher capacity communications entails either placing a large quantity of processing equipment locally, or frequent collection of tapes, or using high capacity links to satellites. Each approach brings an elevated risk of detection and nullification

Higher capacity messages, such as "multiplex" signals carrying thousands of simultaneous conversations or electronic exchanges, are carried by radio beams using extremely short (microwave) wavelengths. These beams are highly directional. To intercept these beams requires an attacker to choose an appropriate location near to the transmitter. Such sites can be found in cities, where microwave radio relay traffic will always be concentrated. NSA also operates a fleet of Sigint satellites orbiting in approximately geostationary positions, from which weak microwave signals can be intercepted using large antennae.

Optical fibre cables fall into a different, harder category. The signals they carry cannot easily be intercepted without damage to the physical cable, which is likely to be detected. One method of intercepting an optical fibre cable is to gain physical access to the optoelectronic repeaters that amplify the optical signal between sections of cable. Within the repeater, the signal will be available electrically. However, repeaters are no longer required on many routes.

An attacker can consider inserting their own optoelectronic repeater to tap the cable. But any temporary break in the cable will be detected and can be located by simple means. A more complex strategy involves multiply cutting the cable, so that the point at which a tap is inserted is masked by other cuts, which may be made to appear accidental. Since the early 1980s, NSA has invested substantially in devising techniques to extract signals from optical fibre cables without breaking the cable or creating a detectable impact on the signal. The continuing pattern of investment in research and development in this area suggests that techniques have been found to do this.

[18] A specimen of such tapping equipment is held in the former KGB museum in Moscow. It was used on a cable running from Moscow to a nearby scientific and technical institution.

In emergency situations, according to military and intelligence officers, the preferred technique is not to try and access optical fibre cables but to destroy them. This can force an adversary to switch to radio, satellite, microwave or other more readily interceptable communications methods. But this method cannot be used for peacetime or long-term collection.

For the UKUSA Sigint agencies, there is no physical difficulty in accessing many land cables that carry large volumes of foreign traffic. Many of these are the shore connections for intercontinental and regional submarine cables. The majority of Atlantic and Pacific transoceanic cables start, finish or pass through UKUSA countries, or connect via controlled territories such as Hawaii, Guam or the U.S. Virgin Islands.

Undersea submarine cables have also been intercepted in a series of secret operations. At first, submarine cables that did not connect to or through UKUSA countries appeared intrinsically secure because of the nature of the ocean environment. But this security was illusory, as the USSR learned from an NSA spy, Rodney Pelton, in the early 1980s. He revealed to them an adventurous submarine tapping project codenamed IVY BELLS. Starting in 1971, U.S. submarines visited the Sea of Okhotsk, off the eastern USSR, and laid tapping equipment on the seabed to intercept a military cable from Vladivostock to the Khamchatka Peninsula. The tapping pods, constructed to be carried in the torpedo tubes of the submarine USS Halibut, were packed full of high bandwidth, long duration tape recorders. The pods were collected and re-laid every few months.[19] One is now on display in the Moscow intelligence museum.

The Okhotsk cable tapping operation continued for ten years, involving routine trips by three different submarines to collect old pods and lay new ones; sometimes, more than one pod at a time. A new submarine to carry more advanced equipment under the seas was fitted out in the late 1970s. In the summer of the 1979, the new submarine, USS Parche, sailed from San Francisco and under the North Pole to the Barents Sea, adjacent to the northwestern USSR. It laid new cable tapping pods, codenamed ACETONE, on Soviet cables near Murmansk. Its crew received a presidential citation for their achievement. The Okhotsk cable tap ended in 1982, after its location was compromised. Cable tapping tap in the Barents Sea continued in operation, undetected, until tapping was stopped in 1992.

Submarine cable tapping did not stop after the Cold War ended. Instead, it appears to have been extended, and directed towards civilian rather than military targets. Tapping of non-Soviet cables commenced in 1985, when the USS Parche sailed for the Mediterranean, to intercept cables linking Europe to West Africa.[20] After the cold war ended, the Parche was refitted with an extended section to accommodate larger cable tapping equipment and pods. Cable taps could then be laid by remote control, using robot drones.

It is evident from the citations and merit awards presented to the submarine and its crew that the Clinton administration has highly valued its secret achievements. Every year from 1994 to 1997, there were top-level awards.[21] Submarine cable tapping technology continues to be a major investment for NSA. In 1999, it was revealed that a

[19] Blind Man's Bluff, the untold story of American submarine espionage, Sherry Sontag and Christopher Drew, Public Affairs, New York, 1998.
[20] *Op cit.*
[21] *Op cit.*

new submarine of the *Seawolf* class, the USS Jimmy Carter, was to be refitted at a cost of about $400 million for special intelligence missions. The converted submarine will be launched in 2004.[22]

This major expenditure points to covert undersea collection as a major Sigint priority for the next two decades. Until recently, as recounted in the next section, rich intelligence pickings have been available from ECHELON and kindred civil satellite interception systems. But modern digital communications systems have turned back increasingly to cable. Optical fibres offer data communications rates that cannot be equalled by conventional cables or electromagnetic systems. Undersea cables offering data rates of 5 Gigabits/sec[23] are now in use, and much larger systems are in development.

A simple examination of the world's submarine cable layout points to the likely targets of the USS Jimmy Carter. Most cables in the Atlantic and Pacific are accessible from friendly territory at far lower cost than that of a submarine mission. But the communications rich networks passing down and around Asia, especially from Japan to China and on to Singapore and Indonesia, will clearly get attention, as will the cables connecting to and within south Asia, the Indian Ocean and the Gulf. The second obvious target will be communications cables in the Mediterranean, connecting Europe, the Middle East and North Africa. To date, the United States is the only power known to have deployed undersea technology for this purpose.

The end of Cold War led to substantial changes in NSA's collection operations and priorities. Half of its overseas field stations were closed, relocated or turned into Remote Operations Facilities (ROFs) that pass intercepts to centralized processing facilities.

Although there has not been any known change to NSA's declared policy to intercept only communications with "one foreign terminal", new communications systems have made this restriction less meaningful than previously. Until the 1990s, international communications links were clearly physically identifiable. Data communications carried by packet switching (such as the Internet) break the link between physical circuits and endpoints. Each message may be composed of many packets, and packets of the same message can travel by different routes. Proposals for monitoring foreign-derived traffic passing on the U.S. portions of the Internet can easily be extended - and have been extended – to encompass broader domestic surveillance[24].

In these and similar ways, Sigint organisations including NSA, GCHQ and their forerunners have for more than 80 years had arrangements to obtain access to much of the world's international communications. Although NSA Director Michael Hayden has warned of the "alarmingly rapid" scale of change created by new information technologies and their impact on NSA's abilities, some have made the job simpler:

> Some of the very new things look like some of the very old things. One [is] the advent of E-mail … in a very important way, E-mail is a bit going back to the future, looking a

[22] The Intelligence Gap - How the digital age left our spies out in the cold, Sy Hersh, *New Yorker*, 6 December 1999.

[23] A Gigabyte is one thousand million bytes; one word of an English text may typically require 5-6 bytes (unless compressed). Such a link could transmit more than the number of words recorded in the entire Library of Congress, every day.

[24] See note 6.

> lot more like telex, which is the roots of our organization, reading the printed word, rather than the recent past of our organization, which is dealing with the spoken word … the telecommunications [revolution] not only makes our job more difficult. It … makes our job easier. [25]

Sigint processing

Processing is the conversion of collected information into a form suitable for analysis and the production of intelligence, either automatically or under human supervision. Incoming communications are normally converted into standard formats identifying their technical characteristics, together with message (or signal) related information (such as the telephone numbers of the parties to a telephone conversation).

Processing may also involve translation or "gisting" (replacing a verbatim text with the sense or main points of a communication). Translation and gisting can to some degree be automated.

Physical access to electronic signals is the first step in the processing chain before communications can be examined for intelligence. Many high capacity communications links will carry mixed traffic of television, telephone, fax, private voice channels, video and data. Communications satellites carry a variety of transponders, which may serve a multiplicity of cities and countries with connections. The pattern of links may change frequently. SATCOM (communications satellite) analysts at Sigint field stations continually monitor new and existing satellites to track changing connections. Links will be identified as video (and usually ignored), public switched telephony channels, public switched telegraphy channels, or data carriers. For example, a satellite interception station tasked to study a newly launched communications satellite will direct an antenna to intercept all that the satellite sends to the ground. Once a survey has established which parts of the satellite's signals carry, say, television or communications of no interest, these signals will not progress further within the system.

Digital data carriers are the lowest or “transport” layer of modern communications systems, with complex and changing patterns of usage.

Ultimately, intercepted traffic is directed into four basic levels of processing. The simplest and most traditional is telex and telegraphy. These are usually formed in multiple channels, which must first be broken down and separated. They may then be read simply. Within the telephony channels will be found phone calls, fax calls, and some data. This traffic is easily separated by recognition of the signaling tones with which fax machines and modems recognize each other and start their exchanges.

However, fax messages and high-speed modem data signals are not straightforward to intercept. High-speed data exchanges involve simultaneous signalling by machines at both end of the connection, possibly on the same frequencies and using complex modulation systems. An interceptor in the middle has to separate the two signal directions and interpret the exchanges correctly in order to read the signals. According to one account, the New Zealand Sigint agency GCSB failed to read fax traffic for several years, until specially built fax analysis equipment became available.[26] Once intercepted

[25] House Permanent Select Committee on Intelligence, Hearing on legal standards for electronic surveillance, 12 April 2000.

[26] Nicky Hager, Secret Power, Craig Potton Publishing, Nelson, New Zealand

fax images are obtained, they are processed by automatic "optical character recognition" (OCR) software. This turns typescript images into computer readable (and processable) text. OCR systems that can reliably recognise handwriting, however, do not exist.

High-speed data can also be passed to analysis terminals, which work quickly to interpret and analyse every type of telecommunications system, including European and American electronic and optical standards. NSA's data workstations are designed to categorise all aspects of data communications, including systems for handling e-mail or sending files on the Internet.[27] The workstations can store and automatically process thousands of different recorded signals.

Because of the high information rates used in many modern networks, and the complexity of the signals within them, it is common for high-speed recorders or "snapshot" memories temporarily to hold large quantities of data while processing takes place.

At an early stage, if it is not inherent in the selection of the message or conversation, each intercepted signal or channel will be described in standard "case notation". Case notation first identifies the countries whose communications have been intercepted, usually by two letters. A third letter designates the general class of communications: C for commercial carrier intercepts, D for diplomatic messages, P for police channels, etc. A fourth letter designates the type of communications system (such as S for multi-channel). Numbers then designate particular links or networks. Thus for example, during the 1980s NSA intercepted traffic designated as "FRD" (French diplomatic) from Chicksands, England, while the Britain's GCHQ deciphered "ITD" (Italian diplomatic) messages at its Cheltenham headquarters.

Whenever access to international communications channels is obtained for one purpose, access to every other type of communications carried on the same channels is automatic, subject only to the tasking requirements of agencies. Once access is available, as NSA's Director recently acknowledged to Congress, there are no technical systems able to can separate use from abuse:

> For us to do our mission in today's telecommunications world requires a substantial amount of capability, okay. It's theoretically possible for us to use that capability -- technologically possible to use that capability in ways that are prohibited. Of course I have to answer yes. But the oversight mechanisms, the training, the procedures, the culture of the institution, the laws and regulations that we have put in place, make that as a practical matter well nigh impossible to do.[28]

He also claimed:

> The same telecommunications revolution that challenges us also gives us the tools to better filter what we collect on the front end so that we can actually, in many ways, reduce the probability of inadvertent collection of protected communications.

[27] A "Data Workstation" processes TCP/IP, PP, SMTP, POP3, MIME, HDLC, X.25, V.100, and modem protocols up to and including V.42.

[28] See note 25.

In all circumstances, it is clear that the business of Sigint has moved far from the era when (albeit erroneously), it was publicly associated only with monitoring diplomatic or military messages.

Tasking and dissemination

The final step of the intelligence cycle is dissemination, meaning the passing of reports to intelligence consumers. Although such reports can consist of raw (but decrypted and/or translated) messages, gists, commentary, or analyses, raw sigint material is not usually disseminated outside NSA except for the purpose of "analytical exchanges" with other intelligence agencies. Instead, NSA (and allied Sigint agencies) issue "serialized" (separately enumerated series of) end product reports, containing summaries and analysis of intercepted material. The end reports seen by consumers may have details of protected information removed from them, a process called "minimization". Minimization procedures are intended to balance intelligence interests with constitutional protections for privacy. In such cases, however, although the information is withheld from consumers, it continues to be available inside the agency's databanks. Those working inside the United States Sigint System are thus placed in a unique position in relation to their fellow-citizens privacy and constitutional rights.

In collecting, processing and disseminating Sigint information, NSA is required to act in "accordance with guidance from the Director of Central Intelligence". The agency does not set its own collection requirements, or "tasking", but accepts these from and reports back to other agencies in the government, military and intelligence community. The collection of targeted information and links is co-ordinated between stations and allied agencies.

For users, delivery of NSA intelligence looks and feels like using the Internet. Authorized users with appropriate permissions to access "Special Compartmented Intelligence"[29] now use standard web browser software to peruse the output of NSA's Operations Directorate from afar. The system, known as "Intelink", is run from the NSA's Fort Meade HQ. Completed` in 1996, Intelink connects 13 different U.S. intelligence agencies and some allied agencies with the aim of providing instant access to all types of intelligence information. Just like logging onto the world wide web, intelligence analysts and military personnel can view an atlas on Intelink's home page, and then click on a subject or country they choose in order to access intelligence reports, video clips, satellite photos, databases and status reports.[30]

The UKUSA network supporting both collection and dissemination is an integrated network of stations and systems described as "one of the largest WANs [Wide Area Networks] in the world". Few people are aware that the first global wide area network was not the Internet, but the international network connecting Sigint stations and processing centers. This network is connected over high capacity transoceanic cables and military space links. Most of the capacity of the American and British military

[29] "SCI", also known as Special Intelligence, is secret intelligence for which codeword clearance is required. Special regulations also apply to offices in which SCI is examined. They must be physically secure and electromagnetically shielded. These offices are known as SCIFs (SCI Facilities).

[30] The US intelligence intranet is described in Frederick Martin , Top Secret Intranet: How US Intelligence Built Intelink -- the world's largest, most secure network, Prentice Hall 1999.

communications satellites, Milstar and Skynet, is devoted to relaying intelligence data. It was not until the mid 1990s that the public Internet became larger than the secret Internet that connects the stations of the global surveillance network. Britain's Sigint agency GCHQ boasts on its web site: "all GCHQ systems are linked together on the largest LAN in Europe … connected to other sites around the world". The site also claims "the immense size and sheer power of GCHQ's supercomputing architecture is difficult to imagine".[31]

The UKUSA alliance's wide area network is engineered according to the same principles as the Internet[32] (Internet Protocol (IP)), and provides access from all field stations to and from NSA's central computer system, known as PLATFORM. This global network was developed as project EMBROIDERY, and includes PATHWAY, the NSA's main computer communications network. It provides fast, secure global communications for ECHELON and other systems.

Other parts of the system are known as TIDEWAY and OCEANFRONT. NSA's internal intelligence news network is NEWSDEALER. A TV conference system, highly encrypted like every other part of the network, is called GIGSTER. They are supported by applications known as PREPPY and DROOPY. NSA's e-mail system looks and feels like everybody else's e-mail, but is completely separate from the public network. Messages addressed to its secret internal Internet address, "nsa", will not get through.

Access to Sigint product or knowledge of Sigint operations is restricted by a complex, multi-level series of clearances, generally known as compartments. The compartments are governed and allocated on the basis of "need to know". Sigint product is generally known as "Special Compartmented Intelligence, or SCI. Within recipient organizations, it may only be received and examined within physically and electronically secured spaces called SCIFs.[33] The international regulations for Sigint security[34], require that before anyone is admitted to knowledge of the arrangements for obtaining and processing Sigint, they must first undertake a lifelong commitment to complete secrecy. Each individual joining a UKUSA Sigint organization must be "indoctrinated" and, often "re-indoctrinated" each time they are admitted to knowledge of a specific project. On leaving, they are "de-indoctrinated". They are told only what they "need to know", and that the need for total secrecy about their work "never ceases". Under a special 1959 law, information about U.S. communications intelligence activities is specially protected.[35]

Comint activities everywhere are highly classified because, it is argued, knowledge of the success of interception would be likely to lead targets to change their communications methods to defeat future interception. Within the UKUSA system, the outside dissemination of Sigint reports is limited to individuals holding high-level security "SCI" clearances. Further, because only cleared officials can see the reports, only they can set requirements and thus control tasking.

---

[31] These claims are made on GCHQ's web pages, at www.gchq.gov.uk.
[32] TCP/IP, or Transmission Control Protocol/Internet Protocol.
[33] Special Compartmented Intelligence Facility.
[34] Called IRSIG.
[35] 18 USC §798. The US Code can be read online at www4.law.cornell.edu/uscode.

Sigint end product is marked by numerous special codewords that to indicate compartments, including details of interception system. The basic level, which is effectively a higher classification than "Top Secret" is "Top Secret Umbra". More highly classified documents, involving especially sensitive interception systems, are identified as "Umbra Gamma". In the 1970s, the intercepted messages of American antiwar leaders were classified at this especially sensitive level, which had previously been restricted to top level Soviet intercepts.[36] Other codewords can be added to restrict circulation still further. This procedure was used for the intercepts of antiwar activists. A further precaution was that the reports were not "serialized" in the normal way, nor identified as NSA product.

Less sensitive information, such as analyses of telecommunications traffic, may be classified "Secret Spoke". One consequence of the compartmentalization system is that the majority of NSA staff and all uncleared outsiders are unaware of the details of operations in which they are not directly involved.

Watch lists, Dictionaries and filters

By the early 1970s, the laborious process of scanning paper printouts for names or terms appearing on the "watch lists" had begun to be replaced by automated computer systems. These computers performed a task essentially similar to the search engines of the Internet. Prompted with a word, phrase or combination of words, they will identify messages containing the desired words or phrases. Their job, now performed on a huge scale, is to match "key words" or phrases of interest to intelligence agencies to the huge volume of international communications, extract them and pass them to where they are wanted. During the 1980s, the NSA developed a "fast data finder" microprocessor that was optimally designed for this purpose. It was later commercially marketed,[37] with claims that it "the most comprehensive character-string comparison functions of any text retrieval system in the world". A single unit could work with:

> trillions of bytes of textual archive and thousands of online users, or gigabytes of live data stream per day that are filtered against tens of thousands of complex interest profiles.

FDF technology is described as the "fastest, most accurate adaptive filtering system in the world. Devices like this are ideal for use in the Dictionary system.

In a 1992 speech on information management, former NSA Director Studeman described the level and scale of filtering involved in systems like ECHELON:

> One [unidentified] intelligence collection system alone can generate a million inputs per half hour; filters throw away all but 6500 inputs; only 1,000 inputs meet forwarding criteria; 10 inputs are normally selected by analysts and only one report is produced.

---

[36] Messages of activists intercepted, *Washington Post*, 13 October 1975. The TOP SECRET Sigint codeword during the 1960s was TRINE. The messages were marked TOP SECRET TRINE GAMMA, with a further designator. After a compromise, TRINE was replaced throughout the UKUSA network with UMBRA. (This codeword was in turn compromised in 1978, but was never replaced.)

[37] By the Paracel Corporation, as the Fast Data Finder chip.

> These are routine statistics for a number of intelligence collection and analysis systems which collect technical intelligence. [38]

In other words, for every million communications intercepted only one might result in action by an intelligence agency. Human eyes would see only one in a thousand of the messages. In one sense, the main function of Dictionary computers is to throw most intercepted information away.

Selecting messages for collection and processing is in most cases automated, involving large on-line databanks holding information about targets of interest. The selection process depends on large intelligence databases, supporting computers called Dictionaries. These contain tables of information related to each target. At their simplest, these can be a list of telephone, mobile (cell) phone, fax or pager numbers associated with targets in each group. They can include physical or e-mail addresses, names, or any type of phrase or concept that can be formulated under normal information retrieval rules.

Nicky Hager has described in detail the organization of the Dictionary computers used to support an ECHELON site and other stations run by the New Zealand Sigint agency, GCSB. The system controls what each station is searching for and who will be given access. Individual Dictionary computers at each site are programmed with search lists organized into specific categories. These lists are referred to by four digit numbers, which are used by analysts as shorthand to denote the subject that is being collected. The lists reflect tasks given to GCSB by the New Zealand government or by its Sigint allies. The agency then decides the categories to use, according to its responsibilities for producing intelligence for the network. For the GCSB this included the communications of South Pacific governments, Japanese diplomatic messages, and operations of Russian fishing boats and at Antarctic bases.

Each entry in the Dictionary will contain key words, telex, fax and e-mail numbers and communication "gateways". The key words may include organizations and people, country names and subject names. They will include all known telecommunications addresses for people who are specifically targeted. They also specify combinations of terms that can exclude unwanted communications. In principle, the operation of the Dictionary system is thus akin to using an orthodox on-line database, such as a newspaper archive. The difference is that what is searched is private communications, not public data.

Dictionaries implement the tasking of their host station against the entire mass of collected communications, and automate the distribution of selected raw product. They read through incoming messages. Whenever the address or contents match a search condition in one of the Dictionary's catalogue, it is selected and relayed to the remote requesting agency or organisations. The message is tagged with details including the date, time and site of interception. Finally the computer adds the four-digit code or "Dictionary number" in as a tag for the intercepted message before it is relayed and stored for subsequent retrieval. This system, devised by NSA, is in use throughout the global interception network.

---

[38] Address to the Symposium on "National Security and National Competitiveness: Open Source Solutions" by Vice Admiral William O. Studeman, Deputy Director of Central Intelligence and former director of NSA, 1 December 1992, McLean, Virginia.

The Dictionary thus holds the target list for each station, and is the practical implementation of its tasking priorities. Dictionary entries may be placed in each station's catalogue by allied agencies, as well as by its own operators. If so, the intercepted messages will not be seen by the country collecting them. Thus, for example, 80 per cent of the product of the Australian interception site near Geraldton in western Australia is never seen in Australia but is sent automatically as raw Sigint to the U.S. Australians do however supervise the contents of the Dictionary.

Dictionary computers are thus at the heart of UKUSA global Sigint production operations. They are found not only at ECHELON or other satellite interception sites, but also other stations that perform similar filtering tasks. A smaller and more transportable version is known as ORATORY. About the size of a small suitcase, ORATORY units were made for use in embassy collection operations, where processing requirements are limited and equipment space is usually at a premium. Plugged into wideband interception equipment, ORATORY filters and selects messages and phone conversations according to a built in and pre-programmed Dictionary catalogue.[39]

At the remote analysis sites to which messages are posted, the desired raw intercept can be selected from the mass of intercepted communications collected from the global UKUSA network. An analyst scrolling through a selection of intercepted traffic on a terminal may see messages collected by different sites and collection operations. It all works as one system.

Keyword recognition is fundamental to Dictionary computers, and to Sigint. Such processing is only possible when the content of a message is accessible and can be processed by computer. This is not possible with encrypted messages, nor with telephone calls. In these cases, a first stage of selection can only be made from "traffic data", such as the destination, source or routing of a message, and perhaps its timing.

Encrypted messages can readily be identified and selected, and may be submitted further downstream for cryptanalysis. Speech (telephony) is in some ways a larger problem. Developing systems for fully automated speech processing has been a holy grail for Sigint engineers for more than 40 years. It is a goal that has continued to elude the Sigint agencies. What has been developed and deployed since 1990 are speaker recognition modules that can be included in Dictionaries. These are programmed to recognise the personal speech patterns of particular target individuals. Press reports have attributed the tracking down of drug cartel leader Pablo Escobar in 1993, and the Turkish dissident PKK leader Abdullah Ocalon in 1999 to speaker recognition equipment supplied from NSA. Accounts from intelligence insiders vary as to how effective or reliable speaker recognition profiles are as a targeting method, but do not dispute that the technique is now standard and has been added to the catalogue of Dictionary targeting methods.

Many press reports have suggested that Sigint agencies are able to select telephone calls for interception by identifying key words in what is spoken. There is no evidence that such systems can function usefully in a multi-speaker, multi-language environment where numerous previously never heard speakers may each feature physiological differences, dialect variations, and speech traits.

Only one account from a first hand source has implied that Sigint agencies do have the capability to process telephone calls according to spoken key words. This claim

[39] Mike Frost and Michel Gratton, Spyworld, Doubleday Canada, 1994, pps 152-154.

was implied in the description of ORATORY published by former Canadian Communications Security Establishment manager Mike Frost in his book "Spyworld".[40] The six-inch high unit, he reported, could do "key word selection" in "voice, fax or teletype". Frost has recently clarified the context in which he recalled ORATORY's speech recognition capacity being used.[41] When loading the appropriate Dictionary elements into the portable box, NSA staff could pre-load recordings of sample spoken key words. But it was the speaker of the selected words who was being targeted. "You had to have the target saying the word", says Frost. If so, then it appears that ORATORY was targeting speakers, and only incidentally targeting words they might speak.

The contention that telephone word-spotting systems are readily available may appear to by supported by the recent availability of a string of low-cost software products. Although commercial voice recognition software can be purchased for personal computers, these are not analogous to the Sigint problem. They require one or more hours of training in order reliably to recognize a single speaker. Even then, the error rate may be high. Voice recognition programs also computationally demanding. This might not appear a problem to NSA, which operates its own custom microchip manufacturing plant, but it should be noted that contemporary telephony links may carry 50,000 or more simultaneous speech channels.

For Sigint, where the interception system has no prior knowledge of what has been said (or even the language in use), and has to operate in the poorer signal environment of a telephone speech channel, acceptable error rates remain unachievable. I have explained in an earlier report that even moderate error rates can make a keyword recognition system worthless by generating both false positive outputs (words wrongly identified as keywords) and false negative outputs (missing genuine keywords).[42]

When encryption or other problems restrict content-based analysis and message selection, traffic analysis ("TA") is an alternative approach. Traffic analysis is a method of obtaining intelligence from signal related information, such as the number dialled on a telephone call, or the Calling Line Identification Data (CLID) that identifies the person making the call. By analysing calling patterns, networks of personal associations may be analysed and studied. This is a principal method of examining voice communications. Traffic analysis is particularly effective in studying military communications, where the timing and pattern of message exchanges may allow analysts to deduce the hierarchy and command structures of their targets.

Powerful though Dictionary methods and keyword search engines may be, however, they and their giant associated intelligence databases may eventually be replaced by "topic analysis", a more powerful and intuitive technique, and one that NSA is developing strongly. Since 1992, the U.S. Defense Advanced Research Projects Agency (DARPA) has sponsored a series of conferences at which commercial and academic researchers have been invited to compete in developing computer techniques to

---

[40] *Ibid.*.

[41] Interview with the author, April 2000.

[42] Interception Capabilities 2000 (IC 2000), report to the Director General for Research of the European Parliament (Scientific and Technological Options Assessment programme office) on the development of surveillance technology and the risk of abuse of economic information. Duncan Campbell, April 1999. Available (in PDF format) at http://www.europarl.eu.int/dg4/stoa/en/publi/pdf/98-14-01-2en.pdf The report is one of four in a series on the "Development of surveillance technology and risk of abuse of economic information".

solve its problems in speech recognition and document classification. The National Institute of Standards and Technology (NIST) run the conferences. NSA has reported its own results from time to time at these open conferences. The agency has also obtained patents for the ideas it has described.

The first Text REtrieval Conference (TREC-1) was held in Gaithersburg, Maryland, from November 4-6, 1992. The eighth conference was held in November 1999. Among the new techniques that NSA researchers have reported to TREC conferences are "n-gram analysis" and "Semantic Forests". Both are forms of topic analysis. Topic analysis searches databases to answer questions formulated as "find me messages about a subject". Instead of listing keywords, the search system may be referred to a collection of other messages or reports that define the subject of interest.

N-gram analysis was developed in the early 1990s and has been patented by NSA.[43] This is a fast, general method of sorting and retrieving machine-readable text according to language and/or topic. The N-gram system is claimed to work independently of the language used or the topic studied. To use N-gram analysis, the operator ignores keywords and defines the enquiry by providing the system with selected written documents concerning the topic of interest. The system determines what the topic is from the seed group of documents, and then calculates the probability that other documents cover the same topic. NSA has offered the system for commercial exploitation, claiming that it could be used on "very large data sets (millions of documents)", could be quickly implemented and that it could operate effectively "in text containing a great many errors (typically 10-15% of all characters)".

In April 1997, NSA staff filed a further patent describing "Semantic Forests", said to be an invention for "automatically generating a topic description for text and searching and sorting text by topic". Text, however, did not mean that the invention was intended for sorting newspaper articles. In papers presenting the method to two subsequent TREC conferences, one of the inventors explained that "our primary interest, however, is in transcribed speech, where the text is imperfect … Semantic Forests was developed originally to work with imperfect speech recognizer transcripts."[44]

In describing the "background to the invention" in their 1997 patent application, the inventors explained the problems in searching automatically transcribed speech with keywords:

> Identifying topics of text has been an area of study for several years, and identifying such in unconstrained speech has been an area of growing interest. The latter of these two areas, however, seems to be more difficult since much of the information conveyed in speech is never actually spoken and since utterances frequently are less coherent than written language.
>
> The standard method of electronically searching for a document related to a particular topic is by using keywords. In a keyword search, a user selects a small set of words (i.e., the keywords) which may be expected to occur in documents related to the topic of

[43] Method of retrieving documents that concern the same topic, US Patent number 5418951, 23 May 1995; named inventor, Marc Damashek.

[44] Text Retrieval via Semantic Forests, Gregory D. Henderson, Patrick Schone, Thomas H. Crystal, TREC 7 Conference, November 1998; available from http://trec.nist.gov.

.

> interest. The documents are then searched for occurrences of the keywords. Documents containing the keywords are then presented to the user. A disadvantage of this method is that relevant documents that do not include the keywords will not be retrieved.

The authors of this paper identified themselves as working in the Speech Research Branch of the " Department of Defense" located at Fort Meade, MD. The Speech Research Branch is part of NSA's R (research) division. Their paper was filed under the title of nsa-dev.pdf. These and other NSA papers and patents strongly suggest that the state of the art in automatic speech processing is still under development, but that speech recognizer transcription systems are available. This would not be a surprise, but the critical question is their reliability for use in spotting message sor phone calls likely to be of interest. Unlike a conventional database or web search engine, the written accuracy of the information will be less than 100%, probably far less. High rates of false positive and false negative hits have been reported to make conventional information retrieval search methods all but useless. Adding to the difficulty of analyzing telephone calls, the information searched for may not directly be present in the conversation, unless examined in context and as a whole. One part of the Semantic Forests patent suggests pre-processing automatically transcribed speech to remove duplicated syllables or phonemes as so-called "stutter phrases". The method was designed to work universally "where the text may be derived from speech and where the text may be in any language".

The release of these papers and patents tends to confirm indications that NSA has abandoned attempts to select phone calls by reference to single spoken words ("keywords"), and that research is now focused on topic recognition. If an effective system of topic recognition is being built or has been built, this would be a major extension to the capabilities of the global surveillance network. Further, the capabilities of a deployed and effective topic analysis system would not only apply to solving the problem of targeting the contents of telephone calls. Topic analysis also works with large text databases. It would enable NSA to enlarge its surveillance of e-mail and the Internet by allowing Sigint analysts to target the topics U.S. citizens (and others) may discuss on overseas links, without targeting individuals.

ECHELON

ECHELON is the name for much of the UKUSA system for intercepting civilian and commercial communications carried by satellite. It is part but not the whole of the worldwide Sigint system. Like all NSA codewords, the term has no meaning in relation to its subject. It does not, in this context, have any relation to the conventional military meaning of formations or ranks.

The first steps towards ECHELON were taken in the mid or late 1960s. The plans followed closely on a 1964 agreement to establish an International Telecommunications Satellite Organization (Intelsat) to own and operate a global constellation of communications satellites, providing shared long distance and intercontinental links. By 1966, the first Intelsat satellites, Intelsat 2, were in orbit. The UKUSA organization resolved that all Intelsat links should be accessed and intercepted. Unlike the cables across the major oceans, the most important of which passed through a UKUSA country, and thus afforded access to all wired circuits, satellite links could cross-connect any two nations without regard to surface geography. The only way to intercept all the satellite traffic was for NSA and GCHQ secretly to build their own shadow ground stations.

Early in 1967, specialists from GCHQ visited the British Post Office's satellite communications station at Goonhilly Downs, in Cornwall, south west England. This was the British terminal of the Intelsat system. Staff at Goonhilly learned that the GCHQ team intended to build their own station at Morwenstow, near Bude, a town on the other side of the Cornwall coast. According to a newspaper report, the GCHQ engineers studied "the methods used … for handling telephone traffic … this will be the type of messages coming by way of the Bude station.[45] The report quoted the British Foreign Office as saying that the new station would provide satellite links to British embassies. This soon proved to be untrue.

Some time later, it emerged that GCHQ had had difficulty persuading the British treasury of the intelligence value of building an expensive new station with the sole function of intercepting western civil communications crossing the Atlantic and Indian oceans. They resisted paying for it until told that it was an NSA requirement. In July 1969, in a parting letter to Lieutenant General Marshall 'Pat' Carter, the retiring director of NSA, GCHQ Director Leonard Hooper explained how he had imputed American needs to get British funds to pay for the site and its two large dish antennae:

> I know that I have leaned shamefully on you, and sometimes taken your name in vain, when I needed approval for something at this end. The aerials at Bude ought to be christened "Pat" and "Lou"[46].

"Pat" was General Carter while "Lou" referred to the long-serving Deputy Director of NSA, Dr Lou Tordella. In another official letter to Carter sent a few days previously,

---

[45] *Times*, 2 February 1967

[46] The letters quoted here were deposited in the George C Marshall Research Library, Lexington, Virginia; and were found by and quoted in Bamford, *op cit*, p333. Sir Leonard Hooper refused to comment on the letters when approached by the *Sunday Times* in 1981. He appeared shocked by the public revelation of his personal messages - an ironical situation for an official who for 36 years previously had been employed to read other peoples' mail.

Hooper had asked Carter to convey good wishes to his successor Admiral Noel Gayler and "to assure him that we in GCHQ will do our best to assist NSA in continuing its great and important mission under his leadership". He added:

> Between us, we have ensured that the blankets and sheets are more tightly tucked around the bed in which our two sets of people lie ... Like you, I like it that way.

The two 30 meter diameter interception aerials at Bude came into operation soon afterwards, positioned prominently on high western cliffs of the Cornwall coast. One of the dishes pointed west, at the Atlantic Ocean Intelsat. The second pointed low to the east and its Indian Ocean sister. The tracking dishes pointed in the same direction as those at Goonhilly. The dishes were civil, not military equipment, bought from the same suppliers as legitimate Intelsat earth stations. Identical dishes could then have been seen around the world, in Hawaii, California or Italy.

Plans for the construction of a second site needed to complete global coverage were revealed in a Washington state newspaper in November 1970. The Department of Defense announced that it was constructing a "research station" in a remote northwestern district, 250 km from Seattle. No details were given about the purpose of the research, or about the part of the Defense Department was to run it. The proposed new station was to be built within the Yakima firing range, which the department already operated.

The Yakima station, now known to be an NSA civilian run field station, was initially equipped with a third large tracking dish to cover Pacific regional Intelsat communications. The station was codenamed "COWBOY"[47] and continues to function as NSA field station F92. The British station at Morwenstow was operated for GCHQ by its civilian field agency, the Composite Signals Organisation. Its codename may be "CARDIGAN".[48]

The overall codename for the NSA-GCHQ civilian communication satellite interception project at this time is not known reliably. What is known is that the ECHELON system was already in its second generation by 1981. A document from NSA's Menwith Hill field station prepared that year lists intelligence databases in use at the site as including ECHELON 2, as well as a number of others known as SIGMA.[49]

It is now clear that the use of automated Dictionary methods dates from these early days of communications satellite (COMSAT) interception. Although tiny by modern standards, the volume of the message traffic to be carried by each Intelsat 3 satellite made existing Sigint analytical methods untenable. According to some sources, NSA had already had a degree of success by 1970 in automating the processing of "record" or written communications through its early advanced computers, possibly including the IBM "Harvest" system. The need for efficient processing systems to replace human operators who performed watch list scans was necessitated by the development of the satellite interception stations handling many thousands of channels. Each nominal telephone channel could carry twelve telegraph or telex links. Thus, even the first satellite interception stations had to anticipate processing thousands of telegraph and

[47] Secret Power, op cit, Chapter XX
[48] Personal communication. The codename is said to be related to a large UK Sigint station, substantially funded by the U.S.
[49] IC2000 report (note 32), p13.

speech connections in simultaneous operation. Their response was to develop the Dictionary.

Two military sites that now function as part of the ECHELON system were also constructed in late 1970s. One was Sugar Grove, VA, until then an orthodox Naval long-range radio communications station, which was due to close. The base, in a remote part of the Shenandoah mountains 250km from Washington included a two storey underground operations building which had previously been associated with a large radio receiver complex. Following a 1978 inspection, NSA took the site over for a new satellite interception project operating under the codenames TIMBERLINE, LANFORD, LATERAL, and SALUTE. The Naval Security Group, the naval arm of the Central Security Service, thereafter operated three satellite-tracking dishes linked to these projects.

Also in 1978, NSA designed a new satellite interception station at Misawa, Japan. This was an existing USAF Sigint site that until then had focused on high frequency radio interception. The $700,000 project, codenamed LADYLOVE, included the first of a complex of satellite earth terminals and a new operations building. LADYLOVE was described in military appropriations applications as a "key element of an important electronic surveillance system which must be implemented to keep pace with current technology". Both stations were in operation by 1982. By this time, the interception capacity of the British and U.S. civilian run stations at both Bude and Yakima had doubled.

A third new U.S. satellite interception station was also developed in 1981, at Rosman, NC. Like Sugar Grove to the north, the Transylvania County station was located in a remote and electrically quiet region, surrounded by woodland. It was operated under civilian management as NSA field station F63. Some systems at Rosman were operated in common with the large British station at Menwith Hill. About 10 dish antennae were eventually deployed. The station has not been linked to the ECHELON network, however. Its targets were reputedly Soviet satellites crossing the U.S., rather than western satellites. It was closed in 1993 as part of NSA's reduction program.

By 1982, NSA had begun planning the global expansion of ECHELON. The enlargement project was known as P-415 by its principal contractor, Lockheed. It was planned from Lockheed's Western Development Laboratories in Palo Alto, CA. According to recently published contractor documents, Lockheed also oversaw the related project CARBOY II (also known as Project P-377). CARBOY II comprised a standard kit of "ADPE" (automated data processing equipment) software and hardware components for equipping a chain of Echelon sites. According to P-377 specifications and documents, the "commonality of automated data processing equipment (ADPE) in the Echelon system" included units that would break down satellite links into component parts of telephone and telegraph channels.[50]

The telegraphy components could be either analog or digital. Their output was fed to the "telegraphy message processing subsystem". Other ECHELON components were a "facsimile processing subsystem", a "voice processing subsystem", a "voice collection module" and a"[voice] Tape Production Facility". Written or "record"

[50] "Echelon P-377 Work Package for CARBOY II", published in March 2000 at http://cryptome.org/echelon-p377.htm

communications could be processed according to their full content and the desired targets of the watch list. Voice communications, however, could only normally be targeted by using the telephone numbers of known targets. If a number was recognized, the voice collection module would direct the call to the tape production unit.

CARBOY II's specifications for the ECHELON system also called for software systems to load and update Dictionary databases. At this time, the hardware for the Dictionary processing subsystem was based on a cluster of DEC VAX mini-computers, together with special purpose units for processing and separating different types of satellite communications. The implementation of these pojects, P-377 and P-415 completed the automation of the "watch list" activity of previous decades.

Details of Project P-415 and the plans for the expansion of the Echelon system were revealed in 1988 by Margaret "Peg" Newsham. Ms Newsham, a former computer systems manager, had worked on classified projects for NSA contractors from 1975 to 1984. [CH] From August 1978 onwards, she worked at NSA's Menwith Hill Station as a software co-coordinator. In this capacity, she helped managed a number of Sigint computer databases, including "ECHELON 2". She also helped establish "SILKWORTH", a system for processing information relayed from signals intelligence satellites. Her revelations led to the first ever report about ECHELON, published in 1988.[51]

From 1982 on in Sunnyvale, Ms Newsham worked on plans for project P-415 software. During her employment by Lockheed, she become concerned about corruption, fraud and abuse she believed was occurring in the organization's planning and operating electronic surveillance systems. After leaving, she reported her concerns to the House Permanent Select Committee on Intelligence early in 1988. She also told them how she had witnessed and overheard the interception of a telephone call made by a U.S. Senator, Strom Thurmond, while working at Menwith Hill.

By the mid 1980s, communications handled by Dictionary computers around the world were heavily sifted, with a wide variety of specifications available for non-verbal traffic. The network started to expand.

New stations

After 1988, the full details of Echelon would probably never have come to serious public attention but for six further years of research by New Zealand writer Nicky Hager, who investigated the new Sigint station that started operating at Waihopai on the South Island of New Zealand in 1989. His 1996 book *Secret Power*[52] is based on extensive interviews with and help from members of the New Zealand signals intelligence organization. It remains the best-informed and most detailed account of how Echelon works.

UKUSA plans to expand ECHELON, Hager revealed, date from a 1984 meeting of western Sigint chiefs in Wellington, New Zealand. The meeting was attended by then

[51] New Statesman (UK), 12 August 1988. At the time, Ms Newsham was a confidential source of information and was not identified in the article. In February 2000, living in retirement and facing a serious illness, Ms Newsham, said she could be identified as the original source of information on Echelon. She also appeared on a CBS television programme about Echelon, *Sixty Minutes* (shown on 27 February 2000).
[52] See reference 9.

NSA Director Lt-Gen Lincoln D. Faurer, Sir Peter Marychurch, head of GCHQ, and by their Australian and Canadian counterparts from DSD and CSE. The plans discussed at the Wellington summit started to surface in 1987, when both Australia and New Zealand announced plans to construct new "defense communications" stations.

Both countries were embarrassed when, during a 1988 visit to Australia, New Zealand's Defense Minister Bob Tizard revealed that the two new stations were not for military communications, but were intended to intercept civilian communications satellites launched by third world countries such as India and Indonesia. Construction began later that year at Waihopai, near Blenheim in New Zealand's South Island and at Kojarena, Geraldton, near Perth in Western Australia.

In New Zealand, as had happened in Britain 20 years before, it appeared that the Sigint alliance had secretly pressured a reluctant government into paying for them to access private satellite communications. In a foreword to Hager's book, former New Zealand prime minister David Lange said that much of the book's information had been a surprise to him, despite having been Prime Minister of New Zealand from 1984-89, and having taken the key decision which allowed the ECHELON project to go ahead. "It is an outrage that I and other ministers were told so little", he said. "This raises the question of to whom those concerned saw themselves ultimately answerable."

Lange said that he had grudgingly authorized the construction of the satellite monitoring station in an attempt to limit punishment inflicted on New Zealand by America and Britain after the country's "nuclear free zone" policy of the mid 1980s. "In the national interest it became necessary to say "ouch" and frown and bear certain reprisals of our intelligence partners". But he was not told that "we had been committed to an international integrated electronic network".

The new station at Waihopai came in operation late in 1991, just before the fall of the Berlin wall. Inside the global Sigint network it is designated as NZC333, and codenamed FLINTLOCK. It monitors the Pacific region by intercepting the ground signals from the commercial communications satellite Intelsat 701. A key target is Japan. Intelligence from the station goes to all the English-speaking intelligence agencies, including NSA and GCHQ. Staff working at the base say that 20% of the data intercepted is relayed to the U.S. without being examined in New Zealand.

Like other Echelon stations, the Waihopai installation is protected by strong security including double (in this case, electrified) fences, intruder detectors and infrared cameras. Despite this, Hager and a New Zealand TV reporter were able to enter the site in 1996, complete with a TV camera and a stepladder. Through high, incompletely shuttered windows, they filmed into and inside the operations center. They observed that the station was empty save for a security guard (at night) and that it operated completely automatically. Lights flashed on long racks of electronic equipment as messages were analyzed and sent on. A horseshoe row of computer monitors sat unattended, as the codeword "ENVOY" rotated round the otherwise blank screens. In part of their film, shown in 1996 on TV3 New Zealand, the camera zooms into a supervisor's desk, showing viewers that the manuals the New Zealand Sigint agency was using were indeed the manuals for the Intelsat satellite supplying communications to the South Pacific. Waihopai now has two domes containing dishes targeted on Intelsats.

According to Sigint sources quoted in *Secret Power*, GCSB produced Sigint end product at the rate of about 2000 a week. The sources also described the unequal nature

of UKUSA collaboration, claiming that while the U.S. has access to everything collected by allies, they do not share all they acquire. "The [intelligence] agencies can all apply for numbers on each other's Dictionaries. The hardest to deal with are the Americans. [There are] more hoops to jump through, unless it is in their interest in which case they'll do it for you".

A new satellite interception site was noted in 1999 in the British Eastern Sovereign Base area in Cyprus. Cyprus has been a major Sigint site for 40 years, principally directed at Middle Eastern communications. Further information about the new site, at Paramali, has not become available. If this station is also part of Echelon, it would be the tenth station in the network.

Australia's more extensive intercept facility near Geraldton, western Australia opened in 1993. It had (and has) four intercept dishes targeted on Intelsats orbiting above the Indian Ocean. Among the tasks contained in the Geraldton dictionary are ones related to North Korea's economic, diplomatic, and military situation, Japanese trade plans, and developments in Pakistani nuclear weapons technology. The Australian government has said that Geraldton is a fully integrated part of the global surveillance network, and in constant contact with all ECHELON stations. But they use a different (and undisclosed) codeword for the station. Australians also confirmed that Hager had correctly described the Dictionary method of targeting. Although most of the station's take was relayed automatically to the U.S., Australians controlled the tasking of the Dictionary, thereby retaining some oversight as to how the station was used. Although it is under Australian command, the station - like its controversial counterpart at Pine Gap, near Alice Springs (which downlinks U.S. Sigint satellites) - employs American and British staff in key posts.

Another Australian intercept site, at Shoal Bay near Darwin, Northern Territories began satellite interception operations in 1979, with two dishes targeted on Indonesian regional communications satellites called *Palapa*. Since then the station has expanded dramatically, with 9 satellite interception antennae in operation by 1999. Shoal Bay is not, however, part of the ECHELON network, as Australia refuses to share the raw intercepts with the United States and Britain. Indonesia is one of the world's most populous countries and most lucrative emerging markets. Australians do not trust either the U.S. or Britain not to exploit Indonesian Sigint from Shoal Bay for national political or commercial ends. During the 1990s, the station produced a great deal of intelligence on Indonesian dissident and separatist movements, particularly in East Timor. When Britain was trying to push through a controversial deal to sell fighters and other arms to Indonesia, staff at Australia's Office of National Assessments feared that the British would, if given the chance, hand over DSD intelligence on the East Timorese opposition to the Soeharto regime in order to win the lucrative contract.

The fifth partner in the UKUSA alliance, Canada's Communications Security Establishment (CSE) entered the satellite interception business in 1986, with the construction of the first of four terminals at their principal interception site, CFS (Canadian Forces Station) Leitrim, south of Ottawa. The station was substantially enlarged under a $30 million (Canadian) contract awarded in 1992, and now includes four radomes containing satellite terminals. The station also remotely controls other formerly manned Canadian interception stations.

Leitrim is linked directly to the U.S. Department of Defense communications network, and to NSA. "Communications Researchers" from Canada's military Sigint service, called the "Supplementary Radio System" work at Leitrim to analyze satellite communications patterns. Overall, 900 civil and military staff work for CSE.

Reports in the Canadian press have suggested that Latin American communications are a principal target of CFS Leitrim. The station is also said to have a large complement of Spanish linguists. Staff from Leitrim are also posted to the NSA's Regional Sigint Operations Center at San Antonio, TX which provides Sigint support to the U.S. Southern Command.

One of the acknowledged operations mounted from Leitrim, codenamed SANDKEY, targets the communications of narcotics traffickers from South America.[53] Brazil's aerospace company, Embraer, has recently been reported to be one of the targets listed in the Leitrim Dictionary.[54] Although the Canadian government has neither acknowledged nor denied participating in ECHELON, CSE budget data for 1995/96 identified the two largest items of capital expenditure for that year as $7 million (Can) for ECHELON and $6 million for Cray (supercomputers). No other explanation has suggested for CSE's ECHELON expenditures.[55]

Official identification of ECHELON units in U.S. government documents

In 1998 and 1999, the intelligence specialist Dr Jeff Richelson of the National Security Archive, Washington, DC used the Freedom of Information Act to obtain a series of modern official U.S. Navy and Air Force documents which have confirmed the continued existence, scale and expansion of the ECHELON system. The documents from the Air Force and Navy identify units at four sites and suggest that a fifth site also collects information from communications satellites as part of the ECHELON system.[56]

The first station to be confirmed as part of ECHELON was Sugar Grove. An upgraded Sigint system, TIMBERLINE II, was installed at Sugar Grove in the summer of 1990. At the same time, according to a declassified Naval Security Group Command history, an "Echelon training department" was established. With training complete, the first of the "specific functions and tasks" assigned to the station's commander in 1991 became "to maintain and operate an ECHELON site".[57] The second was to "[deleted – probably "collect], process and report intelligence".[58]

---

[53] Private communication from Dominic Patten.
[54] CBC (French language channel), *Zone Libre*, 12 May 2000.
[55] CSE Financial Status Report, 1 March 1996, released under the Freedom of Information Act.
[56] "Desperately Seeking Signals", Jeff Richelson, *Bulletin of the Atomic Scientists*, March-April 2000.
[57] Mission, Functions and Tasks of Naval Security Group Activity (NAVSECGRUACT) Sugar Grove, West Virginia, September 3, 1991.Naval Security Group Command Regulation C5450.48A, 8 August 1996.
[58] Some commentators have questioned whether the use of Echelon in upper and lower case type in parts of this and other US military documents might indicate that the word was not a codename but bore its ordinary military meaning. It is evident from the context of the documents that this is not the case; further, the word appears in capitals in the NSG instruction to Sugar Grove to "operate an ECHELON site" (sic). http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/09-03.htm. Other important documents relating to Echelon stations can also be found at the National Security Archive web site, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index2.html. An Air Force document referenced at

By 1994, other U.S. Naval Security Group stations had become part of ECHELON (if they were not already). Developments at these sites are described in the declassified official History of the U.S. Air Force Air Intelligence Agency. In a section entitled "Activation of Echelon Units", the history reports that in 1994 AIA, NSA, and NSG "drafted agreements to increase AIA participation in the growing [deleted][59] mission" and that AIA was to establish new detachments of the 544th Intelligence Group to accomplish this. The agreement referred to NSG sites in West Virginia, Puerto Rico, and Guam. It was noted that "AIA's participation in the [mission deleted] had been limited to LADYLOVE operations at Misawa AB, [Japan]".

In January 1995 "Echelon Units" were established at Sugar Grove, Yakima and Sabana Seca, Puerto Rico. They have continued to operate. The location and functions of these "Echelon Units" is described in editions of the 1998-99 Air Intelligence Agency Almanac[60], within the entry for the parent military unit, the 544th Intelligence Group, based at Peterson Air Force Base, CO. The group began operations in September 1993 and now employs 500 personnel around the world to "deliver global, space related information to national agencies and military commands".

These AIA and 544th IG documents define the mission of Detachment (Det) 3 of the 544th IG, located at Sugar Grove. The mission statements precisely characterize the station's operations as being a COMSAT satellite interception system. They identify the mission as:

> To provide enhanced intelligence support to Air Force operational commanders and other consumers of COMSAT information …
>
> to direct satellite communications equipment supporting research and development for multi service national missions …
>
> to direct satellite communications equipment [in support of] consumers of COMSAT information ... this is achieved by providing a trained cadre of collection system operators, analysts and managers…
>
> to provide AIA a highly trained cadre of personnel to capitalize on emerging technologies to meet consumer requirements and to establish itself as a leader in the COMSAT environment by remaining on the cutting edge well into the 21st century.

In 1990, satellite photography showed that there were 4 antennae at Sugar Grove field station. In 1998, a ground visit by a TV crew revealed that this had expanded to nine. All were directed towards the southeast, taking advantage of both local topography (a valley on that alignment) and legal restrictions on radio transmissions in the area. The satellites being intercepted from Sugar Grove are therefore over the Atlantic Ocean, providing communications to and from the Americas as well as Europe and Africa. From this, it is inevitable that communications links terminating in the U.S. are being

---

http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/12-03.htm also refers to "Activation of ECHELON units'(sic).

[59] The details of the mission were redacted, but the words "civilian communications" have been suggested as fitting the obscured area.

[60] http://www.fas.org/irp/agency/aia/cyberspokesman/97aug/544ig.htm

intercepted at Sugar Grove. This issue is recognized in the NSG regulations, whose third directive to the station commander is to "ensure the privacy of U.S. Citizens are properly safeguarded pursuant to the provisions of USSID 18".[61] The site histories also record a series of inspection visits by NSA's General Counsel, suggesting that operations at Sugar Grove may be regarded as unusually sensitive.

Detachment 2 of the 544th IG is located within another Naval Security Group field station at Sabana Seca, Puerto Rico. According to the AIA documents, its mission is to "[perform] satellite communications processing and forwarding, identifying emerging technologies, maintaining clear communications" and "to become the premier satellite communications processing and analysis field station in the Department of Defense". The mission statement adds a further goal:

> [To] develop an unmatched capability to identify variations in a rapidly changing communications environment and apply this resource as an integrated part of Department of Defense information operations into the 21st century.

Again, the mission statements characterize the station's operations as being a COMSAT satellite interception system. Detachment 2 was officially activated on Dec. 8, 1995. In 1999, the Sabana Seca field station appeared to have at least four radomes for satellite communications, one located beside an existing high frequency interception system targeted on Cuban radio communications.

Det 4 of the 544th IG at NSA's Yakima field station was also activated on 1 January 1995. It has not published its mission statement. Detachment 5, said to be located in Washington, D. C. was activated on 5 December 1995. This detachment may be located at Fort Meade.

The 544th IG has also published a group mission statement of an unusually political (if garbled) character:

> The 544th IG envisions a multipolar world political situation with continued multiple contingencies. Economically, the country faces continued budget constraints. Technologically, the 544th IG sees a space based future of integrated architecture with a focus on information operations.

Questions were raised in the U.S. and Europe about the precise tasking of ECHELON and the 544th were raised after a Danish newspaper[62] published details of an unclassified industry briefing that the group placed on the Internet in 1999.[63] Entitled "Our Changing World", this was a slideshow featuring 25 different images. After detailing the 544th's operating locations in the U.S., Europe, and Japan, the slides portrayed the group's job as "fishing" for Comint and other intelligence, to pass it on to regional sigint centers. One slide mentioned "Lots of Small Ponds in lots of locations". Two slides then displayed the "fish", with the comment: "A lot of new FISH, in a lot of unfamiliar ponds. They are mobile, diverse, and technology has made them advanced". The images and captions displayed "hackers … disgruntled employees … Non-government organizations … Red

[61] For information about USSID 18, see page 51 onwards.
[62] *Ekstabladet*, 8 March 2000.
[63] The pages, formerly at http://www.aia.af.mil/homepages/cc/inddays/544_indu were removed after the article was published.

Cross". The millennium bug was also mentioned. One photograph showed Red Cross teams in action.

Challenged that the "fish" slides indicated that NGOs including the Red Cross were Sigint surveillance targets, AIA public affairs officer Major Joe Mecadon, denied this:

> The slide in no way, shape or form identifies NGOs as intelligence targets …any information related to specific intelligence targets, sources or methods is classified, so information of that type is deliberately excluded from unclassified materials.[64]

This answer is inconsistent with the character of the slides displayed. The second slide of "fish" for the 544th depicted Hussein, Milosevic, and Bin Laden. Other slides mentioned "multi-level access", "comm[unication]s pipes" and "1st Echelon reporting". Despite the partial denial, the slideshow was clearly intended to depict the diversity of Sigint targets at which intelligence systems like ECHELON were being directed.

Foreign and private Sigint

Apart from operations within the UKUSA alliance, U.S. communications passing by satellite or radio can be and are intercepted from overseas sigint sites. These communications are also within reach of private corporations and even amateur enthusiasts who have sufficient knowledge and motivation to run their own Sigint operations. The largest is Russia's FAPSI (Federal Government communications and information agency), which operates a chain of Sigint sites within Russia, and overseas at Cam Ranh Bay, Vietnam and Lourdes, Cuba.[65] The Lourdes facility has been depicted in U.S. overhead reconnaissance pictures released by the Department of Defense. These photographs show two "space-based electronics" areas with satellite reception equipment to receive the downlinks from U.S. satellites. The CIA has warned U.S. journalists that their telephone numbers are likely to be targeted by the Russian version of the Dictionary system operated at Lourdes. More recently, China has been rumored to have acquired its own Sigint facilities in Cuba.

The technical department of the French espionage service, DGSE, operates a major communications satellite collection site at Domme, in the Dordogne valley to the east of Bordeaux, in south-western France. This site, which includes at least 11 collection antennae, seven of them directed at Atlantic satellites, is clearly as extensive and capable as the largest sites in the UKUSA network. DGSE has also been reported to operate further satellite interception facilities in New Caledonia, and in the United Arab Emirates. DGSE and the Germany intelligence service BND have also been reported to collaborate in the operation of a COMSAT collection site at Kourou, Guyana, targeted on "American and South American satellite communications".[66] During 1999, two small European nations (the Netherlands and Denmark, the latter being a "third party" in the UKUSA system) revealed that they were intercepting communications from civilian

---

[64] Setting The Record Straight - Air Force Agency Does Not Admit to Spying on Red Cross, ABC News Online, 31 March 2000

65. Sword and Shield : The Soviet Intelligence and Security Apparatus, Jeffrey Richelson, Ballinger, Cambridge, Massachusetts, 1986.

66. Les Francais aussi ecountent leurs allies, Jean Guisnel, *Le Point*, 6 June 1998.

satellites. The Swiss intelligence service also announced plans to build two Comsat interception stations.[67] It has also been reported that, in the late 1980s, staff from China were being trained in ECHELON operations in California.[68] China and the U.S. secretly co-operate in operating two monitoring sites in western China.

Unencrypted phone calls, data and faxes sent by satellite are thus vulnerable to interception and exploitation both within and outside the ECHELON network. The technical and financial cost of unauthorized access to Intelsat links is low. In 1993, the author filmed a demonstration of Intelsat interception techniques. Within less than an hour of setting up, we were able to overhear U.S. conversations over one of the Intelsat Atlantic satellites.[69]

Although little is known of private or corporate use (and abuse) of satellite Sigint, the ease with which this can be done has been demonstrated with skill and humor by a German engineer, who uses the sobriquet "Dr Dish".[70] Reporting in TELE-Satellite International magazine and on the Internet, Dr Dish described in October 1996 how had intercepted satellite faxes and phone calls from Nigeria that appeared to relate to corrupt and criminal activities. In another article, he described setting up his own fax interception system.[71] He was able to solve the problem of "blind" fax interception more quickly and simply than New Zealand's Sigint engineers, however. By 1997, commercial fax interception systems had become available.

Extended coverage

Although not part of ECHELON, the UKUSA network also collects Sigint from international communications cables. In the UK, transatlantic submarine cables land at Widemouth Bay close to Morwenstow on the Cornwall coast. A microwave link also appears to connect the communications station to other cable terminals further south, at Lands End. Separately, all international telex links and telegram circuits passing in, out or through the country were and are connected to a GCHQ monitoring site in central London, known to the Sigint network as UKC1000. A 1991 British television program reported on the operations of the Dictionary computer at GCHQ's London station in Palmer Street, Westminster. The program quoted GCHQ employees, who spoke off the record about why the work carried out on the building's fourth floor was performed by security-vetted staff employed by a private company, British Telecom:

> It's nothing to do with national security. It's because it's not legal to take every single telex. And they take everything: the embassies, all the business deals, even the birthday greetings, they take everything. They feed it into the Dictionary."

67. *Intelligence* (Paris), 93, 15 February 1999, p3.
68 See note 51.
69 "The Hill", Shown on Britain's Channel 4 *Dispatches*, 8 October 1993. The demonstration was filmed on rented land adjacent to NSA's Menwith Hill Station. Ironically, the US conversations intercepted were military, apparently passing via a transponder leased to the defense communications system.
70 See http://drdish.com .
71 http://drdish.com/features/spy_18.html

Starting in 1990, GCHQ also obtained illegal access to the international communications of the Irish republic, which (save for satellite connections) was then linked to the rest of the world by a microwave system from Dublin to Manchester in northern England. The link across England and Wales was tapped at the mid-point between two relay towers. The interception site, officially labeled an "Electronics Test Facility", was a windowless 150-ft high tower. Inside the $30 million tower were eight floors of hi-tech electronics, three floors of aerial interception galleries, a domestic area for its round-the-clock operating crew, and extensive air conditioning. The interception antennae on the top floors of the tower were concealed from view behind opaque white fiberglass panels.

From 1990 until 1998 the tower at Capenhurst, Cheshire intercepted the international communications of the Irish Republic crossing from Dublin to Anglesey on a newly installed optical fiber submarine cable, called UK-Ireland 1. A major part of the purpose of the tower was to watch for terrorist communications connected with the IRA. If these were the only communications desired, the project could have legally been authorized under UK law. But the UK's major common carrier, British Telecom, did not regard the plan to trawl all Irish communications as clearly lawful, and refused to provide direct access. As had happened at Morwenstow two decades earlier, GCHQ had to construct its own station to obtain comprehensive access to traffic. The revelation of this facility led to diplomatic protests to Britain by the Irish government, and to an action in the European Court of Human Rights by Irish civil rights groups.[72] In Canada, communications are intercepted from cables leaving its Atlantic and Pacific shores, or as they pass through the Trans-Canada microwave system. Foreign circuits on these systems are believed to be intercepted by CSE. In the U.S., most Atlantic cables are accessible in New Jersey or New England.

Although NSA's interception operations should be limited by its "one foreign terminal" rule, the direct interception of some U.S. domestic links is permitted. Embassies and some other premises on U.S. territory are nevertheless as foreign territory, and their communications may be targeted or intercepted without a warrant. Another NSA operation identified to EPIC but unconfirmed by other sources is the alleged direct interception of cables from Washington, DC to New York, passing by way of NSA's Fort Meade headquarters. This project is said to be named OCCUPIER. If the allegation is correct, it would not breach FISA for NSA to do this, provide that only foreign traffic was intercepted. Since many diplomatic premises in Washington DC communicate extensively with their UN missions in New York, the intelligence justification for such a project is apparent. But screening and scanning a major U.S. communications artery would obviously raise the possibility of NSA's acquiring a large volume of incidentally intercepted traffic of interest. Even if this example is treated as hypothetical only, it further illustrates the opportunities for NSA's further encroachment into U.S. communications.

The capacity of ECHELON and related satellite interception sites described above amount in total to at least 60 systems in simultaneous operation. The true total may be much higher, as systems formerly targeted on Soviet satellites may have been re-assigned to civilian communications interception missions. These could include two large projects at Menwith Hill, England (MOONPENNY) and Bad Aibling, Germany (GARLICK).

[72] Lodged in May 2000.

Some commentators have argued that the increasingly common practice of utilizing focused "spot beams" from communications satellites to provide much smaller "footprints" has necessitated a much wider global spread of satellite interception stations. This speculation may not be correct. Many of the sites are located in radio quiet areas, and may have larger antennae or higher gain equipment than the normal standard. Technically speaking, all of the communications within the spot beam will be receivable, at some intensity, anywhere on the earth's surface that the satellite is in view. It may not even be necessary to use high quality Sigint equipment. For example, "Dr Dish" has reported finding no difficulty intercepting a West African Intelsat 601 spot beam (intended for Nigeria) from the Netherlands

Some capabilities of the global surveillance system have been exaggerated. A 1998 report about Echelon[73] credited the system with the capacity to intercept "within Europe, all e-mail, telephone, and fax communications". This has proven to be overstatement; neither Echelon nor the Sigint system of which it is part can do this, not least because Europe's internal landline communications would be difficult to access. Nor is it plausible that equipment is available (or affordable) with the capacity to process and recognize the content of every speech message or telephone call. But the American and British-run network can, with sister stations, access and process much of the worlds international communications, analyzing and relaying the raw product to customers who may be continents away.

[73] "An appraisal of technologies of political control", report for the European Parliament Scientific and Technological Options office (STOA) by Dr Steve Wright, Omega Foundation, Manchester, UK, January 1998.

CONGRESS INVESTIGATES

The Echelon project was already more than five years old when the Senate asked Senator Frank Church to lead the first-ever detailed study into the abuse of constitutional rights by U.S. intelligence agencies. When his enquiry began, in January 1975, there had been no press reports or legal indications of NSA's misdeeds. So far as NSA was concerned, the committee started with a blank sheet. The agency's very existence, let alone its operations or their domestic impact, was virtually unknown to press, public or the legislature. Prior to 1972, the little that the U.S. public knew about NSA could be found in a single book - David Kahn's The Codebreakers, published in 1967.[74] The book was published despite opposition from NSA, which read the text before publication and required parts to be removed. Kahn's book gave no indication or account of NSA's then contemporary activities affecting U.S. communications.

In the same year, a Supreme Court case on wiretapping, *Katz*,[75] gave fundamental guidance on the construction and effect of the Fourth Amendment, and led to the establishment of legal standards for domestic wiretapping within the United States. In 1968, Congress enacted the Omnibus Crime Control and Safe Streets Act. Title III of the Act defined standards for the use of wiretaps by the police and FBI. But it also wholly exempted NSA's intelligence activities on traffic to and from the U.S. from the new controls, stipulating that:

> Nothing contained in this chapter … shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications (emphasis added) [76]

At the same time, the position of common carrier international operators who gave NSA access to their traffic was potentially protected by exempting them from the provisions of § 605 of the Communications Act 1934,[77] which ordinarily guaranteed privacy to anyone communicating to or from the U.S.:

> No person receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof

Section 2511(3) of Title III exempted "national security" surveillance from these provisions:

> Nothing contained in this chapter of in Section 605 of the Communications Act of 1934, 47 USC § 605, 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

---

[74] David Kahn, The Codebreakers: The Story of Secret Writing, Macmillan, 1967.
[75] *Katz v United States*, 389 US 347.
[76] 18 USC § 2511(2)(f).
[77] 47 USC § 605.

> essential to the security of the United States, or to protect national security intelligence information against foreign intelligence activities.[78]

In all these statutes, the meanings of "national security" and "foreign intelligence" remained undefined. Even "foreign intelligence" remained wholly undefined for a further 10 years. All of NSA's practices - whether proper and improper - thus remained unaffected by the Title III changes.

A brief first public insight into NSA came in 1972, when a former USAF Security Service analyst described his experiences with NSA in *Ramparts* magazine.[79] Using the pseudonym "Winslow Peck", the analyst alleged that NSA was engaged in the wholesale interception of international telephone calls:

> Q. So far we've been talking about various kinds of sophisticated electronic intelligence gathering. What about tapping of ground communications?
>
> *A.* I'm not sure on the extent of this, but I know that the NSA mission in the Moscow embassy has done some tapping there. Of course all trans-Atlantic and trans-Pacific telephone calls to or from the U.S. are tapped. Every conversation, personal, commercial, whatever is automatically intercepted and recorded on tapes. Most of them no one ever listens to, and after being held available for a few weeks, are erased. They'll run a random sort through all the tapes ..., listening to a certain number to determine if there is anything in them of interest to our government worth holding on to and transcribing. Also, certain telephone conversations are routinely listened to as soon as possible. These will be the ones that are made by people doing an inordinate amount of calling overseas, or are otherwise tapped for special interest.

A second interview with a former NSA employee, published soon afterwards in Australia, gave a few further details[80]. A third, written by a former U.S. Navy Sigint operator, appeared in *Rolling Stone.* But even these dissenters' accounts failed effectively to lift the lid on the use of Sigint to monitor U.S. citizens and political activities. NSA's "compartments" were too watertight for these three of its own staff to have learned anything of the improprieties elsewhere in the organization.

The compartments remained watertight even as a new administration took over following the resignation of President Nixon. New cabinet members apparently remained ignorant of the precise methods NSA used to obtain overseas communications to and from the U.S. It appeared to members of the Church Committee that "the Attorney General did not know about the [CIA] mail openings until 1973 and the NSA interceptions until 1975".[81] The Committee's final report also indicated that, even as President Nixon and Attorney General Mitchell debated and encourage the expansion of

---

[78] 18 USC § 2513.

[79] Electronic Espionage: A Memoir, interview with "Winslow Peck", *Ramparts*, Vol. 11, No. 2, August, 1972, pp. 35-50. Available at http://jya.com/nsa-elint.htm

[80] Uncle Sam and his 40,000 snoopers, *Nation Review*, Australia, 5 October 1973. Available at http://jya.com/nsa-40k.htm.

[81] The National Security Agency and Fourth Amendment Rights, Hearings before the Select Committee to Study Government Operations with Respect to Intelligence Activities, US Senate, Washington, 1976, p121. (Attorney General Richardson was informed about the NSA Watch List activity (although not the specific means by which US citizens communications were being acquired) in the fall of 1973.)

domestic intelligence surveillance within the U.S., including the later notorious "Huston plan", they were never made aware of how NSA actually gathered its information.[82]

The 1975 Congressional enquiries began when President Ford created the Commission to Investigate Central Intelligence Agency Activities Within the United States, better known as the Rockefeller Commission. Also in 1975, Congress created the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the Church Committee) and the House Select Committee on Intelligence (the Pike Committee). In time, these became the contemporary permanent intelligence committees of the House and Senate that sit today.

The Rockefeller Commission was charged only with investigating the CIA and its involvement in monitoring domestic political dissent. NSA was not within its remit. They came across much evidence, and some incidental information about NSA, that would prove fundamental to the reforms of the late 1970s. But neither they, nor their successors led by Pike, Church and later Abzug[83], uncovered NSA's activities in any systematic way. In the face of systematic opposition, reports went unpublished, hearings were postponed or cancelled, and a grand design for an intelligence legislative program finished with one bill passed.

In particular, even though what we now know as the ECHELON project (and which probably bore the codename at that time) was well under way, no hint of this NSA capability emerged in any testimony. It was not until 5 years later, when James Bamford's *The Puzzle Palace*[84], revealed the existence of NSA's Yakima Research Station (and the British co-operation at Morwenstow), that there became available a sketch of the likely nature of the civilian satellite communications monitoring system.

This was despite a stream of press reports from mid-1975 on, alleging "NSA eavesdrops on virtually all cable, Telex and other non-telephone communications leaving and entering the United States, and uses computers to sort and obtain intelligence from the content".[85]

Former Church committee staffer L Britt Snider, now Inspector General of the CIA, has recently recounted how for months in early 1975 he and his colleagues had no leads at all to follow.[86] Casual or even direct enquiries to NSA provided the investigators with no clue to suggest that NSA's tentacles spread far more widely than tracking the radio signals of the Soviets or their allies. Neither cleared staff on the Hill nor a selection of ex-NSA employees approached informally had any idea about NSA's support to domestic intelligence activity or the sources from which it was drawn.

---

[82] Intelligence activities and the rights of Americans, Final Report, of the Select Committee to Study Government Operations with Respect to Intelligence Activities, US Senate, Washington, 1976, pps 111-116.

[83] New York Representative Bella Abzug chaired the Subcommittee on Government Operations and Individual Rights of the House Committee on Government Operations. Her committee conducted a fourth round of enquiries in 1976.

[84] James Bamford, The Puzzle Palace: A Report on America's Most Secret Agency, Houghton-Mifflin, 1982.

[85] National Security Agency reported eavesdropping on most private cables, *New York Times*, 31 August 1975.

[86] L Britt Snyder, Unlucky Shamrock – Recollections from the Church Committee's investigations of NSA, CIA *Studies in Intelligence*, Winter 1999-2000, CIA, 1999 (unclassified edition). Available at www.odci.gov/csi/studies/winter99-00/art4.html.

It was only by happenstance that the Church Committee staff found a lead to follow four months after they began, when a copy of the CIA's so-called "family jewels" study was presented to them. (This was a compilation of known or potentially improper activities which all CIA staff had been required to report by the new director.) Buried in 800 pages of potential abuses by the CIA were two tiny references to NSA. One noted that the NSA had obtained an office in New York from the CIA in order to copy telegrams. The second noted that CIA had asked for NSA helping in monitoring the communications of some U.S. citizens involved in the antiwar movement.

On 6 August 1975, CIA Director William Colby acknowledged NSA's general activities to the Pike Committee. Asked if NSA monitors "telephone calls between American citizens and foreigners abroad, Colby replied "the agency does monitor foreign communications … communications that are abroad or go abroad cannot be separated from the traffic that is being monitored".

> Representative Aspin: Does it involve a U.S. citizen at one end?
>
> Colby: On some occasions, that cannot be separated from the traffic that is being monitored It is technically impossible to separate them."

Pressed as to whether the interceptions were continuing, Colby declined to answer unless in executive (closed) session. Aspin said afterwards that he regarded the practice as a "very, very clear violation of the First and Fourth Amendments".

Late in August, six months after their enquiries began, Church's staff were finally briefed about the telegram copying operation, project SHAMROCK. The program had been terminated in May, Snider was told, by order of the Secretary of Defense. This was the same moment that the Church committee had found out about it:

> I asked if the Secretary had ended it because he knew the committee was on to it. "Not really," he said, "the program just wasn't producing very much of value.[87]

Two days later, NSA Director Lieutenant General Lew Allen, Jr., appeared before the Pike committee in closed session, together with his deputy Benson K. Buffham. He testified that "NSA systematically intercepts international communications, both voice and cable. Messages to and from American citizens have been picked up in the course of gathering foreign intelligence".[88]

According to a staff member who attended the closed sessions of the Pike hearings, General Allen was asked by committee members to testify further about NSA's interception methods. The staff member's recollection was that no information was given that U.S. domestic sites involved in wire or satellite interception, but that two sites in the UK did collect such information, one being Menwith Hill in England. Although the NSA station at Yakima had by then been in operation for several years, neither this activity nor "Echelon" was reportedly mentioned to the committee.

The Rockefeller Commission issued its report on 6 June 1975, five months after the Church Committee had been formed. The Pike report was never published. Completed on 19 January 1996, the House voted to suppress it 13 days later. It was

[87] *Ibid.*

[88] The testimony was published later, when Pike's final report was leaked.

however leaked to CBS newsman Daniel Schorr and given to the *Village Voice*, who republished it in full as a special supplement that fall.[89] Under the heading "Interception of International Communications", the Pike Report repeated that NSA "

> systematically intercepts international communications, both voice and cable … NSA officials concede that messages to and from American citizens and businesses have been picked up in the course of gathering foreign communications intelligence. They maintain, however that these messages are small in number and usually discarded in any case.

The report disclosed a letter that General Allen had sent to Chairman Pike on 25 August 1975. He said he wished to clarify his earlier testimony, adding that:

> At the present time, the telephone calls of U.S. citizens in the United States are not being monitored. The monitoring of telephone conversations of United States citizens in the United States has never been authorized by NSA. Currently, we are not now monitoring any telephone circuits terminating in the United States

In its first and third sentences, this testimony appears to contradict prior testimony by CIA director Colby as well as by General Allen himself. Consistent with NSA's history of concealing its methods and operations from Congress and even senior officials of the Executive Branch, his account omitted reference to the character of the operations at Yakima, as well as to the directly relevant input to NSA from its integrated satellite interception operations with GCHQ at Morwenstow, Cornwall. The suggestion that NSA was not "at the present time" monitoring telephone calls to or from the U.S. could only have been true, if the agency had turned off all access to telephone channels, direct or indirect, for the period in which the letter was written and presented – or at least were not listening to any product. By omission, the letter also acknowledged that NSA (and GCHQ) were conducting surveillance of, written, wires, telegraph, telex or "record" communications.

Allen's letter also acknowledged that until 1973, NSA had specially monitored certain radio-telephone circuits from the U.S. and "some foreign countries". The calls were searched for the names or phone numbers. The circumstances relating to this admission had by then been described in the press. It refers to interception of radio-telephone links to South America from the Naval Security Group intercept station at Northwest, VA. The interception was begun at the request of the Bureau of Narcotics and Dangerous Drugs, who in 1970 had requested NSA's assistance in targeting Americans via the Watch List.

The Church Committee

By September 1976, Church committee staff had learned the full details of SHAMROCK from NSA's retired deputy director Lou Tordella and then from NSA itself. Starting in 1945, NSA and its predecessors had systematically obtained cable traffic from the offices of major cable companies - RCA Global, ITT World

[89] The Pike report was reprinted in book form by the Bertrand Russell press, Nottingham, England, 1977.

Communications and Western Union. Over time, the collection of copies of telegrams on paper was replaced by the delivery of magnetic tapes and eventually by direct connection of the monitoring centers to international communications circuits. From 1966 until 1973, the CIA had assisted in the operation by renting office space in Manhattan.

The total telegram and telegraph traffic from the U.S. at this time was about 72 million message a year. According to Church committee [90], NSA analysts selected about 150,000 messages a month to review (1.8 million message a year, or about 1 message in 40). "Thousands of these messages in one form or another were distributed to other agencies".

Formal hearings into NSA were scheduled for early October. They were cancelled following intense pressure from the administration. In a last minute phone call from President Ford to Chairman Church, the President asked for the committee's findings on SHAMROCK, NSA and the Watch List to stay secret. Church declined, and the committee voted to defer while hearing representations from Attorney General Levi in closed session. The committee reportedly heard "no arguments or excuses it hadn't heard before". They resolved to go ahead, despite continued strong opposition to holding any open hearing by ranking minority member Senator John Tower.

NSA Director Allen attended Congress on 29 October 1975 to testify on for the first time in public. He confirmed that NSA had no constitutional authority or charter, and that its activities stemmed solely from Presidential authority. The Secretary of State for Defense, responding to a Presidential instruction, had directed the formation of the agency in 1952. NSA's fundamental document at the time was a National Security Council Intelligence Directive, NSCID-6. So far as the law on American's communications was concerned, NSA's position was that Congress had imposed no prohibition on what it did:

> While NSA does not look upon Section 2511(3) as authority to conduct communications intelligence, it is our position that nothing in Chapter 119 of Title 18 affects or governs the conduct of communications intelligence for the purpose of gathering foreign intelligence.[91]

Although neither the Presidential directive of 1952 nor NSCID-6 defined the meaning of "foreign communications", he explained, NSA operated a "one foreign terminal" rule. "NSA has always confined its activities to communications involving at least one foreign terminal". Despite this, "many unwanted communications are potentially available for selection".

Gen Allen described how NSA used "'watch lists" as an "aid to watch for foreign activity of reportable intelligence interest". After first accepting requirements for intelligence on foreign influence or presence in antiwar or black power groups from the Army intelligence in 1967, a "consolidated listing" of U.S. citizens' names began in 1966 and was fully implemented by 1970.

From 1967 until 1973 (when the watch list activity ceased) U.S. citizens appeared in four target categories.

---

[90] Intelligence activities and the rights of Americans, *op cit*, p60.
[91] *Ibid*, p8.

Under the heading of "international drug trafficking", 450 U.S. and 3000 foreign names were supplied by the BNDD. The FBI asked for intelligence on 1000 U.S. and 1700 foreign names, concerning persons who were alleged to be "active in civil disturbances" or to be terrorists. The Defense Intelligence Agency passed on 20 names of U.S. citizens who had traveled to North Vietnam. The CIA asked for intelligence on 30 U.S. and 700 foreign organizations and groups categorized as "extremists".

The lists were used by NSA to select the international communications of such citizens from its systems, including the telegrams provided by SHAMROCK. NSA had begun doing this in the early 1960s on a limited basis in order to monitor U.S. citizen travel to Cuba and threats to the President. In 1967, however, the list was expanded to include the names of U.S. citizens involved in antiwar and civil rights disturbances, ostensibly to determine any foreign influence over such persons. In 1973, at the height of this activity, the names of 600 U.S. citizens were on the list. In the fall of 1973, however, in response to concerns about its legality, the "watch list" program was terminated.

On 1 July 1969, NSA had established Project MINARET as a "sensitive Sigint operation", governing the dissemination of "communications concerning individuals or organizations involved in civil disturbances [and] anti-war movements/demonstrations".

Under the category of Presidential protection, 180 and 525 foreign names were added to the lists. In total, the list of U.S. citizens whose communications were targeted amounted to 1650, of whom 450 appeared only on the narcotics list.

During the period 1967-1973, Allen stated, NSA had produced and disseminated 3900 reports, of which 2000 had concerned narcotics. Some 1100 pages of data had been supplied to the CIA's illegal domestic intelligence operation, CHAOS. NSA had placed unusually severe restrictions on the reports. They formed a special series apart from NSA's normal reporting, and were normally hand carried to specified recipients. The reports concealed that they were from NSA, and were not identified with the agency.

During Allen's testimony in October 1975, neither he nor the committee revealed details about SHAMROCK. But its name was mentioned after Allen finished testifying, by Senators opposed to the release of the SHAMROCK report. Again, President Ford telephoned the Chairman and other members of the Committee "imploring them to reconsider".[92] The Committee voted to ignore the President's objections and to publish the report, naming three companies who had handed over their telegrams. According to Snider (whose subsequent life remained close to or in the intelligence community):

> It remains to this day the only occasion I know of where a Congressional committee voted to override a presidential objection and [to] publish information the President contended was classified.

On 6 November 1975, Church read the SHAMROCK report into the committee record. Although the Attorney General gave evidence that day, the executive branch refused to allow witnesses to testify on the subject.

Five months later, the Department of Defense suddenly "discovered" new documents about SHAMROCK. They revealed that the operation had not been limited to telegraph offices in New York but had included others in Washington, San Francisco, and San Antonio. They revealed that the telegraph companies had been concerned for years

[92] Snider, *op cit.*

about the legality of their cooperation. In 1947, the companies had sought assurances from the President, Attorney General, and Secretary of Defense that their participation in SHAMROCK was essential to the national interest and that they would not be subject to Federal prosecution. According to Snider, "the documents showed that Secretary of Defense James Forrestal, stating that he was speaking for the President, had met with representatives of ITT and RCA in December 1947 and provided such assurances, but with a warning that he could not bind his successors in office".

In June 1948, Forrestal tried to have Congress amend section 605 of the Communications Act of 1934 to make the SHAMROCK activity clearly legal:

> [Forrestal] met informally with the Chairman of the Senate and House Judiciary Committees to explain the situation, and an amendment was drafted to accomplish the objective. The amendment was never reported by either committee … The Senate Judiciary Committee voted to allow the Chairman discretion to report the amendment to the floor or not, but, because of the Defense Department's reluctance to have the matter discussed on the floor, the amendment was never reported out by the Chairman.[93]

The issue of whether or not the government and wire companies had broken section 605 of the Communications Act (or whether the exemption in Title III would protect them) was never tested. A case was brought, but remained untried. The new information arrived after the Church committee formal enquiries had closed. There was no new investigation of SHAMROCK. NSA's kindred (and continuing) activities remained concealed from view.

Congress mounted one final attempt to examine NSA's interception of American communications, through Bella Abzug's Subcommittee on Government Operations and Individual Rights, of the House Committee on Government Operations. Her committee staff prepared a report on "Interception of International Telecommunications by the National Security Agency". In February 1976, she cited "circumstantial evidence" that NSA was continuing to intercept international telegrams, despite the termination of SHAMROCK on 15 May 1975. Her committee summonsed four current or former FBI staff and one NSA member in an attempt to extract further information. They appeared - but all said that they had been directed by superiors not to testify. The committee cited them for contempt of Congress, without effect. In March 1976, representatives of the cable companies did testify to the committee. But the committee's staff report on the "Interception of International Telecommunications" was never published, although it was later leaked to the press.[94]

Between 1975 and 1977, a U.S. Department of Justice task force investigated possible criminal offences committed by NSA and those with whom it worked on the MINARET project. The Top Secret report was completed in June 1976. No action was taken. Although classified Top Secret, in 1980 a redacted copy was released under the Freedom of Information Act to U.S. author James Bamford. Shortly thereafter, the U.S. government stated that the report had been inadequately redacted and attempted, unsuccessfully, to have it withdrawn. The report noted that MINARET intelligence:

---

[93] *Ibid.*
[94] NSA invades Americans' privacy, *Washington Post*, 14 May 1979.

was obtained *incidentally* in the course of NSA's interception of aural and non-aural (e.g., telex) international communications and the receipt of GCHQ-acquired telex and ILC (International Leased Carrier) cable traffic (SHAMROCK)" (emphasis in original).[95]

In August 1977 Detroit attorney Abdeen M. Jabara sued the FBI and became the first and only American to force disclosure of the scale and extent of NSA surveillance directed against him. FBI targeting of Jabara had begun in 1967, and had continued through 1973. In the course of this, NSA supplied the FBI with the contents of 6 overseas telephone calls or telegrams sent by Jabara.[96] He also learned that NSA had disseminated the data to 13 federal agencies and three foreign governments. Jabara later temporarily won orders preventing the NSA from targeting his communications, by any means, and compelled the FBI to remove the material from his files.

The shutters now came down firmly on NSA's activities. A 1978 suit by 27 anti-war activists was thrown out. The next year, Jane Fonda and her husband Tom Hayden were refused access to their own illegally gathered messages on the grounds that these were "sensitive and properly classified" by NSA.[97] In 1982, *New York Times* correspondent Harrison Salisbury also failed in a similar suit against NSA. Jabara's suit was also eventually blocked. In 1995, Mr. Jabara said he was still angry "Basically, I believed we had a Bill of Rights and a Constitution. ... simply because I was involved in something unpopular was no reason they should be able to violate my privacy".[98]

The Foreign Intelligence Surveillance Act

With the enquiries behind them, Congress took its first - and only – step towards legislative control of the intelligence agencies. Prior to Watergate, most presidents had claimed to hold implicit constitutional authority for warrantless surveillance for national security purposes, under the executive branch's power to conduct foreign policy. Following the exposure of the abuses by the CIA, FBI and other agencies many in Congress wished to place clear limits on these surveillance powers.

Anxious to forestall a move to outlaw warrantless surveillance entirely, the Ford administration offered a new bill, S-3197, which would limit the "inherent authority" hitherto claimed by the President to conduct warrantless surveillance in the name of national security. The bill offered to require warrants in some circumstances.

But S-3197 proved unpopular in the Senate and did not pass. Had it done so, NSA would have faced no restrictions at all on intercepting the international communications of U.S. citizens or organizations, as the agency would have retained unbridled authority (as authorized by the President and tasked by other government departments or agencies) to continue intercepting and conducting warrantless surveillance on all outgoing communications to and from the U.S. Since it was never alleged during the Pike, Church

[95] Bamford, *op cit*, p000.
[96] NSA tapped six overseas messages by attorney for Sirhan, FBI reveals, *Washington Post*, 3 August 1977.
[97] Appeal by Miss Fonda and Hayden for data on selves is rejected, *Washington Post*, 30 October 1979.
[98] Catching Americans in NSA's net, *Baltimore Sun*, 12 December 1995. The report, by Scott Shane and Tom Bowman, formed part of a series published that year. Their series comprises the best-informed reporting about NSA for almost 20 years (since Bamford).

or Abzug investigations that NSA had conducted domestic interceptions,[99] this would have amounted in practice to no legal restriction at all.

The new and revised bill introduced under the Carter administration as S-1566 remedied this but retained the same focus on domestic communications. Senate Judiciary and Intelligence Hearings took place on S-1566 in 1977 and 1978. Opening the Senate Select Committee on Intelligence hearings in July 1977, Chairman Birch Bayh hailed the bill as "an important first step towards full-scale legislative regulation of the intelligence services of our country". He added that he hoped to move on provide

> further measures not only to clarify the authority and structure of the intelligence community but also to place clear legal limits on the full range of intelligence activities which may affect the rights of Americans.

For its purposes, the bill defined "electronic surveillance" as covering communications made by U.S. citizens or permanent resident aliens within the United States, and their international communications to and from the United States (unless these were wire messages, carried by radio). But the incidental acquisition of communications about or to or from U.S. citizens in the U.S. through international communications was not protected, provide that the person concerned was not targeted. To target such persons or their communications would require a special warrant procedure, on application to a court sitting in camera to hear *ex parte* applications.

This, the Foreign Intelligence Surveillance Court (FISC), was to be constituted by FISA in order to meet the intelligence agencies' claims that ordinary judges sitting in ordinary courts could not safely or competently handle national security issues. Applications to the court have to be certified by the Attorney General before submission. To grant a warrant, the court must be satisfied that probable cause has been shown that the proposed target is a foreign power, an agent of a foreign power, or is engaged in sabotage or terrorism. "International terrorists" can be considered as a foreign power. The FISC was not required to consider whether the target's conduct was or was likely to be criminal, although the statute permitted the Attorney General to retain or disseminate for law enforcement purposes incidental material "that is evidence of a crime which has been, is being, or is about to be committed" (emphasis added). No standard was set for the severity of a crime that thus became reportable.[100]

In case the court rejected an application, FISA also created a Foreign Intelligence Surveillance Appeals Court. A further procedure allows applications to be referred on to the Supreme Court. But the FISA Appeals Court has never been asked to sit.

As the Senate Intelligence Committee hearings started, Chairman Bayh highlighted the bill's most important feature as the clamp it placed on Presidential power as it affected U.S. citizens while in the U.S. The new law, without exemption, defined the "exclusive means by which electronic surveillance [as the Act would define it] may be conducted". But he still expressed misgivings about the reach of S.1566.

---

[99] The Army Security Agency, which later became part of the Central Security Service under NSA control, had conducted domestic surveillance operations during the 1968 Democratic National Convention. Also, then as now, NSA regarded communications from foreign embassies in the US as being foreign, even if links were entirely within the US.

[100] 18 US § 1801(h)(3).

> In my judgment there is still room for the President to claim inherent authority to target Americans abroad for surveillance and to use information about Americans acquired directly from surveillance of international communications ... Until Congress enacts legislation in this area, the foreign intelligence surveillance activities of the Executive Branch will continue to raise serious problems for the rights of Americans.

NSA, he noted, "has a massive capacity to monitor communications … most of what NSA does is not covered by this bill" [101]

His argument was correct. Three months later, a particularly well-informed report in *Science,* later carried in the *Washington Post*[102] reminded their audiences of the "little-known but long-standing" practice" of the NSA in intercepting foreign cable and satellite links from the U.S. Writer Deborah Shapley pointed with sagacious accuracy to the U.S. phone calls that were relayed by the Intelsat earth stations at Etam, West Virginia and Goonhilly Downs, England. "The signals could be picked up in their entirety by another receiving station … a land-based receiver in England", she wrote.

But there was no fresh evidence, and no first-hand sources. Congress was enmeshed in its own battle to get FISA through. FISA was approved by Congress and signed into law by President Carter on 25 October 1978. [103] Executive Order 12139 which he signed a few months later, officially chartered the FISC. FISC hearings now take place behind cipher-locked doors in a windowless, electronically shielded courtroom, on the top floor of the Department of Justice. Since 1995, it has also been empowered to grant warrants for secret physical searches – the so-called "black bag jobs" of the 1960s and 70s.[104]

The court comprises seven federal judges chosen from the district courts by the Chief Justice of the Supreme Court. Each serves for a non-renewable seven-year term. The chief judge of the FISC, Judge Royce Lamberth of the U.S. District Court for the District of Columbia was formerly an assistant U.S. Attorney. In 1980, Royce had represented the Army in a lawsuit brought by 21 Americans formerly living in Germany and who had been wiretapped by Army intelligence agents. At the time, the Army promised to bring in regulations requiring a warrant to be issued before conducting electronic surveillance on Americans living overseas. There is no evidence that this was ever done.[105] The NSA and CIA have recently consulted Lamberth extensively over powers to extend electronic surveillance inside America in the interests of "critical infrastructure" protection.[106]

Notoriously, the reduced standards of the FISC court (compared to Title III applications) have led it consistently to issue more surveillance warrants than the balance of the federal judiciary.[107] The numbers of FISA warrants issued is reported annually to Congress, but without amplifying detail. The reports chronicle a steady growth in

---

[101] Bayh warns on surveillance in US, *New York Times*, 20 July 1977.
[102] 9 and 10 October 1977.
[103] 50 USC § 1801 *et seq*.
[104] Executive Order 12949, 13 February 1995.
[105] Army agrees to rules on wiretaps of Americans living abroad, *Washington Post*, 5 April 1980.
[106] See Madsen, note 6;comments by Judge Lamberth at the Critical Infrastructure Protection Conference of the American Bar Association, Standing Committee on Law and National Security, July 15, 1998.
[107] Patrick S. Poole, Inside America's Secret Court: The Foreign Intelligence Surveillance Court, Free Congress Foundation, 1999.

surveillance orders. During 1999, FISC approved 886 warrant applications, a record number. The numbers have been rising steadily since the early 1980s, when an average of 500 warrants were approved annually. But almost none of these warrants are issued to NSA, according to the current Director:

> Since the enactment of the FISA in 1978, there have been no more than a very few instances of NSA seeking FISA authorization to target a U.S. person in the United States. In those instances there was probable cause to believe that the individuals were involved in terrorism.[108]
>
> How frequently does this take place? It's difficult for me to talk about specific examples, but on average fewer than a half a dozen times per year. And you recall the instance of FISA court applications against American persons as I defined them inside the United States, significantly fewer times than that. Now, that's intentional targeting of American persons.[109]

It would follow from this that 99 per cent of FISC warrants have been applied for and obtained by the FBI. Thus, in most of the cases where NSA intentionally targets the communications of a U.S. citizen who is in the U.S., the targeting will consist of Comint support requested by the FBI. The figure involved – 500-800 warrants a year – is comparable to the number of U.S. citizens who were targeted by the FBI and NSA in the watch list activity of 1967-1973. Under FISA, however, the agencies are required to show probable cause that their target is an agent of a foreign power (or an alternative qualifying category). It is impossible to test whether the law is now applied properly and constitutionally. All details of FISA warrants are classified, sealed and secret.

The history of investigations and legislation in the 1970s suggests that relevant and critical information about collection systems may have been previously withheld from Congress. The investigational committees of 1974-1978 were led to believe that they had to deal with and protect the Constitution only in relation to a single program of intercepting outgoing telecommunications from the United States which had ceased 3 years before the Foreign Intelligence Surveillance Act (FISA) was passed (SHAMROCK). But other programs of a larger, more intrusive and broader character were under way before, during and after these hearings. They continue to this day, and have been significantly enlarged.

[108] House Permanent Select Committee on Intelligence, Hearing on Legal Standards of electronic surveillance, 12 April 2000, written statement submitted by Gen Hayden.
[109] *Ibid*, testimony by Gen Hayden.

Electronic surveillance: 1980 and after

Organizational culture inside NSA started to change in 1973, after growing public concern alarmed the new head of the agency. Director Allen questioned the wisdom of continuing some of its operations in the political climate of the time, and brought the watch list activity to a final end by October 1973. Seen with hindsight, the story from then until the end of the decade was one of damage limitation, making minimal and guarded disclosures (where possible in secret), and fighting to preserve the authority for what it did to remain entirely within the discretion of the executive branch.

Damage limitation extended especially to sacrificing one questionable operation (SHAMROCK) so that its successors (ECHELON and similar overseas wire taps) might continue and flourish. To the extent that the scale and character of these operations were suspected, no facts were permitted to emerge. This was public relations management, not the protection of national security. By the canons of Sigint security, the damage was done when Director Colby alluded to the scale of NSA interceptions, and many press reports[110] followed up with detailed assertions now known to be correct. In 1975, serious enemies of the U.S. would have deemed the reports true in any event and acted accordingly to protect their communications (if they had not done so previously).

NSA's damage limitation policy was a success. New legal controls on the intelligence agencies began and ended with FISA. FISA, as discussed above, hardly makes a difference. Its only bite on NSA operations as they were conducted before 1973 is to require the Attorney General (not the FISC) to issue a certificate authorizing the targeted interception of a U.S. citizen who is outside the U.S. FISA itself imposed no controls or rules on what NSA did with mountains of "incidental" interception that might concern U.S. citizens. It did however set out minimization procedures (such as replacing the name of an innocent person who inadvertently came under FISA-authorized surveillance with the words "U.S. person").

Even before 1973, NSA had not operated in a constitutional void, without policies on the gathering and dissemination of information about U.S. citizens. NSA policy and practice is codified in a library of U.S. Signals Intelligence Directives (USSIDs), covering every aspect of administration and operations from office security to planning targets for nuclear weapons. USSID 18, entitled "Limitations and procedures in Signals Intelligence Operations of the USSS", has been in existence since at least 1976 (although this was almost certainly a revision of earlier editions of a similar document).

In January 1978, President Carter restructured and redefined the policies and functions of the U.S. intelligence community in Executive Order 12036. This was superseded on 4 December 1981 by Executive Order 12333 issued by President Reagan. EO 12333 has not been revised or amended since then. Its principal terms affecting NSA are reproduced at Appendix 1. In the absence of explicit statutory authority or legal charter, it is this executive order and its predecessors that grant and have granted NSA authority to collect, process and disseminate signals intelligence for national foreign intelligence purposes, or in support of military operations.

[110] Cited above.

By 1980, NSA's activities were also governed by a DoD directive, 5240.1-R, on "Procedures governing the activities of DoD intelligence components that affect United States persons". The first date of issue of this directive is unknown. The current version was issued by the Reagan administration in December 1982. Procedure 5 of DoD 5240.1-R governs "Electronic Surveillance in the United States for Intelligence Purposes".

These, plus a classified annex prepared and circulated by NSA, are the two critical documents that now govern NSA procedures in relation to U.S. citizens.[111] The classified annex has never been released, in whole or in part. Appendix II includes the section of DoD 5240.1-R, Procedure 5, dealing with Sigint activities. The classified annex to the directive apparently specifies how NSA should handle untargeted and incidentally collected messages.

> Foreign communications. The United States Signals Intelligence System may collect, process, retain, and disseminate foreign communications that are also communications of or concerning United States persons, but only in accordance with the classified annex to this portion.

USSID 18, which is the standard directive used by Sigint staff handling information affecting U.S. citizens, is based on both these documents. It was reissued on 24 October 1980, and is classified "Secret – Handle Via Comint Channels Only". It was revised several times during the 1980s. A redacted version has been released under FOIA.[112] NSA has denied the existence of a revised version of USSID 18 to researchers who have requested it, but acknowledged in April 2000 that a revised edition was issued in 1993.

The purpose of the 19-page directive, with 9 annexes, is to "ensure that the missions and functions of the United States SIGINT System (USSS) are conducted in a manner that safeguards the constitutional rights and privacy of U.S. persons". Separate sections deal with collection, processing, storage and dissemination of U.S. person specific information. According to NSA Director Lt-Gen Allen

> [USSID 18] takes … statutes and executive orders and turns them into a specific cookbook that can be understood by every 18- or 19-year-old airman, soldier, sailor or Marine who comes to work for the National Security Agency.

Much of the released version of USSID 18 has been redacted, particularly sections that deal with processing and storage. Three of the specific categories allowing the release of citizens' identities in SIGINT have been redacted from the publicly available version. USSID 18 also specifies "policies and procedures [in relation to the] maintenance of data bases that may relate to U.S. persons". This information also remains classified.

USSID 18 confirms the position as it stood following the enactment of FISA. Electronic surveillance to gather foreign intelligence information within the United States may only be directed at U.S. citizens if a FISA warrant has been issued. Outside the U.S., no warrant is required. In these circumstances, NSA or other agencies can apply to

---

[111] Executive Order 12333, Intelligence Activities, 4 December 1981; and Department of Defense Regulation 5240.1-R., Procedures governing the activities of DoD intelligence components that affect United States persons, December 1982.

[112] Available at http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/07-01.htm.

the Attorney General for approval a certificate. This procedure is not merely warrantless, but – unlike FISA warrants – is unreported as to its scale. Testifying about this issue for the first time in April 2000, NSA Director Allen gave no details of the extent of authorized NSA surveillance of Americans who travel or live abroad.

The guidelines set by USSID18 say that if it incidentally obtains a communication from or to or about a U.S. citizen or organization in the United States for which there is no warrant or court order, the agency can retain the message but must remove the name of the citizen or company. But there are many exceptions to this, several of them classified - the name or other details can be retained if NSA analysts believe the information is "necessary to understand foreign intelligence information or assess its importance", if it indicates that a crime is being or had been committed, or if the intercept indicates that the U.S. person appears to be "an agent of a foreign power."

Whistleblowers or others who leak government information can be tracked and reported on, despite NSA's fundamental mission is to procure only foreign intelligence. NSA regulations permit the dissemination of the communications and identities of U.S. persons if "the communication or information that is being reported indicates that the U.S. person may be engaged in the unauthorized disclosure of classified information."

Another exception is made for law enforcement. According to USSID 18, "dissemination of information derived from foreign communications that includes an identification of a U.S. person may be made if … the communication or information is evidence that a crime has been, is being, or is about to be committed, provided that dissemination is for law enforcement purposes."[113] In these circumstances, information that is examined as a result of a broad search for foreign intelligence may be seized and used for law enforcement purposes. No standard is set of severity for the crime disclosed, in contrast to Title III domestic wiretapping. However, NSA says the procedure is infrequently used, with incidentally acquired information being passed to law enforcement agencies only on the specific authority of the Director. This is said to have happened on 18 occasions in 16 months in 1999-2000.[114]

1997 and after

Between 1976 and 1999, Congress never again returned to the questions about the National Security Agency and Fourth Amendment Rights that had occupied the Church and Abzug committees. But the issue started to surface in the U.S. after increasing concern in the late 1990s, particularly in Europe, about ECHELON. The rising profile of electronic surveillance in Europe and then in America followed the publication of a European Parliament report on "The Technology of Political Control".[115] Publicity for this report introduced a wide audience for the first time to information about the global surveillance network that had first been reported in 1988, and enlarged by the New Zealand book, *Secret Power.* In December 1998, I was asked to prepare a second report on the "Development of surveillance technology and risk of abuse of economic

[113] USSID 18, Limitations and procedures in signals intelligence operations of the USSS, 8.1 j (1980 edition).
[114] Testimony to HPSCI by Lt-Gen Michael Hayden, Director of NSA, 12 April 2000.
[115] See note 53.

information". The report was published in May 1999 and presented to the European Parliament in February 2000.[116]

In the U.S., the issue was enlarged when the House Permanent Select Committee on Intelligence (HPSCI) asked NSA to provide copies of its legal memoranda concerning electronic surveillance and U.S. citizens. The initial concern of Chairman Porter J. Goss was not merely that the memoranda might appear too permissive of NSA's activities; his concern was also that that they might be too restrictive. Surprisingly, and damagingly (for them), NSA refused to respond, claiming the documents to be protected by attorney-client privilege.

This cut short shrift in the House. In the committee's report in May 1999, Goss issued a public reprimand to the agency. He wrote that NSA's basis for withholding the memoranda was "unpersuasive and dubious", adding that if NSA attorneys "construed the Agency's authorities too permissively, then the privacy interests of the citizens of the United States could be at risk". NSA supplied the documents– about 100 memoranda, manuals, letters and cables dated from 1993 to 1999 - to HPSCI several months later. Meanwhile, Representative Bob Barr had expressed concern that NSA was covering up the scale, nature and impact of its surveillance activities, including ECHELON. Barr attached a requirement to the Intelligence Authorization Act for the year 2000 intelligence budget, requiring NSA to produce a report on the legal standards employed by elements of the Intelligence Community in conducting signals intelligence activities, including electronic surveillance. The requirement passed, and was signed into law by President Clinton in December 1999, as Section 309 of the Intelligence Authorization Act for FY2000.

The Director of NSA, the Director of the CIA, and the Attorney General submitted NSA's report on "Legal standards applied for electronic surveillance" to Congress on 1 February 2000. Classified appendices, said to contain little or no further substantive information, were attached to the report. The five-page report set out NSA's authority and procedures broadly as they are described in the documents mentioned above. But the report gave no details of the numbers of U.S. citizens affected by its electronic surveillance, or of the scale of its intrusions.

The report received little attention. But NSA became apprehensive about increasing publicity and concern about its operations. The concern that had spread to the U.S. was highlighted by the planned broadcast of CBS *60 Minutes* segment on Sunday 27 February 2000. Although the broadcast contained no new information about Sigint activities, NSA took a unique step for the once utterly secretive agency. They sent personal letters to every member of Congress. Kenneth A. Heath, NSA's chief of staff for legislative affairs, wrote that:

> We want to assure you that the NSA's activities are conducted in accordance with the highest constitutional, legal and ethical standards, and in compliance with statutes and regulations designed to protect the privacy rights of U.S. persons.

[116] Interception Capabilities 2000, April 1999, available at http://www.europarl.eu.int/dg4/stoa/en/publi/pdf/98-14-01-2en.pdf.

The agency also attached a "frequently asked questions" list, intended to provide reassurance, posing questions such as "Who is a U.S. person?" or "Couldn't the Agency simply ask its allies to provide them with information about U.S. persons?" The list was also published on its web site.[117] An oversight chart depicted NSA as being continually supervised by a network of six executive and legislative organizations. As to ECHELON, the Chief of Staff stated that:

> As is long-standing policy within the United States intelligence Community, we must refrain from commenting on actual or alleged intelligence activities; therefore we can neither confirm nor deny the existence of specific operations (emphasis added).

As with the report to Congress three weeks earlier, Heath's letter did not address questions about how new technology issues, such as e-mail, had affected its methods and procedures, but asserted that "the Fourth Amendment transcends whatever technology happens to be involved in a particular form of electronic surveillance". This provoked the rebuke, in a letter from Representative Barr, that NSA's position "grossly oversimplifies the difficulty of protecting privacy in light of recent technological advances". Barr also highlighted the weakness of relying on Executive Orders in regulating and authorizing NSA activities:

> An Executive Order can be rewritten or revoked on a moment's notice, whereas legislative restrictions are more permanent. As past NSA abuses have shown, privacy rights are better protected by relying on an evolving, explicit legal structure than by counting solely on the good faith of government employees wielding massive power and reciting generalities.[118]

Barr announced that he had secured the agreement of the Chairman of the House Government Reform Committee, Representative Dan Burton, to hold hearings into ECHELON, NSA surveillance and the privacy issues they raised. "Such a comprehensive review would build far more public confidence in [the NSA] and its vital mission than simply offering pat assurances that the privacy rights of Americans are being protected".

For HPSCI, Chairman Goss announced that the intelligence committee would schedule its own hearing on the same issues. This was held on 12 April 2000. For the government, the witnesses were CIA Director George Tenet, NSA Director Hayden, and Frances Fragos Townsend, counsel for intelligence policy in the Office of Intelligence Policy and Review, of the Department of Justice. Under light questioning, NSA's position extended little beyond "pat reassurances" from Gen Hayden:

> We are required to guard American privacy at every step in the intelligence process. That's usually divided up into four categories collect, process, analyze and report. And I need to emphasize to the committee that guarding American privacy is, at each point in that step, not merely in the finished intelligence product. The law requires us to do everything we can to prevent touching American privacy even at the very front end of that process, in the collection.

---

[117] www.nsa.gov:8080.
[118] Letter to Lt-Gen Hayden, Director of NSA, 28 February 2000.

USSID 18 and U.S. citizens

It is possible to examine the proposition that privacy is "guarded at every step" in more detail. Using the Freedom of Information Act, EPIC obtained from NSA copies of the legal advice memoranda that HSPCI had demanded from the agency in the spring of 1999. These documents describe NSA policy, relay case-by-case decisions, and set out its rules and regulations concerned with collecting, processing and identifying information about U.S. persons in Sigint materials and products. They identify NSA's internal departments that issue guidance and take decisions about the release of U.S. identities. Many of the documents are concerned with training staff to understand USSID 18, which NSA acknowledges to be complex and, as new situations arise, necessarily incomplete. The guidance is issued by NSA's Office of General Counsel (OGC), which also has attorneys working within the NSA Directorate of Operations.

In NSA's favor, the documents do not suggest that the agency sets out deliberately to disobey clearly enacted provisions or directives. Many show that its staff were carefully introduced to, reminded of and taught about USSID 18 and FISA. Regular training courses are held. The scale of the dissemination of U.S. identities is monitored and reviewed. But the results of such reviews, and the numbers involved, are classified. The key problem, however, is not with the nature of NSA's compliance with existing regulations, but with abundant flaws, loopholes, and interpretations that mean that compliance with regulations cannot be equated with support for the letter and spirit of the Constitution.

General NSA policy distinguishes between "FISA surveillances" and "non-FISA surveillances". FISA surveillances are those that target U.S. citizens either in the U.S. (with a FISC warrant) or outside the U.S. (requiring only the approval of the Attorney General. While there are reportedly few FISA warrants issued directly to NSA, many others (issued to the FBI) may call for support by the NSA. NSA is specifically authorized to support the FBI on request, and may provide personnel, equipment or knowledge to the FBI to gather foreign intelligence or counterintelligence. [119] In cases where personnel or services are supplied, the FBI must hold a warrant or the approval of the Attorney General, as required by the circumstances. Non-FISA surveillances constitute the balance (and majority) of NSA activities, where no specific limitations are imposed by the Act.

Under FISA, U.S. citizens may give NSA consent for the monitoring of their communications in specified circumstances. Even where consent is offered, the Director of NSA must authorize the surveillance. Such occasions appear rare. The NSA documents disclosed indicate that only one such consensual surveillance occurred between 1993 and 1998. Consent for monitoring can also be deemed to be given in a few specified situations. The example most commonly quoted is if U.S. citizens are taken hostage abroad. In such circumstances, NSA will deem that it has consent to monitor and pass on communications to, from and about them.

The rules for handling the material obtained in each case are different. FISA surveillances impose strict rules laid down by Congress, because of the high likelihood

[119] USSID 18, Annex B; see also EO 12333.

that surveillance of U.S. citizens, especially in the U.S., will create consequential intrusions into many other citizens' privacy. The "minimization" rules in this situation are statutorily required, and are contained in USSID 18.[120] They were most recently updated by Attorney General Reno in 1997. Rules for handling "inadvertently" or "incidentally" obtained U.S. person information in non-FISA surveillances are less strict.

The rules require that staff monitoring FISA electronic surveillances "shall destroy inadvertently acquired communications of or concerning a United States person at the earliest practicable point in the processing cycle at which such communication can be identified". There are two principal exceptions - if the communication contains "foreign intelligence information", or if it contains evidence of a crime. Other exceptions are listed, but have been deleted in the released versions of the document. NSA has also withheld details of the rules for the acquisition, processing and retention of such information. "Incidental" information about U.S. persons not the target of a FISA surveillance are thus more likely to be removed early in the system, because the material can be quickly judged as to its relevance in relation to the principal and authorized U.S. target.

The general rule in USSID 18 is that U.S. identities should be removed from NSA end product Sigint reports unless "such information is necessary to understand the foreign intelligence or assess its importance". In such cases, the principal information that NSA analysts are asked to remove from their reports is detail of "U.S. persons" or "U.S. identities". U.S. persons means citizens, permanent resident aliens, U.S. registered corporations, and also U.S.-registered ships and aircraft. It would normally include associations or non-governmental organizations headquartered in the U.S., unless these were held to be or to represent a foreign power. It does <u>not</u> include associations or non-governmental organizations (NGOs) whose headquarters are outside the United States unless "<u>a substantial number</u> of the members are U.S. citizens" (emphasis in original). U.S. citizens who work with or for non- corporations or international non-governmental organizations thus have diminished protection. According to the regulations, any non-incorporated corporation may be targeted or reported on (without outside authority), irrespective of whether or not its employees within the U.S. or elsewhere are U.S. persons.

The documents released under FOIA demonstrate that handling such "incidental" information is an everyday occurrence. As might be expected, it appears that such information is collected frequently as the result of NSA's tasking and targeting of foreign individuals, organizations, or of general subjects of intelligence interest. Collecting U.S. information of this type is routine, and has necessitated complex and frequent guidance to staff on methods and procedures. The documents also indicate that a large amount of the U.S. person-related information gathered by NSA is passed on in some form.

"Non-targeted or 'incidental'" surveillance of international communications from, to or about U.S. citizens occurs frequently. This has necessitated much legal guidance from in-house attorneys to NSA staff about the status and handling of the "incidental" interception of specifically cited U.S. citizens. For example, in authorizing the dissemination of reports concerning the First Lady in 1993, NSA counsel warned staff: "as with other senior officials of the Executive Branch, no reports may be published concerning Mrs. Clinton's private life or activities absent evidence of criminal

[120] USSID 18, Annex A, Appendix 1.

wrongdoing."[121] Other specific guidance has been issued concerning communications of, or about, former President Carter.[122]

NSA may also report on U.S. politicians, political parties and candidates. According to a 1996 NSA directive concerned with that year's elections, "oral and written dissemination [of details of a particular U.S. person, political party or candidate] can occur … [in] instances when references to political parties and candidates will be necessary to understand foreign intelligence or assess its importance".[123]

Among the documents released is a 1994 manual entitled "U.S. Identities in Sigint."[124] Like many others, this document is classified "Secret - Handle Via Comint Channels Only." All of the specified circumstances in which U.S. citizens' identities and information may be reported have been redacted. NSA has also concealed information about its "Identity Rules" within this handbook, even though many of these rules are marked therein as unclassified.[125]

It appears from this handbook that hundreds of different U.S. non-governmental organizations can be intercepted and reported on in NSA reports. NSA has withheld the contents of the eight-page list that states the agency's "List of approved generic references [to] U.S. identities that might appear in traffic". It is apparent that this table contains approximately 400 different "generic" ways that NSA can refer to specified U.S. organizations and entities in their finished reports.

Normally, NSA's processing and dissemination system does not involve the release of "raw" sigint data. Instead, the information obtained from intercepted messages is "gisted", replacing the full contents with a summary of the principal points and meaning. Contextual and collateral information may be added. The resulting end product is usually a "serialized" Sigint report. Reports covering general or specific subjects are given sequential serial reference numbers, within any given group. The serialized Sigint report is then disseminated outside NSA, to those government or military recipients who are cleared and authorized to handle the top secret codeword material. Thus, unless NSA has deemed a U.S. person's name as "necessary to understand the foreign intelligence or assess its importance", it will be withheld and replaced with "U.S. person", "U.S. ship" or one of the many other available "generic identities".

Analysts are cautioned not to use this technique in ways that would, nevertheless, convey apparently undisclosed identities to the recipients of the Sigint report in which they are mentioned. There are exceptions. Senior officials of the executive branch can be referred to when their communications are intercepted, or their names are referred to. However, the report must identify the official by their title, and not by their name (for example, "Vice-President of the United States").

But NSA retains this information within its databases and information systems. The legal memoranda indicate that "raw traffic storage systems which contain identities of U.S PERSONS" can be operated without restriction within NSA, save that access is

---

[121] NSA DOCS 64 and 65, 28 June and 8 July 1993. In this and subsequent references, individual documents released to EPIC under FOIA in April 2000 are identified by the serial number placed on them by NSA.
[122] NSA DOC 38, 15 December 1994.
[123] NSA DOC 90, 6 June 1996.
[124] NSA DOC 61, 15 April 1998.
[125] By the marking "(U)" appearing before or after the deletions.

"limited to SIGINT production personnel".[126] Such "incidentally intercepted communications to, from or about U.S. persons" can be stored within NSA for up to one year without special permission. Even this restriction does not apply to "approved cryptanalytic and other technical data bases" [127](emphasis added). In a summary of the "Main provisions of USSID 18" staff are told not to:

> STORE incidentally intercepted communications to, from or about U.S. persons longer than one year (except for certain approved cryptanalytic and other technical data bases) …

The summary also stipulates that:

> Access to ANY [deleted] databases that contain U.S. person identities is limited to SIGINT production personnel.

Testifying to Congress on 12 April 2000, NSA Director Lt-Gen Hayden appeared not to be familiar with these procedures. In answers to repeated questions by Congressman Roemer, and even after consulting his advisers, he told the intelligence committee that processing to remove U.S. person related data took "a few minutes … in some cases, it's minutes and seconds. In others it may be hours."

Besides permitting the retention of information about U.S. citizens in raw traffic or other storage systems, NSA also maintains parallel records of the information that is removed before a report is disseminated. This allows any recipient of an NSA Sigint report to contact the agency and ask for the details of a U.S. name or organization that has been removed. It appears from this that, within NSA, any U.S. person information that is judged sufficiently relevant to be reported in minimized form will be retained permanently within NSA and the U.S. Sigint System.

The U.S. citizen at home

Unless granted a FISA warrant, NSA and other intelligence agencies cannot lawfully directly target a U.S. person for electronic surveillance while they remain within the United States. Nor may NSA seek access to exclusively domestic communications. But many domestic communications links within the U.S. also contain foreign communications, as defined.[128]

The FBI can obtain access to all forms of domestic communications, but only if they hold a warrant under Title III (alleging criminal conduct, on probable cause) or from FISC (alleging involvement with a foreign power (as defined), also on probable cause). The law anticipates that many communications of other U.S. citizens will also be caught by such surveillances. NSA may also access all U.S. international communications that have "one foreign terminal".

In all cases (absent a warrant or other authority to target a specific citizen), the information that NSA may process and pass on is governed by the overriding requirement

[126] NSA DOC 61, 15 April 1998.
[127] NSA DOC 3, 3 September 1991.
[128] USSID 18, 3.13.

that it be relevant to "foreign intelligence". But this critical restriction, which was carefully and precisely defined in FISA, has been re-interpreted in a way that greatly weakens the protection given to U.S. citizens against unreasonable search and seizure of their personal communications and information. In restricting the use of NSA surveillance under the Foreign Intelligence Surveillance Act, Congress defined "foreign intelligence" to be "information that … is necessary to the ability of the United States to protect against actual or potential attack or other grave hostile acts of a foreign power … or sabotage or international terrorism by a foreign power or an agent of a foreign power" (see 50 USC § 1801). But internal NSA guidance, including USSID 18, instructs Sigint staff to use the much broader meaning of "intelligence that relates to the capabilities, intentions and activities of foreign powers, organizations, or persons" (emphasis added).

It is arguable that this definition places little effective restriction on the communications that NSA may collect, process, retain or disseminate. As has been frequently observed, the occasions on which the First Amendment most matters is when those exercising it are lawfully championing an unpopular cause. The activities of international non-government organizations, or any dissent within the U.S. which has an international component, will inevitably involve the "activities" of "foreign persons". Thus, if a lawful U.S. organization has any foreign connection, this can under existing regulations be used to authorize dissemination of the "incidentally" intercepted communications of its U.S. members.

This is exactly what happened to the antiwar protestors of the 1960s and 70s. During the Church Committee hearings in 1975, Senator Walter Mondale observed that among the MINARET intercepts which he had inspected was one from a "leading U.S. antiwar activist – and we know him to be a moderate, peaceful person … [He] sent a message to a popular singer in a foreign country… asking him to take part in a peace concert". NSA Director Lt-Gen Allen testified that such messages nevertheless fell properly within the tasking given to NSA at the time. They involved a U.S. peace group, an international communication to "an overseas location where foreign support and funding was requested". He added:

> It's certainly true that at this moment in time one would have certainly a different view of that than at the time. [129]

Such testimony appears to confirm that NSA regulations, then as now, can make the lawful the targeting of legitimate dissent within the U.S., provided only that NSA can detect some foreign component within their activity. Very few protest groups would avoid falling under such a definition, whether concerned with the environment, privacy, international trade, racial or gender issues, or many others. Even if one administration did not wish the intelligence community to conduct such surveillances, the next could take an entirely different view.

In these and similar circumstances, NSA testimony and information to Congress has been incomplete or inconsistent. In the "Legal Standards Applied for Electronic Surveillance" memorandum submitted to HPSCI on February 1 2000, Lt-Gen Hayden

---

[129] Senate Select Committee to Study Government Operations with Respect to Intelligence Activities (Church), 94th Congress, First session, Volume 5, "National Security Agency and Fourth Amendment Rights", p37.

told the committee that "incidentally collected … information about a U.S. person who is not an approved target … may be retained and disseminated if it amounts to foreign intelligence or counterintelligence; otherwise, it may not be retained or disseminated." His testimony two months later amended this position to include statements that intercepted communications could be retained and disseminated if they related to law enforcement matters, or to narcotics. As noted above, they can also be disseminated if the relate to leaks of government information, or to legitimate protest activities in the U.S. if they have some foreign component. These and other aspects of the NSA Director's testimony appear inconsistent with NSA's internal instructions obtained by EPIC.

The U.S. citizen abroad

Once a U.S. citizen is known to have gone abroad, FISA no longer requires a warrant to target that person. Warrantless electronic surveillance continues of the international communications of certain targeted U.S. citizens, just as was the case under the Nixon and predecessor administrations. Congress and the U.S. public are not and have never been advised of the numbers of U.S. persons so targeted. There could be far more U.S. citizens on NSA's watch lists and in NSA's databanks now than in the 1970s. The scale of such surveillances was not discussed at the HPSCI hearing on April 12, 2000, nor stated in NSA submissions to Congress.

A second area of concern is that U.S. citizens who travel abroad lose all legal protection against NSA interception, save against direct targeting. NSA's regulations presumptively deem any person communicating from outside the U.S. not to be a citizen. According to the current "Standard minimization procedures for NSA surveillances," as amended by Attorney General Reno in July 1997, "a person known to be currently outside the United States, or whose location is unknown, *will not be treated as a United States person* unless such person can be positively identified as such, or [there is] a reasonable belief that such person is a United States person" (emphasis added).[130]

Even where the intercepted communication of a U.S. person has been identified as such, "minimized" information about them in NSA reports is not deleted from internal computer systems, and remains available on demand. This data includes actual identities, titles or other identifying information about U.S. persons. When identities are withheld, NSA continues to retain within its internal systems a record of the actual name or identity that has not been supplied to its customers. This information can be made available on request, 24 hours a day, to customers who receive NSA's SIGINT reports, either on the authority of a junior official, or on request to the National Sigint Operations Center (NSOC) at Fort Meade.

The day-to-day authority to release intercepted personal identifying information of U.S. persons whose names are withheld in Sigint reports has been successively delegated to junior officials. In November 1992, the authority was "streamlined" and passed down to the Chief of NSA's Intelligence Oversight and Policy Office. Two

[130] Attachment to NSA DOC 4, 20 August 1997.

months later, it was passed to his deputy, where it remains.[131] In urgent cases, a Senior Operations Officer in the NSOC can release the same information, 24 hours a day.

Lt-Gen Hayden seemed unaware of this position when he testified to HPSCI on 12 April 2000 that:

> I have delegated [authority to release specific data about U.S. persons on request] to our Director of Operations for some matters. For other matters, I've kept it there to myself.

This appears not to have been an accurate statement of NSA policy.

"Blanket release" of U.S. identities can be and is authorized at a more senior level. NSA's Deputy Director of Operations has been authorized to permit such releases, including retrospectively (if reports containing details of U.S. citizens are found already to have been released).[132] Once an NSA official has authorized the release of a U.S. citizen's name in any Sigint report, their identities and personal information can be permanently "kept in name-retrievable data bases".[133] In the documents NSA has released, the titles and sizes of its name-retrievable databases containing U.S. citizens' identities have been withheld. Evidence about the size of these databases would be a major clue as to the extent to which NSA electronic surveillance now impinges on U.S. privacy, despite the post 1973 changes.

Testifying to Congress, NSA Director Hayden also illuminated the scale of "incidental" interception of U.S. citizens' communications when he said that – in contrast to other straightforward evidence of a crime – the volume of incidental interception of information about narcotics and terrorism in U.S. communications was such that he had delegated his authority to release the U.S. identities involved to his Operations Directorate. The significance of this comment is that any U.S. individual who can be shown (on probable cause) to be involved in such criminal activity can lawfully be targeted directly. But it appears that many U.S. names in Sigint reporting are generated as the result of indirect, perhaps subject-based targeting of the surveillance Dictionaries.

More recently, the distinction between U.S. citizens at home and abroad has faded. New developments in technology mean that NSA's definitions of domestic communications and those with "one foreign terminal" may no longer have a clear meaning.

The U.S. citizen on the Internet

USSID 18 breaks down when NSA taps the Internet. None of the disclosed NSA documents deal with the problems of the tens of millions of U.S. citizens' addresses that are now located in cyberspace. Cyberspace breaks down formerly clear categories of nationality and location, on which Fourth Amendment protections are contingent. In many and perhaps most cases, the senders and recipients of e-mail cannot be tagged as to where they are, let alone as to their nationality. The character of the World Wide Web, for example, allows domains registered in one country to be operated from another. E-mails can only be unambiguously associated with one particular country or another if this

[131] NSA DOC 43, USSID 18 Authorization to Approve Dissemination of US Identities, 27 January 1993.
[132] NSA DOC 34, 23 September 1994; NSA DOC 42, 28 January 1992.
[133] NSA DOC 102, US Identities in SIGINT, March 1994, p31.

is conveyed in the top-level domain (the final group of letters at the end of the address), for example .au for Australia or .fr for France. There is no .us domain, although some domains, such as .gov or .mil are exclusive to the United States. For the rest of the world's global Internet customers, with e-mail addresses ending in .com, .org, .net (or .int), the address found in mail gives no clue as to location. Large U.S. Internet providers such as Hotmail.com, or AOL have customers all over the world. Thus, users of America On-line (or other U.S. ISPs) cannot assume that NSA will treat them as Americans or grant their e-mail any protection.

Nor does the destination or sending address found in an intercepted e-mail have any fixed meaning. The addresses do not change as the users travel the world. E-mail between the same two recipients might on one day be a purely U.S.-to-U.S. communication, which NSA is prohibited from intercepting. The next day it might be a completely foreign communication. The only clue that an NSA analyst or computer may have is the knowledge of where and how it was intercepted. But that information is not definitive. Because the largest capacity of the Internet (switches and bandwidth) is located in the U.S., many foreign Internet messages pass to, through and out of the U.S. The opposite can also happen, with U.S. domestic traffic moving through foreign channels.

Although routers do add detailed information to a message, indicating the route through which it has passed, this provides only information about the point at which the mail has been inserted into the electronic postbox.[134] It does not disclose the physical location of the sender, or the electronic path on the phone system or Internet network by which the sender has reached that postbox. It is almost trivial to point out that Internet or e-mail traffic gives no clue as to a user's nationality, or that basic identities may easily be masked or given falsely.

Yet the Internet creates a serious intelligence problem as well as a human rights problem. Dangerous international terrorists use Hotmail. So do schoolchildren. If the Internet is to be monitored to track the communications of bombers assembling their lethal wares, how are the two classes of people to be separated and granted the rights to which there are entitled (or denied)?

How is NSA to handle intercepted e-mail, after Dictionaries have selected it for examination, if the location of the sender and recipient is unknown? In some cases (for example, a mail from a U.S. university's .edu domain) it might presume that the sender was in the U.S. If so, the sender would be presumed to be a U.S. citizen. But a user of Hotmail, CompuServe, or AOL can enjoy no such presumption. According to the "standard minimization procedures for NSA surveillances, the sender (or recipient) will be at unknown locations and "will not be treated as a United States person" unless there is evidence to the contrary within the content of the message.[135]

These considerations are also critical in determining whether or not an e-mail address may be targeted, and if so, whether a warrant is required. Similar considerations affect satellite personal communications systems and international roaming cell phones. NSA has not published any guidance or instructions indicating how the domestic or international communications of U.S. citizens should be safeguarded in its interception operations directed against e-mail and the Internet.

---

[134] Often, an SMTP (Specific Mail Transfer Protocol) server.
[135] See note 127.

Such answers as the agency has given smack of complacency. In the report to Congreess on 2 February 2000, General Hayden claimed that:

> The privacy framework is neutral and does not require amendment to accommodate new communications technologies.[136]

In their February letter to individual members of Congress, the agency had claimed "the Fourth Amendment transcends whatever technology happens to be involved in a particular form of electronic surveillance". Testifying to HPSCI on 12 April 2000, Gen Hayden said that he understood the importance of the issue:

> One of the issues that has been raised in the open press is with the advent of E-mail, for example, and how that might affect how we guarantee privacy …. we understand why questions of privacy are now more prominent.

But his only comment was that NSA saw:

> no crying need for a change in statute or regulation for clarity or flexibility or any other purpose …

Plainly, this is not correct. As Representative Barr observed:

> new generations of telecommunication satellites and the Internet are rapidly blurring the borders that traditionally delineated … domestic and international intercept activities … [this] leaves American citizens … with precious little understanding of how legal standards written in the 1970s are protecting their privacy today.

These were issues the NSA could not or did not address. CIA Director Tenet said he had "nothing to add" to Gen Hayden's remarks. But, apparently contradicting her co-witnesses, Department of Justice representative Ms. Townsend acknowledged "a recent example … a classified matter". She offered no further details.

In the absence of further information about NSA procedures for filtering intercepted e-mail to identify and exclude U.S. citizen' communications (or even evidence that such procedures exist or can be devised) the inevitable consequence of NSA's known policies is that most intercepted e-mail will come from and to users at unknown physical locations. Except in a few cases, therefore, they will be deemed to be abroad or unknown, and not to be U.S. citizens – with a corresponding loss of protection.

Similar considerations affect satellite personal communications systems and international roaming cell phones. NSA has not published any guidance or instructions indicating how the domestic or international communications of U.S. citizens should be identified and safeguarded in its interception operations directed against e-mail and the Internet.

[136] Written submission to HPSCI by Lt-Gen Michael Hayden, Director of NSA, 12 April 2000.

Intercepting the Internet

Although few details have been published about how and where the NSA obtains access to Internet traffic, it is obvious that it is potentially a major source of foreign intelligence of all kinds. Most of the world's Internet capacity lies within the United States or connects to the United States. Many international communications in cyberspace will inevitably pass through intermediate sites within the United States. For example, communications from Europe to and from Asia, Oceania, Africa or South America normally travel via the United States.

Internet traffic can be accessed either from international communications links entering the United States, or when it reaches major Internet exchanges. Both methods have advantages. Access to communications systems is more likely to remain undetected - whereas access to Internet exchanges might be more detectable but provides easier access to data and allows simpler sorting methods. In either case, the quantities of data involved are immense.

Standard Internet messages are composed of packets called "datagrams". Datagrams include numbers representing both their origin and their destination, called "IP addresses". The addresses are unique to each computer connected to the Internet. Handling, sorting and routing millions of such packets each second is fundamental to the operation of major Internet centres.

The routes taken by Internet "packets" depend on the origin and destination of the data, the systems through which they enter and leaves the Internet, and a myriad of other factors including time of day. Thus, routers within the western United States are at their most idle at the time traffic elsewhere in the world is reaching peak usage. It is thus possible (and reasonable) for messages travelling a short distance in a busy European or Asian network to travel via Internet exchanges in California. The opposite situation is also possible, although less likely.

Much Internet traffic, domestic or foreign, is of trivial intelligence interest or can be handled openly and not as Sigint. For example, messages sent to "Usenet" discussion groups amount to about 15 Gigabytes (GB) of data per day; roughly the equivalent of 10,000 books. These are open discussions, accessible to anyone wanting (or willing) to read them. Messages for Usenet are readily distinguishable. It is pointless to collect them clandestinely. Like other Internet users, therefore, intelligence agencies have open source access to this data to collect, store and analyse.

Massive storage systems have been constructed to provide on-line processing of the Internet and new international communications networks. By the early 1990s, both GCHQ and NSA employed “near line” storage systems capable of holding many terabytes[137] of data. In the UK, the Defence Evaluation and Research Agency maintains a 1 Terabyte on-line intelligence database containing the previous 90 days of Usenet messages.[138] Databases of this size and larger are now a fundamental part of Sigint activities. Storage can be either on-line (usually as Redundant Arrays of Inexpensive

[137] One thousand gigabytes (GB), or 10^{12} bytes.

[138] Personal communication from DERA.

Disks, or RAID servers) or "near-line", meaning automated stores of high capacity tape or disc cartridges. The cartridges are located and loaded by robots on demand.

One cartridge server of this kind is now on display at NSA's cryptology and Sigint museum at Fort Meade. Named POWDERHORN, by the time it was retired the server held 6000 cartridges each of 50GB (Gigabytes) capacity. The unit thus held 300 Terabytes of data (equivalent to 15,000 years of the Wall Street Journal.) POWDERHORN was retired from service in the mid 1990s. Some sources have suggested that in 2001, NSA will take delivery of a 1000 Terabyte on-line disk array.

Similar to Usenet, most of the World Wide Web is openly accessible. "Search engines" examine web sites continuously, generating catalogues of their contents. "Alta Vista" and "Hotbot" are prominent public sites of this kind. NSA openly employs computer "bots" (robots) to collect data of interest from the Web. One site they inspect routinely is a New York site with extensive public information on Sigint and cryptography, cryptome.com. Records of access to the site show that every morning it is visited by a "bot" from NSA's National Computer Security Centre, which looks for new files and makes copies of any that it finds.[139]

According to a 1995 report[140] by a former NSA employee, the agency had by 1995 installed software to sort and collect traffic of interest from nine major Internet exchanges (IXPs). The report identified nine sites. The first two such sites identified, FIX East and FIX West, are operated by government agencies. They are closely linked to nearby commercial locations, MAE East and MAE West (see table). Three other sites listed were Network Access Points originally developed by the National Science Foundation to provide the Internet "backbone".

Internet site	Location	Operator	Designation
FIX East	College Park, Maryland	U.S. government	Federal Information Exchange
FIX West	Mountain View, California	U.S. government	Federal Information Exchange
MAE East	Washington, DC	MCI	Metropolitan Area Ethernet
New York NAP	Pennsauken, New Jersey	Sprintlink	Network Access Point
SWAB	Washington, DC	PSInet / Bell Atlantic	SMDS Washington Area Bypass
Chicago NAP	Chicago, Illinois	Ameritech / Bellcorp	Network Access Point
San Francisco NAP	San Francisco, California	Pacific Bell	Network Access Point
MAE West	San Jose, California	MCI	Metropolitan Area Ethernet
CIX	Santa Clara California	CIX	Commercial Internet Exchange

A 1997 hacking case in Britain produced some evidence of NSA surveillance of the Internet. Witnesses from the Air Force component of NSA, AIA, acknowledged using packet sniffers and specialised programmes to track attempts to enter U.S. military computers. But the prosecution collapsed after the U.S. witnesses refused to provide evidence about the methods they had used.[141]

---

[139] Personal communication from John Young.

[140] "Puzzle palace conducting internet surveillance", Wayne Madsen (now also of EPIC), *Computer Fraud and Security Bulletin*, June 1995.

[141] More6 Naked Gun than Top Gun, Duncan Campbell, *Guardian*, 26 November 1997.

However NSA may have enlarged and enhanced its access to the Internet in the U.S, it is apparent that this new technology is, for reasons of geography and technology, now central to many "foreign" communications systems. NSA's charter to conduct only foreign intelligence gathering thus places increasingly fewer restrictions on its encroachments into domestic communications.

Collaboration with allied Sigint agencies

Sigint organizations in the UKUSA alliance have used each other's services to carry out tasks that they have been unwilling to do for themselves. Testifying to Congress, Gen Hayden has disputed that this occurs:

> Another of the urban myths out there … [is that] we ask others to do on our behalf that which we cannot do for ourselves.[142]

Hayden added that "NSA may not ask another country's intelligence service to do what it is prohibited by law or regulation from doing itself":

> By executive order, it is illegal for us to ask others to do what we cannot do ourselves, and we don't do it. And by policy we will not do for others what it is illegal for them to do, and we haven't done it and we will not do it.

The restraints applied to NSA in these circumstances appear to be less clear that his words may have conveyed. The specific section of EO 12333, section 2.12 says:

> **2.12 Indirect Participation.**
> No agency of the Intelligence Community shall participate in or request any person to undertake activities forbidden by this Order.

But in the section dealing specifically with NSA, there are no prohibitions to be found. The Order does say that intelligence agencies may "collect, retain or disseminate information concerning United States persons only in accordance with procedures established by the head of the agency concerned and *approved by the Attorney General*" (emphasis added).[143] This provision excuses NSA from having to make its own determination of legality, about which EO 12333 stipulates:.

> **2.8 Consistency With Other Laws.**
> Nothing in this Order shall be construed to authorize any activity in violation of the Constitution or statutes of the United States.

[142] HPSCI hearing, 12 April 2000.
[143] EO 12333 also generally prohibits other types of conduct, such as assassination or human experimentation, not relevant to this discussion of NSA.

For whatever reason, the Executive Order falls short of saying that intelligence agencies shall not request any person to undertake activity in violation of the Constitution or statutes of the United States.

Whether for such purposes or otherwise, several accounts suggest that UKUSA intelligence agencies do ask each other to do tasks which they could undertake technically but are unwilling to do for themselves, whether for reasons of legality or political expediency. Two Canadian CSE workers say that they have undertaken such tasks in the United States, for NSA.

In the fall of 1975, according to former CSE manager Mike Frost, CSE was asked by NSA to provide staff for a two week counter-intelligence operation in the Chesapeake Bay area. He was one of two Canadian Sigint staff who did the job. They entered the US and drove to Maryland, to monitor a dwelling in the Chesapeake Bay area for possible HF transmissions. Some were found, he says, and "the tape and the conclusions were turned over to NSA" . The Canadians went home. In his book *Spyworld*, Frost says he was uncertain as to whether the NSA were "bending the law [or] breaking it", adding:

> NSA wanted to pull a "Pontius Pilate" and wash their hands from it (sic).[144]

On a second occasion revealed by Frost, in 1993 Britain's GCHQ asked CSE to undertake the bugging of two British Cabinet Ministers. The reason for the operation, was that Prime Minister Margaret Thatcher questioned her colleagues' political loyalty:

> A request had come through GCHQ from Margaret Thatcher asking if CSE could 'do something' to aid her in finding out if two of her Cabinet ministers were, to use her terms, 'on side'.

One of Frost's colleagues was dispatched to London with special receiver equipment in his luggage. Using frequencies provided by GCHQ and working from Macdonald House, the Canadian High Commission in London, the officer eavesdropped on and recorded the two Ministers' car phone conversations. He then handed the tapes to GCHQ. Frost says the reason GCHQ asked CSE to carry out the bugging was precisely so that British ministers could deny all knowledge if it were exposed and they were asked about it in British Parliament. After Frost's book was published and its contents reported in Britain in 1994, the operation was indeed denied.

About the same time, according to a senior British official, GCHQ was asked to carry out Sigint activities against a number of U.S. citizens in the Caribbean.[145] The request was regarded in Britain as unusual. NSA had far better collection resources in the Caribbean area than GCHQ. The ostensible justification for the surveillance was that the individuals concerned were involved in narcotics trafficking.

Former Australian intelligence officers say that their service has undertaken electronic surveillance missions on behalf of the United Kingdom, so as to create "deniability" for the British if the operations were detected. These operations have included the bugging of Kuwait after the liberation operations of the Gulf War; bugging

[144] See note 40.

[145] Personal communication. The official was unwilling to identify the targets of the surveillance.

in Hong Kong before the handover to China; and a 1988 counterterrorist operation tracking an IRA team who planned to detonate a bomb in Gibraltar.

These accounts suggest that while it may be correct that NSA and its sister agencies do not ask others to commit clearly unlawful acts, they may ask foreign agencies to carry out activities which may be politically questionable or potentially embarrassing if they were to do so themselves.

What limits for NSA surveillance?

In a booklet providing the public history of NSA, supplied to visitors at its Fort Meade museum, NSA accepts that its activities were "improper" in the 1970s, in relation to events described to the Church Committee. Congress has recently been told that such conduct is now almost impossible:

> It's theoretically possible for us to use [our] capability -- technologically possible to use that capability in ways that are prohibited. Of course I have to answer yes. But the oversight mechanisms, the training, the procedures, the culture of the institution, the laws and regulations that we have put in place, make that as a practical matter well nigh impossible to do.[146]

Despite this, NSA surveillance of U.S. citizens now may be far larger than in the 1970s. Then, for purposes not linked to law enforcement or criminal conduct, NSA performed warrantless searches against about 1200 U.S. names. At any one time, about 600 U.S. citizens were on the watch list. The reasons for targeting them, as set out in documents appended to the Church report, were to find foreign involvement connected to civil disturbances, or in the activities of antiwar protesters, or narcotics trafficking, or alleged terrorism or threats to the president. These are all still authorized targets. Now, NSA surveillance is both warranted and warrantless.

In 1999, nearly 900 FISC warrants were issued. Although the vast majority of the warrants were issued to the FBI, it would be lawful, and probably essential and automatic, for NSA to supplement FBI surveillance by ensuring that international communications about, to or from these targets were also covered. To this must be added the unknown number of warrantless surveillances directed against U.S. citizens who are abroad, for which merely a certificate from the Attorney General is sufficient authority. In total, the aggregate number is likely to be at least similar and may well be larger than the total number of U.S. citizens under direct surveillance in the Nixon era.

The NSA meaning of "incidental", a critical term, appears to have changed. In the 1970s, all U.S. communications obtained and processed in MINARET were described by the then NSA Director as "incidentally acquired". By this, he meant that NSA had not set up new collection systems to collect on the Americans that NSA targeted. The meaning now seems to be that the names of U.S. citizens have not been into NSA's databases as *primary*, direct targets. But the nature of contemporary targeting methods means that they need not be primary targets in order for their international communications to be covered.

---

[146] HPSCI hearing, 12 April 2000.

This will occur if NSA's "technical databases" list U.S. persons or their associated personal identifiers within filtering databases such as those used by "Dictionary". It appears from NSA documents that this may be permissible, provided it is not done simply in order to circumvent Fourth Amendment and legislative protection. Dictionary systems can target the communications traffic of citizens who may not be direct, specific targets of the agency's operations. NSA did not declare the filtering methods it used to Congress in 1975, nor during the hearing on 12 April 2000.

As much as Lt-Gen Hayden said on the latter occasions was that agency rules did not permit "mere association or what we call reverse or indirect targeting to target [a] person". The example he gave was targeting a U.S. citizen who was overseas, but whose parents were not U.S. citizens and whose communications could therefore be targeted without a warrant or a certificate from the Attorney-General, in the hope (were it permitted) of acquiring information about their child.

The key test disclosed in NSA rules is one of intent or purpose. The agency clearly recognizes that it may not directly target a U.S.person without proper authority. It also says it recognizes that to set out to target a person by targeting a different person is impermissible. If there is an NSA rule actually saying this, however, it is not to be found in the available public documentation. It is therefore impossible to verify stated policy, to assess how carefully drafted it may be, or to know what exemptions are permitted.

Moreover, the test of purpose may have no practical effect so far as actual collection or its effects on First and Fourth Amendment Rights are concerned. An NGO, other than one based in the U.S. and "substantially" populated by U.S. citizens can be a legitimate and likely NSA target. The names of key U.S. officers of the U.S. branch of the organisation would be proper terms for inclusion in the Dictionary search mechanism. Nothing in NSA's disclosed rules prohibits this, provided that the target is the organization and that collection of U.S. identity-related information is "incidental".

The rules do require minimization. If an official of a U.S. branch of the World Health Organization sent a fax to her head office in Geneva, that message could be collected and processed. The U.S. official's name or post could appear in an NSA end product report, provided that her identity was "necessary to understand foreign intelligence information or assess its importance". But a private e-mail sent by the same writer to a personal friend in Paris should be removed from the system once its contents had been appraised as private.

GCHQ, the British arm of UKUSA, routinely targets NGOs, including third world Aid groups such as Christian Aid. Other GCHQ targets include Amnesty International and the hierarchy of the Catholic Church. Telephone calls made by these organizations are recovered from a system called MANTIS. For telex messages, the system was called MAYFLY.[147]

There are many NGOs and issue-based groups in the U.S., some of whom – such as the recent campaigns against the IMF in Washington or the WTO in Seattle – are involved in civil disorder at the same time as being actively involved with foreign contacts and supporters. Such events are the contemporary counterpart of the Vietnam War protests of the 1960s and 1970s. Filtering technology can permit NSA to conduct warrantless interception of the communications of U.S. citizens involved in such activity, provided that targeting is directed against the organization. Publications by the US Air

[147] *Observer,* 28 June 1992.

Force 544th Intelligence Group, referred to above, suggest that NGO's may indeed important foreign intelligence targets for ECHELON.[148]

In Britain, recent changes to legislation have made the test of "purpose" quite explicit in relation to Dictionary level targeting. Warrants issued to GCHQ to conduct Sigint activities have to specify "classes" of communications (i.e. general Dictionary targets) to be intercepted and processed, but may not normally specify individuals *per se,* if they are in the UK. But "factors", including names, can be put into the Dictionary and intelligence officials can "read, look at or listen to" the resulting intercepts provided that the "purpose" of the interception was not "the identification of material contained in communications sent by him, or intended for him". Thus, Sigint Dictionaries may target individuals known to be in the UK, provided that the purpose of the targeting is not directed at that individual. In practice, in the US as in the UK, the intrusion that this method makes on individual rights, and the chilling effect it may have on free speech is identical whether or not an individual is directly targeted.[149]

Within NSA, there are many large databases whose contents are not disseminated outside the Sigint organisations, but are used for intelligence analysis, traffic analysis or cryptanalysis. According to the "U.S. Identities in Sigint" manual:

> USSS personnel may establish and maintain analytic or reporting systems (data bases, files, working aids, etc.) that can be accessed by a U.S. identity or personal identifier [150].

Further rules on the information that may be retained indicates that incidentally acquired "recognizable US identities" can be stored in technical data bases if this is necessary, or if it is not practical to minimize or exclude the information, or if the identity has been permitted to be disseminated in NSA reports. For analytic and reporting systems:

> US Identities or [deleted] which the DDO or his designee has authorized dissemination may reside in name-retrievable storage systems

Otherwise, they should be replaced by a generic term "whenever practical"[151] Separate rules govern the retrieval of U.S. identities from traffic databases, but these have been withheld from disclosure.

Current USSID 18 storage criteria, referred to earlier, indicates that the normally permitted retention period for raw Sigint that contains U.S. identities is one year, but that it may be indefinite if the data enters an appropriate data base. [152]

---

[148] See pages 32-34.

[149] The United Kingdom has no written Constitution. However, its laws are subject to the European Convention on Human Rights, which contains provisions similar to the U.S. Constitution and Bill of Rights. Article 8, concerning the integrity of the individual, includes provisions broadly similar to the Fourth Amendment. (The European Convention also provides protections to individuals who are in the UK irrespective of nationality, whereas in the U.S. protection is limited to U.S. citizens or permanent resident aliens.)

[150] NSA DOC 102, US identities in Sigint, page 31.

[151] *Ibid*.

[152] NSA DOC 3. "Section 6-RETENTION …DO NOT STORE incidentally intercepted communications to, from or about U.S. persons longer than one year (except for certain approved cryptanalytic and other technical data bases)".

Intelligence databases can include or be based on "collateral" data not drawn from Sigint, or even from secret sources. For example, the full U.S. phone directory (including unlisted numbers) is relevant data for NSA to hold. The names and details of U.S. journalists, business people and politicians who travel overseas is important data for NSA to hold. Such databases may start from information of the type that is held in a public library or a newspaper archive. But they are also NSA's internal intelligence and analytic databases. They can enable analysts to determine who a person is when a U.S. name is mentioned in an intercept, if only for the beneficial purpose of identifying citizenship and applying minimization if required.

Provided these databases are retained inside NSA, they can go far further. None of the directives or disclosed documents place a legal limit on what data may be retained, if it is judged useful to future processing activity. Personal information about U.S. citizens obtained from any Sigint can be added to these internal personal files, for technical, analytic or traffic purposes. The information obtained and added can be held raw, or processed.

During the 1970s, it was revealed that the NSA maintained "technical" files on 75,000 U.S. citizens who were not its direct targets. These files were claimed not to have been developed "for any sinister reason" but simply to aid the agency in its "legitimate foreign intelligence mission'.[153] Today's equivalent databases can only be larger.

NSA's rules clearly say that such information can only be passed *outside* NSA[154] if it minimized, and if the resulting data is relevant to foreign intelligence. (As noted above this requirement can be met if the information concerns <u>any</u> activity of <u>one</u> foreign person.) In 2000 or 2001, a message saying that a German pop group had agreed to sing at a "save the forests" protest concert is sufficient for the communication to be valid "foreign intelligence". This is not fanciful speculation – documents provided to the Church Committee show that this happened.[155]

The absence of clear legal controls in these delicate areas, and the flexibility of executive branch instructions mean that intelligence agencies like NSA can be led into abuse by higher authority. Such conduct, which was the essence of the Nixon White House's unlawfulness, did not end in 1975. Eleven years later, National Security Adviser John Poindexter and Colonel Oliver North were doing the same. When they learned that a former Contra mercenary was providing details of U.S. covert involvement to the press and Congressional staff, an authorised wiretap was arranged on the grounds that the mercenary, Jack Terrell, was a foreign agent for the Nicaraguan government who was threatening to assassinate the President. The falsity of this allegation by North and Poindexter was eventually established by the FBI – but meanwhile, the White House was supplied with transcripts of conversations Terrell held with the staff of Senator John Kerry, who was investigating Contra affairs as a member of the Senate Foreign Relations Committee. At the same time, in 1986, Poindexter took the lead role in expanding NSA's

[153] Report says NSA had files on 75,000 in US, *Washington Post*, 11 May 1976.
[154] As all references to GCHQ and other foreign Sigint agencies have been redacted from the documents disclosed to EPIC, it is impossible to determine NSA's policies in relation to sharing such databases with foreign Sigint partners. In practice it is likely that some databases are shared, and some are not. Besides shared UKUSA material, each country also holds and processes purely national information, as "U.S. Eyes Only", "Canadian Eyes Only", etc.
[155] See page 00.

domestic information security role including the controversial "unclassified sensitive" category of data held by private corporations.[156]

USSID 18 also contains an "equipment testing" exemption, which allows intelligence agency staff to test or train on electronic surveillance equipment for up to three months at a time. Complex surveillance equipment intended for use abroad can in these circumstances be deployed against private U.S. communications. Training takes place at Fort Meade and other NSA offices in the Baltimore area, and in Warrenton, VA, where both NSA and CIA run electronic surveillance centers. A recent report quoted an NSA linguist who had studied at the Warrenton Training Center in the mid 1980s, :

> We listened to all the calls in and out of Washington …We'd listen to Senators, Representatives, government agencies, housewives talking to their lovers.[157]

The calls were obtained from AT&T microwave radio links passing nearby.

The conversation of one U.S. Senator was monitored from NSA's Menwith Hill Station in England, according to a witness who was invited to listen in by Sigint staff. The witnesss was Peg Newsham, then a software systems manager for a new Sigint satellite project. She says she was handed headphones and invited to listen to a telephone call being made by Senator Strom Thurmond. In 1988, Ms Newsham described this incident to HPSCI. But no substantive investigation took place, and no report was made to Congress. Neither of these incidents suggest deliberate targeting in an illegal or unconstitutional way. But they do suggest that the boundaries of what NSA may disseminate are substantially different to its internal restraints.

Since 1978, Congress has not been asked to consider providing a statutory basis for the NSA. In Australia, senior staff of the national Sigint agencies have urged statutory legislation. Without a formal legal charter and restrictions, they suggest, there is little to stop politicians from issuing directives for improper or even party political purposes. Conscious of its powers to intrude, DSD says that it would welcome new legislation to define forever what it should and shouldn't do, no matter who might be in power. The Commissioner of Canada's CSE made similar recommendations in 1998, now to be enacted. Even Britain's GCHQ was put on a legislative footing in 1994.[158]

Quite apart from Fourth Amendment rights, the practice of targeting lawful protest groups or NGO's that may have a foreign component attacks First Amendment rights by chilling free speech. Such attacks are both most likely and most powerful when the right of free speech is used to criticize government policy or conduct.

In practice, very little has changed since 1973. If there were a new war, a new generation of Jane Fondas or Benjamin Spocks could be treated in the same way as were their forerunners. All that an administration of the day would need to do is feed a collection of newspaper articles and reports on the subject of antiwar protests into a "topic" targeting database, and pass it to NSA for action by the worldwide Dictionaries of ECHELON and kindred systems. No-one would have *told* the computers to target Jane Fonda. Nothing would have been done by NSA staff that would specify a U.S. citizens as required targets. But, thanks to new technology, the effect would be identical.

---

[156] Madsen, *op cit* (note 6).
[157] Catching Americans in NSA's Net, Scott Shane and Tom Bowman, *Baltimore Sun*, 12 December 1995.
[158] Intelligence Services Act, 1994.

PRIVACY AND INTERNATIONAL TELECOMMUNICATIONS

During the 1980s, staff and visitors who entered the operations block, Building 600, of RAF Chicksands – a USAF listening station in England - would pass a turnstile and a security badge check to be confronted directly with a Sigint in-joke. Pasted to the wall was a copy of the International Telecommunications Convention. The Convention, which both the United Kingdom and the United States have ratified, promises that member states will protect the privacy of communications. Passing by, the operators set out to do the opposite.

This satirical presentation of the telecommunications treaty raises the abiding conundrum of intelligence oversight - that intelligence involves *ipso facto* breaking laws. Since the 1970s, former NSA staff who have talked about their work have often said that they were taught that secrecy was necessary because "Sigint is illegal". The increasing publicity and attention to this issue has raised the question of the general right to international telecommunications privacy, and how it may be enforced. Sigint, which comprehensively attacks the privacy of such communications, remains – unlike domestic wiretapping in most countries – unregulated and beyond the reach of most national jurisdictions.

Two international treaties protect international communications. The first is the International Telecommunications Convention (ITC), which sets up the International Telecommunications Union, based in Geneva. It and its subsidiaries are the governing bodies of international communications. Article 22 of ITC says

> **Secrecy of Telecommunications**
>
> 1. Members agree to take all possible measures, compatible with the system of telecommunication used, with a view to ensuring the secrecy of international correspondence.
>
> 2. Nevertheless, they reserve the right to communication such correspondence to the competent authorities in order to ensure the application of their internal laws or the execution of international conventions to which they are parties

The caveat on the undertaking of secrecy in communications relates only to "internal laws" of states. The Sigint arrangements between the UK, others and U.S. are not an "international convention". The convention appears only to authorize law enforcement undertaken for the proper purposes of law enforcement.

The Vienna Convention on Diplomatic Relations (1961) affects only governments, but is more specific: Article 27 says:

> 1. The receiving State shall permit and protect free communication on the part of the mission for all official purposes. In communicating with the Government and the other missions and consulates of the sending State, wherever situated, the mission may employ all appropriate means, including diplomatic couriers and messages in code or cipher. However, the mission may install and use a wireless transmitter only with the consent of the receiving State.

> 2. The official correspondence of the mission shall be inviolable. Official correspondence means all correspondence relating to the mission and its functions.

Article 30 specifies:

> 1. The private residence of a diplomatic agent shall enjoy the same inviolability and protection as the premises of the mission.
>
> 2. His papers, correspondence and, except as provided in paragraph 3 of Article 31, his property, shall likewise enjoy inviolability

The Universal Declaration of Human Rights, to which all UKUSA nations are signatories, specifies at Article 12 that:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

The same language is reflected in Article 8 of the European Convention on Human Rights reflects the same position, with some qualifications:

> 1.Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The Fourth Amendment stipulates:

> 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.

Each of these provisions is challenged by the activities described previously. As noted in the introduction, when the Bill of Rights was written, it was inconceivable that the British redcoats who had been beaten back to their homeland could intrude on the privacy of an American household. The situation has changed, and with it the question of why privacy in communications should end at national boundaries.

Within Europe, these issues are being addressed in the context of growing federal and police collaborative arrangements which will shortly permit cross-border interception arrangements to deal with law enforcement activities against serious crime, narcotics trafficking, of terrorism. The availability of these new arrangements reduces or removes the need for intelligence agencies to conduct Sigint, if collaborative and effective law enforcement arrangements are in place. According to resolutions in the European Parliament, all international interceptions must:

> have a legal basis, be in the public interest and be strictly limited to the achievement of the intended objective; and
>
> even in the case of the fight against cross-border crime, adequate safeguards governing interceptions should be drawn up; and
>
> any form of interception by a Member State should be notified to the Member States on whose territory the persons whose communications are being intercepted are present.

An accompanying resolution asserts "on a world-wide scale, the rise of the information society has not been accompanied by a corresponding revision of provisions on data protection". In relation to arbitrary searches or unreasonable search and seizure, it says:

> any form of systematic interception cannot be regarded as consistent with that principle, even if the intended aim is to fight against international crime [and] …
>
> any Member State operating such a system should cease to use it.

The duty to protect the privacy of international communications needs to be enhanced. Although existing national and international law is adequate in principle, what is required is building upon existing provisions to extend these instruments and conventions and their effects. Given new international collaborative arrangements for law enforcement, the conflict between Sigint activities and human rights could reduce as its proper remit became more restricted, to specific military and much more narrowly drawn national security purposes.

Privacy and human rights in other UKUSA nations

During the FISA hearings of 1977, the alliance between Sigint agencies under the UKUSA agreement was cited as one reason why U.S. citizens traveling abroad should not enjoy the same protection as at home. On 19 July 1977, Attorney General Griffin Bell told the Senate Select Committee on Intelligence that his reasons for taking this position:

> could only be discussed in executive session … many of the problems arise out of the fact that overseas there is a fair degree of co-operation between our Government and the police and intelligence services of other nations[159]

Why this should be so was not explained, nor is any explanation obvious save a desire to keep concealed the extensive interlinking and collaboration taking place within the international Sigint network.

At the time, none of UKUSA nations had given their citizens any protection, nor had they apparently considered it necessary to do so. Sigint everywhere operated in a

[159] Hearings before the Subcommittee on Intelligence and the Rights of Americans of the Senate Select Committee on Intelligence, on S.1566, p17, 19 July 1977.

realm of its own, where history has shown legality or human rights not to be a significant consideration.

The changes that started in the U.S. spread. In the UK, a complaint about a wiretapping case brought under the European Convention forced the UK government to introduce an Interception of Communications Act in 1984, placing statutory controls over wiretapping and requiring a non-judicial warrant, signed by a Secretary of State, before domestic interceptions could proceed. But the interception of international calls was authorized under a different procedure. In this case, warrants did not name targets but identified groups of communications links, which could be intercepted as a whole. Once intercepted, GCHQ was authorized automatically to extract "classes" of communications described in certificate issued alongside the warrant. These provisions were precisely matched to the technology of the Dictionary.

The certificates described the targets of communications interception about which the British government wished Sigint reporting. According to the law, the certificates should not include specific named persons. But their names could of course be included in the filtering selection databases within the Dictionary. Although the UK does not have an equivalent of the Fourth Amendment, this maneuver prevented even the limited challenges that citizens might bring before an Interception of Communications Tribunal to complain about domestic wiretapping. The law stipulated that a person could only complain about international interception if they were specifically identified in the certificate – but not in the contents of the Dictionary. According to former members of the British Security Service (MI5), no high-level or legal checks were needed on the names that might be added to GCHQ's Dictionary target lists in this way.

The controversy over Echelon led both Australian and Canadian authorities to issue statements acknowledging for the first time their participation in the UKUSA alliance and describing their policies on Sigint and privacy. Australia has an Inspector General of Security and Intelligence with powers to examine the conduct and operations of its Sigint organization, DSD. Canada appointed attorneys to work inside its Sigint organization in 1986. In 1997, a Commissioner was appointed to oversee its Communications Security Establishment (CSE). NSA has an Inspector General, as well a substantial number of legal counsel, including some working in its operations division. Britain and New Zealand have not made provisions of this kind.

According to the Director of Australia's DSD[160], "to ensure that [our] activities do not impinge on the privacy of Australians, DSD operates under a detailed classified directive approved by Cabinet and known as the "Rules on SIGINT and Australian Persons". The directive is said to prohibit the deliberate interception of communications between Australians in Australia, the dissemination of information on Australians gained accidentally during the course of routine collection on foreign communications, and the reporting or recording of the names of Australians mentioned in foreign communications.

There are exceptions. The Cabinet directive specifies that Australians' international phone calls, faxes or e-mails can be monitored by DSD in specified circumstances. These are stated to include "the commission of a serious criminal offence; a threat to the life or safety of an Australian; or where an Australian is acting as the agent of a foreign power". The Director of DSD must give specific approval in each

[160] Statement by DSD Director Martin Brady, broadcast on the *Sunday Programme*, Channel 9 TV (Australia), 11 April 1999.

case. The interception of domestic calls in Australia is restricted to the police and ASIO, the Australian Security Intelligence Organization. As described, the Australian procedures appear similar to U.S. procedures, while not having any force of law.

Although Australian journalists have applied for this document under freedom of information laws, it has not yet been released in whole or in part. The Inspector-General of Security and Intelligence, who can receive complaints and conduct inquiries, monitors compliance with the directive. The DSD Director, Martin Brady also claimed that other UKUSA nations followed common procedures with Australia. "Both DSD and its counterparts operate internal procedures to satisfy themselves that their national interests and policies are respected by the others". The Australian position is that if NSA or another agency intercepts Australian traffic and reports a message from an Australian citizen or company whom DSD has decided to leave alone, they are supposed to strike out the name and insert "Australian national" or "Australian corporation" instead. If DSD has authorized the targeting of that person, the opposite applies.

According to Hager,[161] and also GCHQ sources, Sigint reporters and analysts in New Zealand and Britain are told to follow U.S. minimization rules when dealing with U.S. nationals. Thus, they are asked to replace specific names with standard generic phrases such as "U.S. person".

In his 1997-1998 report, the Commissioner of the Canadian Communications Security Establishment suggested for the first time that such policies were in force across UKUSA, and that one agency would follow the policy of the other in dealing with UKUSA nationals. According to his report, CSE has committed to "respect the corresponding procedures of its close and long-standing allies":

> CSE undertakes explicitly to treat the communications of Second Party nationals in a manner consistent with the provisions issued by the agency of that country, provided such procedures do not contravene the laws of Canada. This is a reciprocal undertaking to ensure that the Second Parties do not target each other's communications or circumvent their own legislation by targeting communications at each others' behest. In other words, they do not do indirectly what would be unlawful for them to do directly".[162]

If this statement is generally true, then it demonstrates that countries co-operating in policing and intelligence can operate with and agree to protect human rights outside their own borders. The value of this assurance is limited by the fact that the agreement to do this has never been published, or referred to by any government; that only Canada has ever suggested that there is an agreement; and that the protections, if valid, extend only as far as the "Second Party" country's own rules for the privacy of its citizens. These rules are substantially classified in the US, and wholly unavailable elsewhere. They do not exist in the UK.

The technical arrangements for the global network also indicate that the restriction on disseminating U.S. identities (etc) is limited to the collective outside boundary of the UKUSA Sigint organizations. The information passed from country to country by Dictionaries is raw, unprocessed traffic, not end product reports. No restriction affects the transmission of raw data from country to country.

---

[161] Secret Power, *op cit.*

[162] Annual Report of the Communications Security Establishment Commissioner, Ministry of Public Works and Government Services, Ottawa, Canada, 1998.

LEGISLATIVE ISSUES

This report has raised a wide range of issues dealing with privacy, human rights and constitutional issues and affecting the oversight, management and operational practices of the National Security Agency and other, collaborative Sigint organizations. To date, these issues have not been examined or examined fully. They include:

1. **Relevant and critical information about collection systems may have been previously withheld from Congress in 1974-78.**

2. **Warrantless electronic surveillance continues** of the international communications of some U.S. citizens. The numbers involved are unknown.

3. **NSA can intercept domestic communications systems** if "foreign intelligence" may can be obtained.

4. **Non-targeted or 'incidental'" surveillance of international communications from, to or about U.S. citizens occurs with great frequency.**

5. **NSA's intelligence "technical databases" can be used to circumvent Fourth Amendment and legislative protection.**

6. **U.S. citizens who travel abroad lose legal protection** and are deemed not to be U.S. persons, unless the opposite is established.

7. **Laws and regulations governing NSA activities no longer have any clear meaning in relation to the Internet.** Surveillance of the Internet may be almost entirely unrestricted, since addresses in cyberspace are seldom linked to physical location or national identity.

8. **"Raw traffic storage systems which contain identities of U.S. persons" can be operated without restriction and can be stored for a year or more**.

9. **"Minimized" information about U.S. persons in NSA reports is not deleted from internal computer systems, and is available to outsiders on application**.

10. **Authority to release intercepted personal information about U.S. persons has been delegated to a junior official.**

11. **"Blanket release" of U.S. identities can be authorized by NSA staff.**

12. **Whistleblowers can be targeted and reported on,** despite the directive that NSA's mission is to procure only foreign intelligence.

13. **Critical restrictions on NSA have been re-interpreted** in a way that greatly weakens the protection given to U.S. citizens against unreasonable search and seizure of their personal communications and information.

14. **NSA may report on U.S. politicians, political parties and candidates** when this is deemed "necessary to understand foreign intelligence or assess its importance."

15. **Hundreds of different U.S. non-governmental organizations can be intercepted and referenced in NSA reports.**

16. **U.S. citizens who work with or for non-U.S. corporations or international non-governmental organizations have diminished protection.**

17. **U.S. persons' international communications can be seized and searched for apparent evidence of lawbreaking, without restriction.**

18. **Important exemptions to Fourth Amendment safeguards have been classified and are being withheld.**

19. **NSA is alleged to have used foreign agencies to collect information about U.S. citizens on its behalf, in circumstances that may be legally questionable or unlawful.**

20. **NSA testimony and information to Congress about Sigint and human rights has been incomplete or inconsistent.**

In the information age, we may need to re-learn a lesson now a century old. Despite the sophistication of 21st century technology, today's e-mails are as open to the eyes of snoopers and intruders as were the first crude radio telegraph messages. Part of the reason for this is that, over many decades, NSA and its allies worked determinedly to limit and prevent the privacy of international telecommunications. Their goal was to keep communications unencrypted and, thus, open to easy access and processing by systems like ECHELON. Until protection become effective and ubiquitous, the threat posed by these systems will not go away, and will continue to chill or deter lawful free speech and action.

GLOSSARY

AIA	Air Intelligence Agency (U.S. Air Force)
CFS	Canadian Forces Station
CLID	Calling Line Identification
COMINT	Communications Intelligence
CSE	Communications Security Establishment
CSS	Central Security Service
DSD	Defence Signals Directorate
FISA	Foreign Intelligence Surveillance Act
FRD	French Diplomatic (intercept)
GCHQ	Government Communications Headquarters
GCSB	Government Communications Security Bureau
HF	High Frequency
HVCCO	Handle Via Comint Channels Only
ILC	International Leased Carrier
IP	Internet Protocol
ITD	Italian Diplomatic (intercept)
NGO	Non Government Organization
DDO	Deputy Director of Operations (NSA)
DO	Director of Operations (NSA)
INFOSEC	Information Security
INSCOM	Intelligence and Security Command (U.S. Army)
GIST	Summary of the meaning and essential points of a communication
NSA	National Security Agency
NSCID	National Security Council Intelligence Directive
NSG	Naval Security Group (U.S. Navy)
OCR	Optical Character Recognition
ROF	Remote Operations Facility
RSOC	Regional Sigint Operations Center
SIGINT	Signals Intelligence
SUKLO	Special UK Liaison Officer
SUSLO	Special US Liaison Officer
TA	Traffic Analysis
TCP/IP	Transmission Control Protocol/Internet Protocol
USSID	U.S. Signals Intelligence Directive

Appendix 1

1.12 Intelligence Components Utilized by the Secretary of Defense.

In carrying out the responsibilities assigned in section 1.11, the Secretary of Defense is authorized to utilize the following:

[…]

(b) National Security Agency, whose responsibilities shall include:

(1) Establishment and operation of an effective unified organization for signals intelligence activities, except for the delegation of operational control over certain operations that are conducted through other elements of the Intelligence Community. No other department or agency may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense;

(2) Control of signals intelligence collection and processing activities, including assignment of resources to an appropriate agent for such periods and tasks as required for the direct support of military commanders;

(3) Collection of signals intelligence information for national foreign intelligence purposes in accordance with guidance from the Director of Central Intelligence;

(4) Processing of signals intelligence data for national foreign intelligence purposes in accordance with guidance from the Director of Central Intelligence;

(5) Dissemination of signals intelligence information for national foreign intelligence purposes to authorized elements of the Government, including the military services, in accordance with guidance from the Director of Central Intelligence;

(6) Collection, processing and dissemination of signals intelligence information for counterintelligence purposes;

(7) Provision of signals intelligence support for the conduct of military operations in accordance with tasking, priorities, and standards of timeliness assigned by the Secretary of Defense. If provision of such support requires use of national collection systems, these systems will be tasked within existing guidance from the Director of Central Intelligence;

(8) Executing the responsibilities of the Secretary of Defense as executive agent for the communications security of the United States Government;

(9) Conduct of research and development to meet the needs of the United States for signals intelligence and communications security;

(10) Protection of the security of its installations, activities, property, information, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the NSA as are necessary;

(11) Prescribing, within its field of authorized operations, security regulations covering operating practices, including the transmission, handling and distribution of signals intelligence and communications security material within and among the elements under control of the Director of the NSA, and exercising the necessary supervisory control to ensure compliance with the regulations;

(12) Conduct of foreign cryptologic liaison relationships, with liaison for intelligence purposes conducted in accordance with policies formulated by the Director of Central Intelligence; and

(13) Conduct of such administrative and technical support activities within and outside the United States as are necessary to perform the functions described in sections (1) through (12) above, including procurement.

Appendix 2

DoD Directive 5240.1-R Procedure 5

Procedures governing the activities of DoD intelligence components that affect United States persons, December 1982

Procedure 5 - Electronic Surveillance in the United States for Intelligence Purposes

Part 3: Signals Intelligence Activities

A. Applicability and Scope

1. This procedure governs the conduct by the United States Signals Intelligence System of Signals Intelligence activities that involve the collection, retention, and dissemination of foreign communications and military tactical communications. Such activities may incidentally involve the collection of information concerning United States persons without their consent, or may involve communications originated or intended for receipt in the United States, without the consent of a party thereto.

2. This part of procedure 5 shall be supplemented by a classified annex promulgated by the Director, National Security Agency/Chief, Central Security Service, which shall also be approved by the attorney general. that regulation shall provide that signals intelligence activities which constitutes electronic surveillance, as defined in parts 1 and 2 of this procedure, will be authorized in accordance with those parts. Any information collected incidentally about United States persons shall be subjected to minimization procedures approved by the attorney general.

B. Explanation of undefined terms

1. Communications concerning a United States person are those in which the United States person is identified in the communication. A United States person is identified when the person's name, unique title, address, or other personal identifier is revealed in the communication in the context of activities conducted by that person or activities conducted by other and related to that person. A reference to a product by brand name or manufacturer's name or the use of a name in a descriptive sense, as for example, "Monroe doctrine, "is not an identification of a United States person.

2. Interception means the acquisition by the United States signals intelligence system through electronic means of a nonpublic communication to which it is not an intended party, and the processing of the contents of that communication into an intelligible form but not including the display of signals on visual display devices intended to permit the examination of the technical characteristics of the signals without reference to the information content carried by the signals.

3. Military tactical communications means United States and Allied military exercise communications with the United States and abroad necessary for the production of simulated foreign intelligence and counterintelligence or to permit an analysis of communications security.

4. United States person. For purposes of signals intelligence activities only, the following guidelines will apply in determining whether a person is a United States person:

a. a person known to be currently in the United States will be treated as a United States person unless the nature of the person's communications or other available information concerning the person gives rise to a reasonable belief that such person is not a United States citizen or permanent resident alien.

b. a person known to be currently outside the United States, or whose location is not known, will not be treated as a United States person unless the nature of the person's communications or other available information concerning the person gives rise to a reasonable belief that such person is a United States citizen or permanent resident alien.

c. a person known to be an alien admitted for permanent residence may be assumed to have lost status as a United States person if the person leaves the United States and it is known that the person is not in compliance with the administrative formalities provided by law that enable such persons to reenter the United States without regard to the provisions of law that would otherwise restrict an alien's entry into the United States. the failure to follow the statutory procedures provided a reasonable basis to conclude that such alien has abandoned any intention of maintaining status as a permanent resident alien.

d. an unincorporated association whose headquarters are located outside the United States may be presumed not to be a United States person unless the collecting agency has information indicating that a substantial number of members are citizens of the United States or aliens lawfully admitted for permanent residence.

5. United States signals intelligence system means the unified organization for signals intelligence activities under the direction of the Director, National Security Agency/Chief, Central Security Service, comprised of the National Security Agency, the Central Security Service, the components of the military services authorized to conduct signals intelligence and such other entities (other that the federal bureau of investigation) as are authorized by the national security council or the secretary of defense to conduct signals intelligence. FBI activities are governed by procedures promulgated by attorney general.

C. Procedures

1. Foreign communications. The United States Signals Intelligence System may collect, process, retain, and disseminate foreign communications that are also communications of or concerning United States persons, but only in accordance with the classified annex to this portion.

2. Military tactical communications. The United States Signals Intelligence System may collect, process, retain, and disseminate military tactical communications that are also communications of or concerning United States persons but only in accordance with the classified annex to this procedure.

a. Collection. Collection efforts will be conducted in the same manner as in the case of signals intelligence for foreign intelligence purposes and must be designed in such a manner as to avoid to the extent feasible the intercept of communications not related to military exercises.

b. Retention and processing. Military tactical communications may be retained and processed without deletion of references to United States persons who are participants in, or are otherwise mentioned in exercise- related communications, provided that the communications of United States persons not participating in the exercise that are inadvertently intercepted during the exercise shall be destroyed as soon as feasible.

c. Dissemination. Dissemination of military tactical communications and exercise reports or information files derived from such communications shall be limited to those authorities and persons participating in or conducting reviews and critiques of such exercise.