Lawmakers Raise Questions About International Spy Network

By NIALL McKAY

A national surveillance network established by the National Security Agency and British intelligence services has come under scrutiny in recent weeks, as lawmakers in the United States question whether the network, known as Echelon, could be used to monitor American citizens.

Last week, the House Committee on Intelligence requested that the National Security Agency and the Central Intelligence Agency provide a detailed report to Congress explaining what legal standards they use to monitor the conversations, transmissions and activities of American citizens.

The request is part of an amendment to the annual intelligence budget bill, the Intelligence Reauthorization Act. It was proposed by Bob Barr, a Georgia Republican and was supported by the chairman of the House Intelligence Committee, Porter Goss, a Florida Republican. The amendment was passed by the House on May 13 and will now go before the Senate.

Barr, a former CIA analyst, is part of a growing contingent in the United States, Europe and Australia alarmed by the existence of Echelon, a computer system that monitors millions of e-mail, fax, telex and phone messages sent over satellite-based communications systems as well as terrestrial-based data communications. The system was established under what is known as the "UKUSA Agreement" after World War II and includes the security agencies of the United States, Britain, Canada, Australia and New Zealand.

Although Echelon was originally set up as an international spy network, lawmakers are concerned that it could be used to eavesdrop on American citizens.

"I am concerned there are not sufficient legal mechanisms in place to protect our private information from unauthorized government eavesdropping through such mechanisms as Project Echelon," Barr said in an interview on Tuesday.

The finished report will outline the legal bases and other criteria used by United States intelligence agencies when assessing potential wiretap targets. It will be submitted to the House and made available
to the public.

"If the agencies feel unable to provide a full account to the public, then a second classified report will be provided to the House Committee on Intelligence," Barr said. "This is to stop the agencies hiding behind a cloak of secrecy."

Judith Emmel, chief of public affairs for the NSA, declined to comment about the UKUSA Agreement but said the agency was committed to responding to all information requests covered by Barr's amendment. "The NSA's Office of General Counsel works hard to ensure that all Agency activities are conducted in accordance with the highest constitutional, legal and ethical standards," she said.

Until last Sunday, no government or intelligence agency from the member states had openly admitted to the existence of the UKUSA Agreement or Echelon. However, on a television program broadcast on Sunday in Australia, the director of Australia's Defence Signals Directorate acknowledged the existence of the agreement. The official, Martin Brady, declined to be interviewed for the "Sunday Program," but provided a statement for its special on Echelon. "DSD does cooperate with counterpart signals intelligence organizations overseas under the UKUSA relationship," the statement said.

Meanwhile, European Parliament officials have also expressed concern about the use of Echelon to gather economic intelligence for participating nations. Last October, the spying system came to the attention of the Parliament during a debate on Europe's intelligence relationship with the United States. At that time, the Parliament decided it needed more information about Echelon and asked its Science and Technology Options Assessment Panel to commission a report.

The report, entitled "Development of Surveillance Technology and Risk of Abuse of Economic Information", was published on May 10 and provides a detailed account of Echelon and other intelligence monitoring systems.

According to the report, Echelon is just one of the many code names for the monitoring system, which consists of satellite interception stations in participating countries. The stations collectively monitor millions of voice and data messages each day. These messages are then scanned and checked against certain key criteria held in a computer system called the "Dictionary." In the case of voice communications, the criteria could include a suspected criminal's telephone number; with respect to data communications, the messages might be scanned for certain keywords, like "bomb" or "drugs." The report also alleges that Echelon is capable of monitoring terrestrial Internet traffic through interception nodes placed on deep-sea communications cables.

While few dispute the necessity of a system like Echelon to apprehend
foreign spies, drug traffickers and terrorists, many are concerned that the system could be abused to collect economic and political information.

"The recent revelations about China's spying activities in the U.S. demonstrates that there is a clear need for electronic monitoring capabilities," said Patrick Poole, a lecturer in government and economics at Bannock Burn College in Franklin, Tenn., who compiled a report on Echelon for the Free Congress Foundation. "But those capabilities can be abused for political or economic purposes so we need to ensure that there is some sort of legislative control over these systems."

On the "Sunday Program" special on Echelon, Mike Frost, a former employee of Canada's Communications Security Establishment, said that Britain's intelligence agency requested that the CSE monitor the communications of British government officials in the late 1980s. Under British law, the intelligence agency is prohibited from monitoring its own government. Frost also said that since the cold war is over, the "the focus now is towards economic intelligence."

Still, Echelon has been shrouded in such secrecy that its very existence has been difficult to prove. Barr's amendment aims to change that.

"If this report reveals that information about American citizens is being collected without legal authorization, the intelligence community will have some serious explaining to do," Barr said.

---

**Related Sites**

These sites are not part of The New York Times on the Web, and The Times has no control over their content or availability.

- [National Security Agency](http://www.nsa.gov)
- [Central Intelligence Agency](http://www.cia.gov)
- [Representative Bob Barr](http://www.house.gov/barr)
- [Sunday Program](http://www.cbs.com/sunday/)
- [DSD memo, page 1](http://www.nsa.gov)
- [European Parliament](http://www.europarl.eu.int)
- [European Union Report](http://europa.eu.int)
- [Science and Technology Options Assessment Panel](http://www.s犒�e.gov)
- [Patrick Poole's report](http://www.freecongress.org/echelon)

---

<http://www.nytimes.com/library/tech/99/05/cyber/articles/27network...>