Free Congress Research and Education Foundation 717 Second Street, NE Washington D.C. 20002 202/546-3000

ECHELON: America's Spy in the Sky

by Patrick S. Poole, Deputy Director, Center for Technology Policy

Executive Summary

In the greatest surveillance effort ever established, the US National Security Agency (NSA) has created a global spy system, codename ECHELON, which captures and analyzes virtually every phone call, fax, email and telex message sent anywhere in the world. ECHELON is controlled by the NSA and is operated in conjunction with the General Communications Head Quarters (GCHQ) of England, the Communications Security Establishment (CSE) of Canada, the Australian Defense Security Directorate (DSD), and the General Communications Security Bureau (GCSB) of New Zealand. These organizations are bound together under a secret 1948 agreement, UKUSA, whose terms and text remain under wraps even today.

The ECHELON system is fairly simple in design: position intercept stations all over the world to capture all satellite, microwave, cellular and fiber-optic communications traffic, and then process this information through the massive computer capabilities of the NSA, including advanced voice recognition and optical character recognition (OCR) programs, and look for code words or phrases (known as the ECHELON "Dictionary") that will prompt the computers to flag the message for recording and transcribing for future analysis. Intelligence analysts at each of the respective "listening stations" maintain separate keyword lists for them to analyze any conversation or document flagged by the system, which is then forwarded to the respective intelligence agency headquarters that requested the intercept.

But apart from directing their ears towards terrorists and rogue states, ECHELON is also being used for purposes well outside its original mission. The regular discovery of domestic surveillance targeted at American civilians for reasons of "unpopular" political affiliation or for no probable cause at all in violation of the First, Fourth and Fifth Amendments of the Constitution – are consistently impeded by very elaborate and complex legal arguments and privilege claims by the intelligence agencies and the US government. The guardians and caretakers of our liberties, our duly elected political representatives, give scarce attention to these activities, let alone the abuses that occur under their watch. Among the activities that the ECHELON targets are:

Political spying: Since the close of World War II, the US intelligence agencies have developed a consistent record of trampling the rights and liberties of the American people. Even after the investigations into the domestic and political surveillance activities of the agencies that followed in the wake of the Watergate fiasco, the NSA continues to target the political activity of "unpopular" political groups and our duly elected representatives. One whistleblower charged in a 1988 *Cleveland Plain Dealer* interview that, while she was stationed at the Menwith Hill facility in the 1980s, she heard real-time intercepts of South Carolina Senator Strom Thurmond. A former Maryland Congressman, Michael Barnes, claimed in a 1995 *Baltimore Sun* article that under the Reagan Administration his phone calls were regularly intercepted, which he discovered only after reporters had been passed transcripts of his conversations by the White House. One of the most shocking revelations came to light after several

GCHQ officials became concerned about the targeting of peaceful political groups and told the London Observer in 1992 that the ECHELON dictionaries targeted Amnesty International, Greenpeace, and even Christian ministries.

Commercial espionage: Since the demise of Communism in Eastern Europe, the intelligence agencies have searched for a new justification for their surveillance capability in order to protect their prominence and their bloated budgets. Their solution was to redefine the notion of national security to include economic, commercial and corporate concerns. An office was created within the Department of Commerce, the Office of Intelligence Liaison, to forward intercepted materials to major US corporations. In many cases, the beneficiaries of this commercial espionage effort are the very companies that helped the NSA develop the systems that power the ECHELON network. This incestuous relationship is so strong that sometimes this intelligence information is used to push other American manufacturers out of deals in favor of these mammoth US defense and intelligence contractors, who frequently are the source of major cash contributions to both political parties.

While signals intelligence technology was helpful in containing and eventually defeating the Soviet Empire during the Cold War, what was once designed to target a select list of communist countries and terrorist states is now indiscriminately directed against virtually every citizen in the world. The European Parliament is now asking whether the ECHELON communications interceptions violate the sovereignty and privacy of citizens in other countries. In some cases, such as the NSA's Menwith Hill station in England, surveillance is conducted against citizens on their own soil and with the full knowledge and cooperation of their government.

This report suggests that Congress pick up its long-neglected role as watchdog of the Constitutional rights and liberties of the American people, instead of its current role as lap dog to the US intelligence agencies. Congressional hearings ought to be held, similar to the Church and Rockefeller Committee hearings held in the mid-1970s, to find out to what extent the ECHELON system targets the personal, political, religious, and commercial communications of American citizens. The late Senator Frank Church warned that the technology and capability embodied in the ECHELON system represented a direct threat to the liberties of the American people. Left unchecked, ECHELON could be used by either the political elite or the intelligence agencies themselves as a tool to subvert the civil protections of Constitution and to destroy representative government in the United States.

Introduction

The culmination of the Cold War conflict brought home hard realities for many military and intelligence agencies who were dependent upon the confrontation for massive budgets and little civilian oversight. World War II Allied political and military alliances had quickly became intelligence alliances in the shadow of the Iron Curtain that descended upon Eastern Europe after the war.

But for some intelligence agencies the end of the Cold War just meant a shift in mission and focus, not a loss of manpower or financial resources. One such US governmental organization is the National Security Agency (NSA). Despite the disintegration of Communism in the former Soviet Union and throughout Eastern Europe, the secretive NSA continues to grow at an exponential rate in terms of budget, manpower and spying abilities. Other countries have noticed the rapid growth of NSA resources and facilities around

the world, and have decried the extensive spying upon their citizens by the US.

A preliminary report released by the European Parliament in January 1998 detailed research conducted by independent researchers that uncovered a massive US spy technology network that routinely monitors the telephone, fax and email information on citizens all over the world, but particularly in the European Union (EU) and Japan. Titled "An Appraisal of Technologies of Political Control,"<1> this report issued by the Scientific and Technological Options Assessment (STOA) committee of the European Parliament caused a tremendous stir in the establishment press in Europe. At least one major US media outlet, The New York Times,<2> covered the issuance of the report as well.

The STOA report also exposed a festering sore spot between the US and our EU allies. The widespread surveillance of citizens in EU countries by the NSA has been known and discussed by European journalists since 1981. The name of the system in question is ECHELON, and it is one of the most secretive spy systems in existence.

ECHELON is actually a vast network of electronic spy stations located around the world and maintained by five countries: the US, England, Canada, Australia, and New Zealand. These countries, bound together in a still-secret agreement called UKUSA, spy on each other's citizens by intercepting and gathering electronic signals of almost every telephone call, fax transmission and email message transmitted around the world daily. These signals are fed through the massive supercomputers of the NSA to look for certain keywords termed by the spy agencies as the ECHELON "dictionaries."

Most of the details of this mammoth spy system and the UKUSA agreement that supports it remain a mystery. What is known of ECHELON is the result of the efforts of journalists and researchers around the world who have labored for decades to uncover the operations of our government's most secret systems. The 1996 publication of New Zealand journalist Nicky Hager's book, Secret Power: New Zealand's Role in the International Spy Network,<3> provided the most detailed look at the system and has inflamed interest in ECHELON as well as the debate regarding its propriety.

This paper examines the expanse of the ECHELON system along with the intelligence agreements and exchanges that support it. The operation of ECHELON serves the NSA's goal of spying on the citizens of other countries while allowing them simultaneously to circumvent the prohibition on spying on US citizens. ECHELON is not only a gross violation of our Constitution, but it violates the good will of our European allies and threatens the privacy of innocent civilians around the world. The existence and expansion of ECHELON is a foreboding omen regarding the future of our Constitutional liberties. If a government agency can willingly violate the most basic components of the Bill of Rights without so much as congressional oversight and approval, we have reverted from a republican form of government to tyranny.

The Parties

The success of the Allied military effort in World War II was due in no small part to successes in gathering enemy intelligence information and cracking those respective military and diplomatic messages. In addition, the Allied forces were able to create codes and encryption devices that would effectively conceal sensitive information from prying Axis Power eyes. These coordinated signal intelligence (SIGINT) programs kept Allied information secure and left the enemies vulnerable.

But at the close of the conflict, a new threatening power – the Soviet Union – was beginning to provoke

the Cold War by enslaving Eastern Europe. These signal intelligence agencies now had a new enemy toward which to turn their electronic eyes and ears to ensure that the balance of power could be maintained. The volleys of electronic hardware and espionage that would follow for forty years would be the breeding ground of the ECHELON spy system.

The diplomatic foundation that was the genesis of ECHELON is the UKUSA agreement. The agreement has its roots in the BRUSA COMINT (communications intelligence) alliance formed in the early days of World War II and ratified on May 17, 1943 between the United Kingdom and the United States.<4> The Commonwealth SIGINT Organization formed in 1946-47 brought together the UK, Canada, Australia and New Zealand post-war intelligence agencies.<5> Forged in 1947 between the US and UK, the still-secret UKUSA agreement defined the relations between the SIGINT departments of those various governments. Direct agreements between the US and these agencies also define the intricate relationship that these organizations engage in.

Foremost among those agencies is the US National Security Agency (NSA), which represents the American interest. The NSA is designated as the "First Party to the Treaty." The Government Communications Headquarters (GCHQ) signed the UKUSA agreement on behalf of the UK and its Commonwealth SIGINT partners. This brought Australia's Defense Signals Directorate (DSD), the Canadian Communications Security Establishment (CSE) and New Zealand's Government Communications Security Bureau (GCSB) into the arrangement. While these agencies are bound by additional direct agreements with the US and each other, these four countries are considered the "Second Parties to the (UKUSA) Treaty." Third Party members include Germany, Japan, Norway, South Korea and Turkey. There are sources that indicate China may be included in this group on a limited basis as well.<6>

National Security Agency (US)

The prime mover in the UKUSA arrangement is undeniably the National Security Agency (NSA). The majority of funds for joint projects and facilities (discussed below), as well as the direction for intelligence gathering operations are issued primarily through the NSA. The participating agencies frequently exchange personnel, divide up intelligence collection tasks and establish common guidelines for classifying and protecting shared information. However, the NSA utilizes its role as the largest spy agency in the world to have its respective international intelligence partners do its bidding.

President Harry Truman established the NSA in 1952 in a presidential directive that remains classified to this day. The US government did not acknowledge the existence of the NSA until 1957. Its original mission was to conduct the signal intelligence (SIGINT) and communications security (COMSEC) for the US. President Ronald Reagan added the tasks of information systems security and operations security training in 1984 and 1988 respectively. A 1986 law charged the NSA with supporting combat operations for the Department of Defense.<7>

Headquartered at Fort George Meade, located between Washington D.C. and Baltimore, Maryland, the NSA boasts the most enviable array of intelligence equipment and personnel in the world. The NSA is the largest global employer of mathematicians, featuring the best teams of codemakers and codebreakers ever assembled. Their job is to crack the encryption codes of foreign and domestic electronic communications, forwarding the revealed messages to their enormous team of skilled linguists to review and analyze the messages in over 100 languages. The NSA is also responsible for creating the encryption codes that protect the US government's communications.

In its role as gang leader for UKUSA, the NSA is primarily involved with creating new surveillance and codebreaking technology, directing the other cooperating agencies to their targets, and providing them with training and tools to intercept, process and analyze enormous amounts of signals intelligence. By possessing what is arguably the most technologically advanced communications, computer and codebreaking equipment of any government agency in the world, the NSA serves as a competent and capable taskmaster for UKUSA.

The ECHELON Network

The vast network created by the UKUSA community stretches across the globe and into the reaches of space. Land-based intercept stations, intelligence ships sailing the seven seas and top-secret satellites whirling twenty thousand miles overhead all combine to empower the NSA and its UKUSA allies with access to the entire global communications network. Very few signals escape its electronic grasp.

Having divided the world up among the UKUSA parties, each agency directs their electronic "vacuum-cleaner" equipment towards the heavens and the ground to search for the most minute communications signal that traverses the system's immense path. The NSA facilities in the US cover the communications signals of both American continents; the GCHQ in Britain is responsible for Europe, Africa and Russia west of the Ural Mountains; the DSD in Australia assists in SIGINT collection in Southeastern Asia and the Southwest Pacific and Eastern Indian Ocean areas; the GSCB in New Zealand is responsible for Southern Pacific Ocean collections, particularly the South Pacific island nations group; and CSE in Canada handles interception in Northern Russian, Northern Europe and American communications.<8>

The Facilities

The backbone of the ECHELON network is the massive listening and reception stations directed at the Intelsat and Inmarsat satellites that are responsible for the vast majority of phone and fax communications traffic within and between countries and continents. The 20 Intelsat satellites follow a geo-stationary orbit locked onto a particular point on the Equator.<9> These satellites carry primarily civilian traffic, but they do additionally carry diplomatic and governmental communications that are of particular interest to the UKUSA parties.

Originally, only two stations were responsible for Intelsat intercepts: Morwenstow in England and Yakima in the state of Washington. However, when the Intelsat 5 series was replaced with the Intelsat 701 and 703 satellites, which had much more precise transmission beams that prohibited reception of Southern Hemisphere signals from the Yakima base in the Northern Hemisphere, additional facilities were constructed in Australia and New Zealand.<10>

Today, the Morwenstow station directs its ears towards the Intelsats traversing the atmosphere above the Atlantic and Indian Oceans that transmit to Europe, Africa and western parts of Asia. The Yakima station, located on the grounds of the Yakima Firing Station, targets Pacific Ocean communications in the Northern Hemisphere as well as the Far East. Another NSA facility at Sugar Grove, West Virginia, covers traffic for the whole of North and South America. A DSD station at Geraldton, Australia, and the Waihopai, New Zealand GCSB facility cover Asia, the South Pacific countries and the Pacific Ocean. An additional station on Ascension Island in the Atlantic Ocean between Brazil and Angola is suspected of covering the Atlantic Intelsat's Southern Hemisphere communications.<11>

Non-Intelsat satellites are monitored from these same stations, as well as from bases in Menwith Hill,

England; Shoal Bay, Australia; Leitrim, Canada; Bad Aibling, Germany, and Misawa, Japan. These satellites typically carry Russian and regional communications.<12> It is known that the Shoal Bay facility targets a series of Indonesian satellites, and the Leitrim station intercepts communications from Latin American satellites.<13>

Several dozen other radio listening posts operated by the UKUSA allies dot the globe as well, located at military bases on foreign soil and remote spy posts. These stations played a critical role in the time prior to the development of satellite communications because much of the world's communications traffic was transmitted on radio frequency bands. Particularly in the high-frequency (HF) range, radio communications continue to serve an important purpose despite the widespread use of satellite technology because their signals can be transmitted to military ships and aircraft across the globe. Shorter range very high-frequencies (VHF) and ultra high-frequencies (UHF) are also used for tactical military communications within national borders. Major radio facilities in the UKUSA network include Tangimoana, New Zealand; Bamaga, Australia, and the joint NSA/GCHQ facility at the Indian Ocean atoll of Diego Garcia.<14>

A separate high frequency direction finding (HFDF) network intercepts communications signals for the unique purpose of locating the positions of ships and aircraft. While these stations are not actually involved in the analysis of messages, they play a critical role in monitoring the movements of mobile military targets. The Canadian CSE figures prominently in the HFDF UKUSA network, hosting a major portion of the Atlantic and Pacific stations that monitored Soviet ship and submarine movements during the Cold War. On the Atlantic side, stations stretching from Bermuda, Gander (Newfoundland), Frobisher Bay (Arctic), Moncton (New Brunswick) and Leitrim (Ontario) monitor shipping and flight lanes under the direction of the NSA.<15>

Another major support for the ECHELON system are the US spy satellites and their corresponding reception bases scattered about the UKUSA empire. These space-based electronic communications "vacuum cleaners" pick up radio, microwave and cell phone traffic on the ground. They were launched by the NSA in cooperation with their sister spy agencies, the National Reconnaissance Office (NRO) and the Central Intelligence Agency (CIA). The Ferret series of satellites in the 1960s; the Canyon, Rhyolite and Aquacade in the 1970s; and the Chalet, Vortex, Magnum, Orion, and Jumpseat series of satellites in the 1980s, have given way to the new and improved Mercury, Mentor and Trumpet satellites during the 1990s.

Table I. US Spy Satellites in Current Use

Satellite	No.	Orbit	Manufacturer	Purpose
Advanced KH-11	3	200 miles	Lockheed Martin	5-inch resolution spy photographs
LaCrosse Radar Imaging	2	200-400 miles	Lockheed Martin	3 to 10-foot resolution spy photographs
Orion/Vortex	3	22,300 miles	TRW	Telecom surveillance

Trumpet	2	200-22,300 miles	Boeing	Surveillance of cellular phones
Parsae	3	600 miles	TRW	Ocean surveillance
Satellite Data Systems	2	200-22,300 miles	Hughes	Data Relay
Defense Support Program	4+	22,300 miles	TRW/Aerojet	Missile early warning
Defense Meteorological Support Program	2	500 miles	Lockheed Martin	Meteorology, nuclear blast detection

Source: MSNBC<16>

These surveillance satellites act as giant scoops picking up electronic communications, cell phone conversations and various radio transmissions. The downlink stations that control the operations and targeting of these satellites are under the exclusive control of the United States, despite their location on foreign military bases. The two primary downlink facilities are at Menwith Hill, England, and Pine Gap, Australia.

Inside Menwith Hill

The Menwith Hill facility is located in North Yorkshire near Harrogate, England. The important role that Menwith Hill plays in the ECHELON system was recognized by the recent European Parliament STOA report:

> *Within Europe, all email, telephone and fax communications are routinely intercepted by the United States National Security Agency, transferring all target information from the European mainland via the strategic hub of London then by satellite to Fort Meade in Maryland via the crucial hub at Menwith Hill in the North York Moors of the UK.*<17>

The existence and importance of the facility was first brought to light by British journalist and researcher Duncan Campbell in 1980.<18> Today, it is the largest spy station in the world, with over 25 satellite receiving stations and 1,400 American NSA personnel working with 350 UK Ministry of Defense staff on site. After revelations that the facility was coordinating surveillance for the vast majority of the European continent, the base has become a target for regular protests organized by local peace activists. It has also become the target of intense criticism by European government officials who are concerned about the vast network of civilian surveillance and economic espionage conducted from the station by the US.<19>

The beginnings of Menwith Hill go back to December 1951 when the US Air Force and British War Office signed a lease for the land, which had been purchased by the British government. The NSA took over the lease of the base in 1966, and they have continued to build up the facility ever since. Up until the mid-1970s, Menwith Hill was used for intercepting International Leased Carrier (ILC) and Non-Diplomatic Communications (NDC). Having received one of the first sophisticated IBM computers in the early 1960s, Menwith Hill was also used to sort through the voluminous unenciphered telex communications, which consisted of international messages, telegrams and telephone calls from the

government, business and civilian sectors looking for anything of political, military or economic value.<20>

The addition of the first satellite intercept station at Menwith Hill in 1974 raised the base's prominence in intelligence gathering. Eight large satellite communications dishes were installed during that phase of construction. Several satellite-gathering systems now dot the facility:<21>

STEEPLEBUSH – Completed in 1984, this $160 million system expanded the satellite surveillance capability and mission of the spy station beyond the bounds of the installation that began in 1974.

RUNWAY – Running east and west across the facility, this system receives signals from the second-generation geosynchronous Vortex satellites, and gathers miscellaneous communications traffic from Europe, Asia and the former Soviet Union. The information is then forwarded to the Menwith Hill computer systems for processing. RUNWAY may have recently been replaced or complemented by another system, RUTLEY.

PUSHER – An HFDF system that covers the HF frequency range between 3 MHz and 30 MHz (radio transmissions from CB radios, walkie-talkies, and other radio devices). Military, embassy, maritime and air flight communications are the main target of PUSHER.

MOONPENNY – Uncovered by British journalist Duncan Campbell in the 1980s, this system is targeted at the communication relay satellites belonging to other countries, including the Atlantic and Indian Ocean Intelsat satellites.

KNOBSTICKS I and II – The purpose of these antennae arrays are unknown, but they probably target military and diplomatic traffic throughout Europe.

GT-6 – A new system installed at the end of 1996, GT-6 is believed to be the receiver for the third generation of geosynchronous satellites termed Advanced Orion or Advanced Vortex. Another new polar orbit satellite called Advanced Jumpseat may be monitored from here as well.

STEEPLEBUSH II – An expansion of the 1984 STEEPLEBUSH system, this computer system processes information collected from the RUNWAY receivers gathering traffic from the Vortex satellites.

SILKWORTH – Constructed by Lockheed Corporation, the main computer system for Menwith Hill processes most of the information received by the various reception systems.

One shocking revelation about Menwith Hill came to light in 1997 during the trial of two women peace campaigners appealing their convictions for trespassing at the facility. In documents and testimony submitted by British Telecomm in the case, R.G. Morris, head of Emergency Planning for British Telecomm, revealed that at least three major domestic fiber-optic telephone trunk lines – each capable of carrying 100,000 calls simultaneously – were wired through Menwith Hill.<22> This allows the NSA to tap into the very heart of the British Telecomm network. Judge Jonathan Crabtree rebuked British Telecomm for his revelations and prohibited Mr. Morris from giving any further testimony in the case for "national security" reasons. According to Duncan Campbell, the secret spying alliance between Menwith Hill and British Telecomm began in 1975 with a coaxial connection to the British Telecomm microwave facility at Hunter's Stone, four miles away from Menwith Hill – a connection maintained even today.<23>

Additional systems (TROUTMAN, ULTRAPURE, TOTALISER, SILVERWEED, RUCKUS, et. al.) complete the monumental SIGINT collection efforts at Menwith Hill. Directing its electronic vacuum cleaners towards unsuspecting communications satellites in the skies, receiving signals gathered by satellites that scoop up the most minute signals on the ground, listening in on the radio communications throughout the air, or by plugging into the ground-based telecommunications network, Menwith Hill, alongside its sister stations at Pine Gap, Australia, and Bad Aibling, Germany, represents the comprehensive effort of the NSA and its UKUSA allies to make sure that no communications signal escapes its electronic net.

The ECHELON Dictionaries

The extraordinary ability of ECHELON to intercept most of the communications traffic in the world is breathtaking in its scope. And yet the power of ECHELON resides in its ability to decrypt, filter, examine and codify these messages into selective categories for further analysis by intelligence agents from the various UKUSA agencies. As the electronic signals are brought into the station, they are fed through the massive computer systems, such as Menwith Hill's SILKWORTH, where voice recognition, optical character recognition (OCR) and data information engines get to work on the messages.

These programs and computers transcend state-of-the-art; in many cases, they are well into the future. MAGISTRAND is part of the Menwith Hill SILKWORTH super-computer system that drives the powerful keyword search programs.<24> One tool used to sort through the text of messages, PATHFINDER (manufactured by the UK company, Memex),<25> sifts through large databases of text-based documents and messages looking for keywords and phrases based on complex algorithmic criteria. Voice recognition programs convert conversations into text messages for further analysis. One highly advanced system, VOICECAST, can target an individual's voice pattern, so that every call that person makes is intercepted and transcribed for future analysis.

Processing millions of messages every hour, the ECHELON dictionaries churn away 24 hours a day, 7 days a week, looking for targeted keyword series, phone and fax numbers, and specified voiceprints. It is important to note that very few messages and phone calls are actually transcribed and recorded by the system. The vast majority are filtered out after they are read or listened to by the system. Only those messages that produce keyword "hits" are tagged for future analysis. Again, it is not just the ability to collect the electronic signals that gives ECHELON its power; it is in the tools and technology that are able to whittle down the messages to only those that are important to the intelligence agencies.

Each station maintains a list of keywords (the "Dictionary") designated by each of the participating intelligence agencies. A Dictionary Manager from each of the respective agencies is responsible for adding, deleting or changing the keyword search criteria for their dictionaries at each of the stations.<26> Each of these station dictionaries are given codewords, such as COWBOY for the Yakima facility and FLINTLOCK for the Waihopai facility.<27> These codewords play a crucial identification role for the analysts who eventually look at the intercepted messages.

Each message flagged by the ECHELON dictionaries as meeting the specified criteria is sorted by a four-digit code representing the source or subject of the message (such as 3848 for political communications coming from and about Nigeria, or 8182 for communications about distribution of encryption technology,)<28> as well as the date, time and station codeword. Also included in the message headers are the codenames for the intended agency: ALPHA-ALPHA (GCHQ), ECHO-ECHO (DSD), INDIA-INDIA (GCSB), UNIFORM-UNIFORM (CSE), and OSCAR-OSCAR (NSA). These messages are then

transmitted to each agency's headquarters via a global computer system, PLATFORM,<29> that acts as the information nervous system for the UKUSA stations and agencies.

Every day, analysts located at the various intelligence agencies review the previous day's product. As it is analyzed, decrypted and translated, it can be compiled into the different types of analysis: reports, which are direct and complete translations of intercepted messages; "gists," which give basic information on a series of messages within a given category; and, summaries, which are compilations from both reports and gists.<30> These are then given classifications: MORAY (secret), SPOKE (more secret than MORAY), UMBRA (top secret), GAMMA (Russian intercepts) and DRUID (intelligence forwarded to non-UKUSA parties). This analysis product is the raison d'être of the entire ECHELON system. It is also the lifeblood of the UKUSA alliance.

The Problem

The ECHELON system is the product of the Cold War conflict, an extended battle replete with heightened tensions that teetered on the brink between annihilation and the diminished hostilities of détente and glasnost. Vicious cycles of mistrust and paranoia between the United States and the Soviet Empire fed the intelligence agencies to the point that, with the fall of communism throughout Eastern Europe, the intelligence establishment began to grasp for a mission that justified its bloated existence.

But the rise of post-modern warfare – terrorism – gave them all the justification they needed to develop even greater ability to spy on our enemies, our allies and our own citizens. ECHELON is the result of those efforts. The satellites that fly thousands of miles overhead and yet can spy out the most minute details on the ground and the secret submarines that troll the ocean floors that are able to tap into undersea communications cables<31> all power the efficient UKUSA signals intelligence machine.

There is a concerted effort by the heads of intelligence agencies, federal law enforcement officials and congressional representatives to defend the capabilities of ECHELON. Their persuasive arguments point to the tragedies seen in the bombings in Oklahoma City and the World Trade Center in New York City. The vulnerability of Americans abroad, as recently seen in the bombing of the American embassies in Dar es Salaam, Tanzania, and Nairobi, Kenya, emphasizes the necessity of monitoring those forces around the world that would use senseless violence and terror as political weapons against the US and its allies.

Intelligence victories add credibility to the arguments that defend such a pervasive surveillance system. The discovery of missile sites in Cuba in 1962; the capture of the Achille Lauro terrorists in 1995; the discovery of Libyan involvement in the bombing of a Berlin discotheque that killed one American (resulting in the 1996 bombing of Tripoli) and countless other incidents that have been averted (which are now covered by the silence of indoctrination vows and top-secret classifications) all point to the need for comprehensive signals intelligence gathering for the national security and defense of the United States.

But for the real threats and dangers to the peace and protection of American citizens at home and abroad, our Constitution is quite explicit in limiting the scope and powers of government. A fundamental foundation of free societies is that when controversies arise over the assumption of power by the state, power never defaults to the government, nor are powers granted without an extraordinary, explicit and compelling public interest. As the late Supreme Court Justice William Brennan pointed out:

> *The concept of military necessity is seductively broad, and has a dangerous plasticity. Because they invariably have the visage of overriding importance, there is always a temptation to invoke*

> *security "necessities" to justify an encroachment upon civil liberties. For that reason, the military-security argument must be approached with a healthy skepticism: Its very gravity counsels that courts be cautious when military necessity is invoked by the Government to justify a trespass on [Constitutional] rights.*<32>

Despite the necessity of confronting terrorism and the many benefits that are provided by the massive surveillance efforts embodied by ECHELON, there is a darker and dangerous side of these activities that is concealed by the cloak of secrecy surrounding the intelligence operations of the United States.

The discovery of domestic surveillance targeted at American civilians for reasons of "unpopular" political affiliation – or for no probable cause at all – in violation of the First, Fourth and Fifth Amendments of the Constitution is regularly impeded by very elaborate and complex legal arguments and privilege claims by the intelligence agencies and the US government. The guardians and caretakers of our liberties – our duly elected political representatives – give scarce attention to these activities, let alone the abuses, that occur under their watch. As pointed out below, our elected officials frequently become targets of ECHELON themselves, chilling any effort to check this unbridled power.

In addition, the shift in priorities resulting from the demise of the Soviet Empire and the necessity to justify intelligence capabilities resulted in a redefinition of "national security interests" to include espionage committed on behalf of powerful American companies. This quiet collusion between political and private interests typically involves the very same companies that are involved in developing the technology that empowers ECHELON and the intelligence agencies.

Domestic and Political Spying

When considering the use of ECHELON on American soil, the pathetic historical record of the NSA and CIA domestic activities in regards to the Constitutional liberties and privacy rights of American citizens provides an excellent guidepost for what may occur now with the ECHELON system. Since the creation of the NSA by President Truman, the spying capability of the NSA has frequently been used to monitor the activities of an unsuspecting public.

Project SHAMROCK

In 1945 Project SHAMROCK was initiated to obtain copies of all telegraphic information exiting or entering the United States. With the full cooperation of RCA, ITT and Western Union (representing almost all of the telegraphic traffic in the US at the time), the NSA was provided with daily microfilm copies of all incoming, outgoing and transiting telegraphs. This system changed dramatically when the cable companies began providing magnetic computer tapes to the agency, which enabled the agency to run all the messages through its HARVEST computer to look for particular keywords, locations, senders or addressees.

Project SHAMROCK became so successful that the in 1966 NSA and CIA set up a front company in lower Manhattan (where the offices of the telegraph companies were located) under the codename LPMEDLEY. At the height of Project SHAMROCK, 150,000 messages a month were printed and analyzed by NSA agents.<33>

NSA Director Lew Allen brought Project SHAMROCK to a crashing halt in May 1975 as congressional critics began to rip open the program's shroud of secrecy. The testimony of both the representatives from

the cable companies and of Director Allen at the hearings prompted Senate Intelligence Committee chairman, Sen. Frank Church, to conclude that Project SHAMROCK was "probably the largest government interception program affecting Americans ever undertaken."<34>

Project MINARET

A sister project to Project SHAMROCK, Project MINARET involved the creation of "watch lists" by each of the intelligence agencies and the FBI of those accused of "subversive" domestic activities. The watch lists included such notables as Martin Luther King, Malcolm X, Jane Fonda, Joan Baez and Dr. Benjamin Spock.

After the Supreme Court handed down its 1972 *Keith* decision,<35> which held that while the President could act to protect the country from unlawful and subversive activity designed to overthrow the government that same power did not extend to include warrantless electronic surveillance of domestic organizations, pressure came to bear on Project MINARET.<36> Attorney General Elliot Petersen shut down Project MINARET as soon as its activities were revealed to the Justice Department, despite the fact that the FBI (an agency under the Justice Department's authority) was actively involved with the NSA and other intelligence agencies in creating the watch lists.

Operating between 1967 and 1973, over 5,925 foreigners and 1,690 organizations and US citizens were included on the Project MINARET watch lists. Despite extensive efforts to conceal the NSA's involvement in Project MINARET, NSA Director Lew Allen testified before the Senate Intelligence Committee in 1975 that the NSA had issued over 3,900 reports on the watch-listed Americans.<37> Additionally, the NSA Office of Security Services maintained reports on at least 75,000 Americans between 1952 and 1974. This list included the names of anyone that was mentioned in a NSA message intercept.

Operation CHAOS

While the NSA was busy snooping on US citizens through Projects SHAMROCK and MINARET, the CIA got into the domestic spying act by initiating Operation CHAOS. President Lyndon Johnson authorized the creation of the CIA's Domestic Operations Division (DOD), whose purpose was to "exercise centralized responsibility for direction, support, and coordination of clandestine operations activities within the United States…."<38>

When Johnson ordered CIA Director John McCone to use the DOD to analyze the growing college student protests to the Administration's policy towards Vietnam, two new units were set up to target anti-war protestors and organizations: Project RESISTANCE, which worked with college administrators, campus security and local police to identify anti-war activists and political dissidents; and Project MERRIMAC, which monitored any demonstrations being conducted in the Washington D.C. area. The CIA then began monitoring student activists and infiltrating anti-war organizations by working with local police departments to pull off burglaries, illegal entries (black bag jobs), interrogations and electronic surveillance.<39>

After President Nixon came to office in 1969, all of these domestic surveillance activities were consolidated into Operation CHAOS. After the revelation of two former CIA agents' involvement in the Watergate break-in, the publication of an article about CHAOS in the *New York Times*<40> and the concerns about distancing themselves from its illegal domestic spying activities, the CIA shut down

Operation CHAOS. But during the life of the project, the Church Committee and the Commission on CIA Activities Within the United States (the Rockefeller Commission) revealed that the CIA had compiled files on over 13,000 individuals, including 7,000 US citizens and 1,000 domestic organizations.

The Foreign Intelligence Surveillance Court (FISC)

In response to the discovery of such a comprehensive effort by the previous administrations and the intelligence agencies, Congress passed legislation (the Foreign Intelligence Surveillance Act of 1978)<41> that created a top-secret court to hear applications for electronic surveillance from the FBI and NSA to provide as some check on the domestic activities of the agencies. In 1995, Congress granted the court additional power to authorize surreptitious entries. In all of these, Congressional intent was to provide a check on the domestic surveillance abuses mentioned above.

The seven-member court, comprised of federal District Court judges appointed by the Supreme Court Chief Justice, sits in secret in a sealed room on the top floor of the Department of Justice building. Public information about the court's hearings is scarce; each year the Attorney General is required by law to transmit to Congress a report detailing the number of applications each year and the number granted. With over 10,000 applications submitted to the FISC during the past twenty years, the court has only rejected one application (and that rejection was at the request of the Reagan Administration, who had submitted the application).

While the FISC was established to be the watchdog for the liberties of the Constitutional rights of the American people against domestic surveillance, it quickly became the lap dog of the intelligence agencies. Surveillance requests that would never receive a hearing in a state or federal court are routinely approved by the FISC. This has allowed the FBI to use the process to conduct surveillance to obtain evidence in circumvention of the US Constitution, and the evidence is then used in subsequent criminal trials. But the process established by Congress and the courts ensures that information regarding the cause or extent of the surveillance order is withheld from defense attorneys because of the classified nature of the court.<42> Despite Congress's initial intent for the FISC, it is doubtful that domestic surveillance by means of ECHELON comes under any scrutiny by the court.

Political Uses of ECHELON and UKUSA

Several incidents of domestic spying involving ECHELON have emerged from the secrecy of the UKUSA relationship. What these brief glimpses inside the intelligence world reveal is that, despite the best of intentions by elected representatives, presidents and prime ministers, the temptation to use ECHELON as a tool of political advancement and repression proves too strong.

Former Canadian spy Mike Frost recounts how former British Prime Minister Margaret Thatcher made a request in February 1983 to have two ministers from her own government monitored when she suspected them of disloyalty. In an effort to avoid the legal difficulties involved with domestic spying on high governmental officials, the GCHQ liaison in Ottawa made a request to CSE for them to conduct the three-week-long surveillance mission at British taxpayer expense. Frost's CSE boss, Frank Bowman, traveled to London to do the job himself. After the mission was over, Bowman was instructed to hand over the tapes to a GCHQ official at their headquarters.<43>

Using the UKUSA alliance as legal cover is seductively easy. As Spyworld co-author Michel Gratton puts it,

> *The Thatcher episode certainly shows that GCHQ, like NSA, found ways to put itself above the law and did not hesitate to get directly involved in helping a specific politician for her personal political benefit.… [T]he decision to proceed with the London caper was probably not put forward for approval to many people up the bureaucratic ladder. It was something CSE figured they would get away with easily, so checking with the higher-ups would only complicate things unnecessarily.*<44>

Frost also told of how he was asked in 1975 to spy on an unlikely target – Prime Minster Pierre Trudeau's wife, Margaret Trudeau. The Royal Canadian Mounted Police's (RCMP) Security Service division was concerned that the Prime Minister's wife was buying and using marijuana, so they contacted the CSE to do the dirty work. Months of surveillance in cooperation with the Security Service turned up nothing of note. Frost was concerned that there were political motivations behind the RCMP's request: "She was in no way suspected of espionage. Why was the RCMP so adamant about this? Were they trying to get at Pierre Trudeau for some reason or just protect him? Or were they working under orders from their political masters?"<45>

The NSA frequently gets into the political spying act as well. Nixon presidential aide John Ehrlichman revealed in his published memoirs, Witness to Power: The Nixon Years, that Henry Kissinger used the NSA to intercept the messages of then-Secretary of State William P. Rogers, which Kissinger used to convince President Nixon of Rogers' incompetence. Kissinger also found himself on the working end of the NSA's global net. Word of Kissinger's secret diplomatic dealings with foreign governments would reach the ears of other Nixon administration officials, incensing Kissinger. As former NSA Deputy Director William Colby pointed out, "Kissinger would get sore as hell…because he wanted to keep it politically secret until it was ready to launch."<46>

However, elected representatives have also become targets of spying by the intelligence agencies. In 1988, a former Lockheed software manager who was responsible for a dozen VAX computers that powered the ECHELON computers at Menwith Hill, Margaret Newsham, came forth with the stunning revelation that she had actually heard the NSA's real time interception of phone conversations involving South Carolina Senator Strom Thurmond. Newsham was fired from Lockheed after she filed a whistleblower lawsuit alleging that the company was engaged in flagrant waste and abuse. After a top secret meeting in April 1988 with then-chairman of the House Permanent Select Committee on Intelligence, Rep. Louis Stokes, Capitol Hill staffers familiar with the meeting leaked the story to the *Cleveland Plain Dealer*.<47> While Sen. Thurmond was reluctant to pressure for a thorough investigation into the matter, his office revealed at the time that the office had previously received reports that the Senator was a target of the NSA.<48> After the news reports an investigation into the matter discovered that there were no controls or questioning over who could enter target names into the Menwith Hill system.<49>

The NSA, under orders from the Reagan administration, also targeted Maryland Congressman Michael Barnes. Phone calls he placed to Nicaraguan officials were intercepted and recorded, including a conversation that he had with the Foreign Minister of Nicaragua protesting the implementation of martial law in that country. Barnes found out about the NSA's spying after White House officials leaked transcripts of his conversations to reporters. CIA Director William Casey, later implicated in the Iran-Contra affair, showed Barnes a Nicaraguan embassy cable that reported a meeting between embassy staff and one of Barnes' aides. The aide had been there on a professional call regarding an international affairs issue, and Casey asked for Barnes to fire the aide. Barnes replied that it was perfectly legal and legitimate for his staff to meet with foreign diplomats.

Says Barnes, “I was aware that NSA monitored international calls, that it was a standard part of intelligence gathering. But to use it for domestic political purposes is absolutely outrageous and probably illegal.”<50> Another former chair of the Senate Intelligence Committee has also expressed his concerns about the NSA’s domestic targeting. “It has always worried me. What if that is used on American citizens?” queried former Arizona Senator Dennis DeConcini. “It is chilling. Are they listening to my private conversations on my telephone?”<51>

Seemingly non-controversial organizations have ended up in the fixed gaze of ECHELON, as several former GCHQ officials confidentially told the *London Observer* in June 1992. Among the targeted organizations they name were Amnesty International, Greenpeace and Christian Aid, an American missions organization that works with indigenous pastors engaged in ministry work in countries closed to Western, Christian workers.<52>

In another story published by the *London Observer*, a former employee of the British Joint Intelligence Committee, Robin Robison, admitted that Margaret Thatcher had personally ordered the communications interception of the parent company of the *Observer*, Lonrho, after the *Observer* had published a 1989 expose charging bribes had been paid to Thatcher’s son, Mark, in a multi-billion dollar British arms deal with Saudi Arabia. Despite facing severe penalties for violating his indoctrination vows, Robison admitted that he had personally delivered intercepted Lonrho messages to Mrs. Thatcher’s office.<53>

It should hardly be surprising that ECHELON ends up being used by elected and bureaucratic officials to their political advantage or by the intelligence agencies themselves for the purpose of sustaining their privileged surveillance powers and bloated budgets. The availability of such invasive technology practically begs for abuse, although it does not justify its use to those ends. But what is most frightening is the targeting of such “subversives” as those who expose corrupt government activity, protect human rights from government encroachments, challenge corporate polluters, or promote the gospel of Christ. That the vast intelligence powers of the United States should be arrayed against legitimate and peaceful organizations is demonstrative not of the desire to monitor, but of the desire to control.

Commercial spying

With the rapid erosion of the Soviet Empire in the early 1990s, Western intelligence agencies were anxious to redefine their mission to justify the scope of their global surveillance system. Some of the agencies’ closest corporate friends quickly gave them an option – commercial espionage. By redefining the term “national security” to include spying on foreign competitors of prominent US corporations, the signals intelligence game has gotten ugly. And it very well may have prompted the recent scrutiny that ECHELON has endured by the European Union.

While UKUSA agencies have pursued economic and commercial information on behalf of their countries with renewed vigor with the passing of communism in Eastern Europe, the NSA practice of spying on behalf of US companies has a long history. Gerald Burke, who served as Executive Director of President Nixon’s Foreign Intelligence Advisory Board, notes commercial espionage was endorsed by the US government as early as 1970: “By and large, we recommended that henceforth economic intelligence be considered a function of the national security, enjoying a priority equivalent to diplomatic, military, and technological intelligence.”<54>

To accommodate the need for information regarding international commercial deals, the intelligence agencies set up a small, unpublicized department within the Department of Commerce, the Office of

Intelligence Liaison. This office receives intelligence reports from the US intelligence agencies about pending international deals that it discreetly forwards to companies that request it or may have an interest in the information. Immediately after coming to office in January 1993, President Clinton added to the corporate espionage machine by creating the National Economic Council, which feeds intelligence to "select" companies to enhance US competitiveness. The capabilities of ECHELON to spy on foreign companies is nothing new, but the Clinton administration has raised its use to an art:

- In 1990 the German magazine *Der Speigel* revealed that the NSA had intercepted messages about an impending $200 million deal between Indonesia and the Japanese satellite manufacturer NEC Corp. After President Bush intervened in the negotiations on behalf of American manufacturers, the contract was split between NEC and AT&T.
- In 1994, the CIA and NSA intercepted phone calls between Brazilian officials and the French firm Thomson-CSF about a radar system that the Brazilians wanted to purchase. A US firm, Raytheon, was a competitor as well, and reports prepared from intercepts were forwarded to Raytheon.<55>
- In September 1993, President Clinton asked the CIA to spy on Japanese auto manufacturers that were designing zero-emission cars and to forward that information to the Big Three US car manufacturers: Ford, General Motors and Chrysler.<56> In 1995, the New York Times reported that the NSA and the CIA's Tokyo station were involved in providing detailed information to US Trade Representative Mickey Kantor's team of negotiators in Geneva facing Japanese car companies in a trade dispute.<57> Recently, a Japanese newspaper, *Mainichi*, accused the NSA of continuing to monitor the communications of Japanese companies on behalf of American companies.<58>
- *Insight Magazine* reported in a series of articles in 1997 that President Clinton ordered the NSA and FBI to mount a massive surveillance operation at the 1993 Asian/Pacific Economic Conference (APEC) hosted in Seattle. One intelligence source for the story related that over 300 hotel rooms had been bugged for the event, which was designed to obtain information regarding oil and hydro-electric deals pending in Vietnam that were passed on to high level Democratic Party contributors competing for the contracts.<59> But foreign companies were not the only losers: when Vietnam expressed interest in purchasing two used 737 freighter aircraft from an American businessman, the deal was scuttled after Commerce Secretary Ron Brown arranged favorable financing for two new 737s from Boeing.<60>

But the US is not the only partner of the UKUSA relationship that engages in such activity. British Prime Minister Margaret Thatcher ordered the GCHQ to monitor the activities of international media mogul Robert Maxwell on behalf of the Bank of England.<61> Former CSE linguist and analyst Jane Shorten claimed that she had seen intercepts from Mexican trade representatives during the 1992-1993 NAFTA trade negotiations, as well as 1991 South Korean Foreign Ministry intercepts dealing with the construction of three Canadian CANDU nuclear reactors to the Koreans in a $6 billion deal.<62> Shorten's revelation prompted Canadian Prime Minister Sheila Copps to launch a probe into the allegations after the Mexicans lodged a protest.

But every spy agency eventually gets beat at their own game. Mike Frost relates in Spyworld how an accidental cell phone intercept in 1981 of the American Ambassador to Canada discussing a pending grain deal that the US was about to sign with China provided Canada with the American negotiating strategy for the deal. The information was used to outbid the US, resulting in a three year, $2.5 billion contract for the Canadian Wheat Board. CSE out-spooked the NSA again a year later when Canada snagged a $50 million wheat sale to Mexico.<63>

Another disturbing trend regarding the present commercial use of ECHELON is the incestuous relationship that exists between the intelligence agencies and the US corporations that develop the technology that fuels their spy systems. Many of the companies that receive the most important commercial intercepts – Lockheed, Boeing, Loral, TRW and Raytheon – are actively involved in the manufacturing and operation of many of the spy systems that comprise ECHELON. The collusion between intelligence agencies and their contractors is frightening in the chilling effect it has on creating any foreign or even domestic competition. But just as important is that it is a gross misuse of taxpayer-financed resources and an abuse of the intelligence agencies' capabilities.

The Warning

While the UKUSA relationship is a product of Cold War political and military tensions, ECHELON is purely a product of the 20th Century – the century of statism. The modern drive toward the assumption of state power has turned legitimate national security agencies and apparati into pawns in a manipulative game where the stakes are no less than the survival of the Constitution. The systems developed prior to ECHELON were designed to confront the expansionist goals of the Soviet Empire – something the West was forced out of necessity to do. But as Glyn Ford, European Parliament representative for Manchester, England and the driving force behind the European investigation of ECHELON, has pointed out: "The difficulty is that the technology has now become so elaborate that what was originally a small client list has become the whole world."<64>

What began as a noble alliance to contain and defeat the forces of communism has turned into a carte blanche to disregard the rights and liberties of the American people and the population of the free world. As has been demonstrated time and again, the NSA has been persistent in subverting not just the intent of the law in regards to the prohibition of domestic spying, but the letter as well. The laws that were created to constrain the intelligence agencies from infringing on our liberties are frequently flaunted, re-interpreted and revised according to the bidding and wishes of political spymasters in Washington D.C. Old habits die hard, it seems.

As stated above, there is a need for such sophisticated surveillance technology. Unfortunately, the world is filled with criminals, drug lords, terrorists and dictators that threaten the peace and security of many nations. The thought that ECHELON can be used to eliminate or control these international thugs is heartening. But defenders of ECHELON argue that the rare intelligence victories over these forces of darkness and death give wholesale justification to the indiscriminate surveillance of the entire world and every member in it. But more complicated issues than that remain.

The shameless and illegal targeting of political opponents, business competitors, dissidents and even Christian ministries stands as a testament that if America is to remain free, we must bind these intelligence systems and those that operate them with the heavy chains of transparency and accountability to our elected officials. But the fact that the ECHELON apparatus can be quickly turned around on those same officials in order to maintain some advantage for the intelligence agencies indicates that these agencies are not presently under the control of our elected representatives.

That Congress is not aware or able to curtail these abuses of power is a frightening harbinger of what may come here in the United States. The European Parliament has begun the debate over what ECHELON is, how it is being used and how free countries should use such a system. Congress should join that same debate, with the understanding that consequences of ignoring or failing to address these issues could foster the demise of our republican form of government. Such is the threat, as Senator Frank Church

warned the American people over twenty years ago.

> ***At the same time, that capability at any time could be turned around on the American people and no American would have any privacy left, such [is] the capability to monitor everything: telephone conversations, telegrams, it doesn't matter. There would be no place to hide. If this government ever became a tyranny, if a dictator ever took charge in this country, the technological capacity that the intelligence community has given the government could enable it to impose total tyranny, and there would be no way to fight back, because the most careful effort to combine together in resistance to the government, no matter how privately it was done, is within the reach of the government to know. Such is the capability of this technology…***
>
> ***I don't want to see this country ever go across the bridge. I know the capacity that is there to make tyranny total in America, and we must see to it that this agency and all agencies that possess this technology operate within the law and under proper supervision, so that we never cross over that abyss. That is the abyss from which there is no return.***<65>

Endnotes

1. Steve Wright, An Appraisal of Technologies of Political Control, European Parliament: Scientific and Technologies Options Assessment, Luxembourg, January 6, 1998.
2. Bruno Giussani, "European Study Paints a Chilling Portrait of Technology's Uses," *The New York Times*, February 24, 1998.
3. Nelson, New Zealand: Craig Potton Publishing, 1996.
4. Desmond Ball and Jeffrey Richelson, *The Ties That Bind: Intelligence Cooperation Between the UKUSA Countries*, (Boston: Allen & Unwin, 1985) pp. 137-8.
5. *Ibid.*, 142-143.
6. *Secret Power*, p. 40. See note 3.
7. National Security Agency, *About the NSA*.
8. *The Ties that Bind*, p. 143.
9. The coverage area of the various Intelsat satellites can be found at the Intelsat website at: http://www.intelsat.com/cmc/connect/globlmap.htm
10. *Secret Power*, p. 28.
11. *Ibid.*, p. 35.
12. *Ibid.*
13. Marco Campagna, *Un Systeme De Surveillance Mondial*, Cahiers de Television (CTV-France), June 1998.
14. *Secret Power*, pp. 35-36, 150; *Ties That Bind*, pp. 240-207.
15. Mike Frost and Michel Graton, *Spyworld: How C.S.E. Spies on Canadians and the World* (Toronto: Seal/McClelland-Bantam, 1995), p. 35
16. Robert Windrem, "Spy Satellites Enter New Dimension," *MSNBC* and *NBC News*, August 8, 1998.
17. *An Appraisal of Technology of Political Control*, p. 19.
18. Duncan Campbell and Linda Melvern, "America's Big Ear on Europe," *New Statesman*, July 18, 1980, pp. 10-14.
19. Simon Davies, "EU Simmers Over Menwith Listening Post," *London Telegraph*, July 16, 1998.
20. Nicholas Rufford, "Spy Station F83," *The Sunday (London) Times*, May 31, 1998.

21. Duncan Campell, "Somebody's Listening," *The New Statesman*, August 12, 1988, pp. 10-12; "The Hill," Dispatches, BBC Channel 4, October 6, 1993 (transcript provided by Duncan Campbell); Loring Wirbel, "Space – Intelligence Technology's Embattled Frontier," *Electronic Engineering Times*, April 22, 1997; Nicholas Rufford, "Cracking the Menwith Codes," *The Sunday (London) Times*, May 31, 1998.
22. Duncan Campbell, *BT Condemned for Listing Cables to US SIGINT Station*, September 4, 1997.
23. *Ibid.*; *Spy Station F83*.
24. Mentioned in *Dispatches: The Hill*.
25. *An Appraisal of Technologies of Political Control*, p. 19. Memex maintains a website describing their defense and intelligence products and contracts: http://www.memex.co.uk/prod/intelligence/comm.html
26. *Secret Power*, p. 49.
27. *Ibid.*, pp. 165-166.
28. Nicky Hager, "Exposing the Global Surveillance System," *Covert Action Quarterly*, No. 59, Winter 1996-1997, p. 14.
29. James Bamford, *The Puzzle Palace: Inside the National Security Agency, America's Most Secret Intelligence Organization*, (New York: Penguin Books, 1983), pp. 138-139.
30. *Secret Power*, p. 45.
31. *Ties That Bind*, pp. 223-224.
32. *Brown v. Glines*, 444 U.S. 348 (1980).
33. *Puzzle Palace*, p. 314, 459.
34. *External Collection Program*: U.S. Senate, Select Committee on Intelligence, Supplementary Detailed Staff Reports on Intelligence and the Rights of Americans, Final Report, Book III, April 23, 1976, p. 765.
35. *United States v. United States District Court*, 407 U.S. 297 (1972)
36. *Puzzle Palace*, pp. 370-373.
37. *Puzzle Palace*, p. 381.
38. Verne Lyon, "Domestic Surveillance: The History of Operation Chaos," Covert Action Information Bulletin, Summer 1990. Lyon is a former CIA undercover operative who was recruited specifically for Operation CHAOS.
39. *Ibid.*
40. Seymour Hersh, "Huge CIA Operation Reported in U.S. Against Antiwar Forces," *New York Times* (December 22, 1974), p. 1.
41. 50 USC Sec. 1801, et. seq.
42. For more information on the FISC, see this author's essay "Inside America's Secret Court: The Foreign Intelligence Surveillance Court," *The Privacy Papers*, No. 2 (Washington D.C.: Free Congress Foundation, 1998).
43. *Spyworld*, pp. 234-238.
44. *Ibid.*, p. 238.
45. *Ibid.*, pp. 93-97.
46. Scott Shane and Tom Bowman, "Catching Americans in NSA's Net," *Baltimore Sun*, December 12, 1995.
47. Keith C. Epstein and John S. Long, "Security Agency Accused of Monitoring U.S. Calls," *Cleveland Plain Dealer*, July 1, 1988, pp. 1A, 10A.
48. Pete Carey, "NSA Accused of Forbidden Phone Taps," *San Jose Mercury News*, July 2, 1988, p. 1A.
49. *Somebody's Listening*, p. 11.
50. *Catching Americans in NSA's Net*.
51. *Ibid.*
52. John Merritt, "UK: GCHQ Spies on Charities and Companies – Fearful Whistleblowers Tell of

Massive Routine Abuse," *Observer (London)*, June 18, 1992.
53. Hugh O'Shaughnessy, "Thatcher Ordered Lonrho Phone-Tap Over Harrods Affairs," *Observer (London)*, June 28, 1992; cited in Secret Power, p. 54.
54. *Dispatches: The Hill*, op. cit.
55. Tom Bowman and Scott Shane, "Battling High-Tech Warriors," *Baltimore Sun*, December 15, 1995.
56. Robert Dreyfuss, "Company Spies," *Mother Jones*, May/June 1994.
57. Cited in Bruce Livesey, "Trolling for Secrets: Economic Espionage is the New Niche for Government Spies," *Financial Post (Canada)*, February 28, 1998.
58. U.S. Spy Agency Helped U.S. Companies Win Business Overseas, *Nikkei English News*, September 21, 1998.
59. Timothy W. Maier, "Did Clinton Bug Conclave for Cash," *Insight*, September 15, 1997. The three article series is online at: http://www.insightmag.com/investiga/apecindex.html
60. Timothy W. Maier, "Snoops, Sex and Videotape," *Insight*, September 29, 1997.
61. Matthew Fletcher, "Cook Faces Quiz on Big Brother Spy Net," *Financial Mail (England)*, March 1, 1998.
62. *Trolling for Secrets*, op. cit.
63. *Spyworld*, pp. 224-227.
64. Lucille Redmond, "Suddenly There Came a Tapping…", *The Sunday Business Post (Ireland)*, March 9, 1998.
65. National Broadcasting Company, "Meet the Press" (Washington D.C.: Merkle Press, 1975), transcript of August 17, 1975, p. 6; quoted in *Puzzle Palace*, p. 477.