

### Wine Racks

Discount Clearance Mention  
Current Sale  
[www.cellar-creations.com.au](http://www.cellar-creations.com.au)

### We ARCHIVE for you...

efficient. accurate. confidential.  
wide  
format.print.copy.scan.archive  
[www.tasprint.com.au](http://www.tasprint.com.au)

### Secret Satellite TV on PC

Shocking discovery they don't  
Want you to know.  
[www.secretsatellite.com](http://www.secretsatellite.com)

### Compare Health Insurance

Compare 100s policy  
combinations many funds get  
cheaper cover here!  
[www.iselect.com.au](http://www.iselect.com.au)

[Ads by Goooooogle](#)

## Trial Subscription

Try 3 Issues of *Smart Computing*, RISK-FREE!

[What is a risk-free subscription?](#)



First Name:

Last Name:

Address:

City:

State:

ZIP:

Email:

**SEND ME SMART COMPUTING!**

[Canadian residents click here](#)  
[All other foreign residents click here](#)

## The Concealment Of Echelon

### *Big Brother*

April 2000 • Vol.8 Issue 4

# The Concealment Of Echelon

## A Network Of Spies In A Web Of Lies



It's the rumor that conspiracy books and movies are based on: A top-secret network that keeps tabs on individuals around the globe. Echelon is the name given to this surveillance network that consists of a group of governments—in what we call the free world—that allegedly are spying on their own citizens and those of other countries.

You wouldn't expect to read about this in a non-fiction magazine devoted to helping consumers learn everything they need to know about running their home and office computers, but nevertheless, you are. Why? Well, because there's a solid possibility that this network exists—and that it exists in part due to the Internet. Rumors about this network, Echelon (the source of this moniker is unknown), have been floating around for many years; but in the past couple of years, these "rumors" have been making their way into reputable reports.

Only recently, though, have we started to hear statements from a few of those who are in a position to know about the network that is purported to capture satellite, microwave, cellular, and fiber-optic communications worldwide. Some estimate that the number of communications that Echelon eavesdrops on ranges as high as *3 billion messages each day*, which consists of a combination of e-mail, phone, and fax communications.

What Echelon is exactly is still unclear, but another thing *is* clear: You won't find out about Echelon from the National Security Agency (NSA), one of the five government organizations that appear to be involved in running this top-secret network. It is widely assumed that the U.S. government is working with security agencies in the United Kingdom, Australia, New Zealand, and Canada in running Echelon. But when *Smart Computing* contacted the U.S. government agency, we were told that the NSA (and Central Security Service [CSS]) doesn't "confirm or deny that Echelon exists." Instead, the agency faxed us the following statement:

"NSA/CSS does not comment on actual or alleged intelligence activities. The National Security Agency (NSA/CSS) operates in strict accordance with U.S. laws and regulations in protecting the privacy rights of U.S. persons. Its activities are conducted with the highest constitutional, legal, and ethical standards."

So, for answers on what Echelon is and its intended purpose, we turned to other sources.

## ■ Where It Started.

To understand what Echelon is, it helps to look at the progression of reports that have been published for the public because each new report and story adds particulars about what the network seems to be and how it works.

One of the first exposés of Echelon was contained in "Secret Power: New Zealand's Role in the International Spy Network," a book by Nicky Hager, who has long kept track of intelligence activities in New Zealand (see "Who's Watching The Watchers?" sidebar). Published in 1996, it was soon followed by a number of other reports.

Another early indication that Echelon exists, as far as the general public is concerned, appeared in the first few months of 1997, when a newsletter called CovertAction Quarterly included an article called "Hager on ECHELON" that gave supposed details on what Echelon does. The piece claimed that Echelon started out as a joint project between the United States and the United Kingdom around the time of World War II and was formed to gather intelligence on the Soviet Union. In the ensuing decades, the NSA (of the United States) and the Government Communications Headquarters (GCHQ; of the United Kingdom) were joined by three other intelligence agencies in this project: the Communications Security Establishment (Canada), the Defence Signals Directorate (DSD; Australia), and the Government Communications Security Bureau (New Zealand).

Echelon, the report claimed, focused on the alliance's ability to monitor almost all telephone calls in the United States and Europe. The report noted that the calls were digitized and then analyzed with a sophisticated keyword search technology.

The report further noted that each agency has its own Echelon "dictionary," which contains information on keywords and phrases it wishes to track, and when any of the computer systems of the five intelligence agencies pick up communications containing these keywords, that information is sent along to the agency whose dictionary contains the particular keyword. In addition to telephone calls, it monitors e-mail, fax, telex, as well as analog and digital cellular phone calls.

Just how do these keyword searches work? According to Barry Steinhardt, the associate director of the American Civil Liberties Union, the NSA holds patents on sophisticated programs that look for patterns in words. It isn't as simple as listening for a single word; instead, the system looks for roots of words, grammatical structures, and other patterns in identifying targeted conversations.

After the CovertAction Quarterly published "Hager on ECHELON," more reports continued to surface, and the European Parliament decided to get in on the action by commissioning Duncan Campbell, an investigative journalist and television producer in the United Kingdom, to discover what he could about Echelon.

The early 1998 report from Campbell (published in part on the Echelon Watch Web site; see the "Who's Watching The Watchers" sidebar) repeated the assertions of the CovertAction Quarterly newsletter on how information is analyzed and gave more details about how Echelon works, including a description of how communications in Europe are intercepted and transferred from London by satellite to Fort Meade, Maryland. Additionally, the report says it obtained quotes from Nicky Hager's research that quotes the "highly placed intelligence operatives" who spoke to *The Observer*, a publication based in London:

"We feel we can no longer remain silent regarding that which we regard to be gross malpractice and negligence within the establishment in which we operate.' They gave as examples: GCHQ interception of three charities, including Amnesty International and Christian Aid. 'At any time, GCHQ is able to home in on their communications for a routine target request,' the GCHQ source said. In the case of phone taps, the procedure is known as Mantis. With telexes, it's called Mayfly. By keying in a code relating to third-world aid, the source was able to demonstrate telex "fixes" on the three organisations. 'With no system of accountability, it is difficult to discover what criteria determine who is not a target.'"

Still, few officials at that time were willing to comment publicly on whether Echelon exists and how it works. That has changed in the past few months, however. In November of 1999, Australia's Inspector General of Intelligence, Bill Blick, was interviewed by the British Broadcasting Corporation (BBC), and he confirmed that those investigating Echelon were on the right track. The BBC quoted Blick as saying that a large number of radio communications are collected by agencies such as Australia's DSD in the interest of national security, and that in some circumstances, this information is passed along to the United States and the United Kingdom.

Blick's comments were given further weight when the security intelligence service in New Zealand issued a year-end report to the government that confirmed outside nations were using its bases. According to television broadcaster TVNZ, the report said the bases, Tangimoana in the North Island and Waihopai in the South Island, "are useful to and are accessible by the intelligence of New Zealand's intelligence partners." This caused a furor with the Green party in New Zealand, which is pushing for an official inquiry into the intelligence gathering and sharing procedures.

Although much of what we know about Echelon has been originating overseas, the NSA is beginning to indirectly release information about Echelon. NSA officials still have not publicly commented on the network, but NSA recently declassified some documents that a researcher claims references the project.

Jeffery Richelson, a researcher at the National Security Archives (not to be confused with the National Security Agency), obtained a group of documents under the Freedom of Information Act, and he published his findings on the Web site at <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index2.html>. To summarize, the findings appear to confirm that Echelon exists, but Richelson says the network appears to be much less intrusive than feared by many. A number of watchdog groups have raised concerns that the network is used to spy on American citizens (which would be illegal), but Richelson says he doubts the agencies have done so.

That belief is seconded by Michael Jacobs, a spokesperson at the NSA, who was reported by Wired News in late January to say that the NSA would not spy on its own citizens. He added that that is not the job of the NSA, and the agency follows strict internal policies that keep it from doing so.

### ■ The Public Swiftly Reacts.

Despite NSA's assurances, a number of citizen groups and organizations are trying to get as much about Echelon out in the open as possible to ensure that the network is not illegally spying on domestic citizens, which is prohibited according to the guidelines set forth in the Foreign Intelligence Surveillance Act of 1978.

In October 1999, a group of Internet users around the globe attempted to cripple Echelon by flooding it with thousands of fictitious messages related to terrorist bombings and attacks. It is unknown what effect, if any, this mass e-mail campaign had on the network.

Others have taken a more long-term approach. Early last year, the Electronic Privacy Information Center (EPIC) filed a request under the Freedom of Information Act asking for documents related to Echelon. But David Sobel, general counsel for EPIC, says the request was ignored. So, in December 1999, EPIC filed a lawsuit in the District of Columbia asking that all internal documents discussing Echelon's legality be made public. In January, the judge issued a scheduling order, so we can expect NSA to respond by early spring.

EPIC is not alone in its calls for more information. A group of six privacy organizations—The American Civil Liberties Union, the Center for Democracy and Technology, the Eagle Forum, the Electronic Frontier Foundation, the Electronic Privacy Information Center, and the Free Congress Foundation—have united in monitoring Echelon. In a memo released in June 1999, the groups raised two main questions:

1. Are the rules governing U.S. government surveillance overseas adequate to protect the rights of U.S. citizens?
2. Are the rules governing the receipt of intercepted information from foreign governments concerning the communications of Americans adequate to protect the rights of U.S. citizens?

These questions may not be answered right away, but they are not going unnoticed. Even though Echelon is apparently run by one arm of the U.S. government, other government groups are concerned by the potential harm the network could inflict upon its own citizens. Several members of the U.S. Congress have been leading the way in trying to learn more about Echelon.

Earlier in 1999, the House Permanent Select Committee on Intelligence, which is chaired by Porter Goss, had asked the NSA to turn over information regarding Echelon. NSA delayed the process for several months, but the committee finally received documents in December, which have not been made public. During the same month, President Clinton signed the Intelligence Authorization Act, which contains a provision (inserted by Representative Bob Barr of Georgia) that asks the NSA to turn over information on the legal standards used regarding Echelon. By law, the NSA has 60 days to comply.

Barr's office continues to work on Echelon, says spokesperson Brad Alexander. Alexander says Barr has gotten a verbal commitment from Dan Burton, the chairman of the Committee on Government Reform, to hold hearings on the matter. And those hearings could possibly reveal much more to the public about Echelon than we know now.

"It's essential that the Congress get to the bottom of this," ACLU's Steinhardt says, "because only Congress has the power to get the NSA to disclose this [information]." ■

*by Heidi V. Anderson*

## Who's Watching The Watchers?

Echelon might be monitoring citizens worldwide, but a number of organizations and individuals worldwide are monitoring Echelon, as well. Here's an introduction to a few Web sites keeping tabs on Echelon.



### *Involved In Echelon?*

#### **Echelon Watch**

(<http://www.aclu.org/echelonwatch/index.html>).

The American Civil Liberties Union, in cooperation with the Free Congress Foundation, the Electronic Privacy Information Center, Cyber-Rights and Cyber-Liberties (United Kingdom), and the Omega Foundation, has created one of the most comprehensive Web sites devoted to Echelon. The site carries a list of frequently asked questions (FAQs), links to articles around the globe, a special section on Echelon activities in the United States, and an online form for urging Congress to investigate Echelon. Echelon Watch also carries information about other government surveillance systems, including two in Russia and three in western Europe.

**JYA** (<http://www.jya.com>). This site is a bit tough to navigate, but if you have the patience, you will discover a wealth of files related to Echelon. View the Truman memorandum that established the National Security Agency in 1952. Read information provided by a then-anonymous former analyst of the National Security Agency provided in 1972. Explore the working document presented by the European Parliament in 1998. To find all of these files, click the Echelon link on the Cryptome section of the home page. On the ensuing page, click the Echelon link under the Archives heading at the bottom of the page.

#### **Secret Power: New Zealand's Role in the International Spy Network**

(<http://www.fas.org/irp/eprint/sp/index.html>). Along with Duncan Campbell, journalist Nicky Hager is widely credited with bringing Echelon to the public light. Here, you can read about the 1996 book that discussed New Zealand's role in Echelon and view some of the actual text. "It was with some apprehension that I learned that Nicky Hager was researching the activity of our intelligence

community. He has long been a pain in the establishment's neck," says a portion of the foreword by former Prime Minister David Lange.

### **ECHELON: America's Secret Global Surveillance Network**

(<http://fly.hiwaay.net/~pspoole/echelon.html>) Patrick S. Poole, the deputy director for the Center for Technology Policy, has composed a comprehensive report that covers the Echelon network, its partners, its technology, political uses, and more. In addition, the site links to a handful of Echelon news stories from around the world. ■

## **The Network Known As Echelon**

While the National Security Agency and security organizations from outside the U.S. refuse to confirm the existence of Echelon, a number of countries are reportedly involved in the network. The following countries are most frequently mentioned by various sources as participants in Echelon: United States; United Kingdom; Canada; Australia; and New Zealand. ■



#### **SENTINEL Security Intl.**

Eliminate the risk of eavesdropping and industrial espionage  
[www.sentinel-corp.com](http://www.sentinel-corp.com)

#### **Fix FAQ.inf**

Download a Free Scan & Repair  
FAQ.inf Instantly!  
[www.TuneupAdvisor.com](http://www.TuneupAdvisor.com)

#### **Archives**

Discover Your Family History With  
Our Free Australian & UK records!  
[www.ancestry.com.au](http://www.ancestry.com.au)

#### **Find Your Documents 24x7**

"Online Access to Offsite Archives"  
Secure DataBank Document Vault  
[www.tmdaust.com](http://www.tmdaust.com)

[Ads by Goooooogle](#)

---

**Want more information about a topic you found of interest while reading this article? Type a word or phrase that identifies the topic and click "Search" to find relevant articles from within our editorial database.**

**Enter A Subject** (key words or a phrase):

- ALL Words ('digital' AND 'photography')
- ANY Words ('digital' OR 'photography')
- Exact Match ('digital photography'- all words MUST appear together)

Search

[Return to Previous Page](#)

---

[Home](#) [Copyright & Legal Information](#) [Privacy Policy](#) [Site Map](#) [Contact Us](#)

Copyright © 2007 Sandhills Publishing Company U.S.A. All rights reserved.