Order broadens surveillance of Internet users

Mike Ingram
26 October 2005

In a serious attack on democratic rights, the US government has greatly increased the scope of legislation introduced in 1994, regarding the electronic monitoring of telecommunications providers.

The legislation, known as the Communications Assistance for Law Enforcement Act (CALEA) obliges telephone companies to make it possible for law enforcement agencies to intercept any phone conversations carried out over its networks, as well as making call records available. The act also stipulates that it must not be possible for a person to detect that his or her conversation is being monitored by the respective government agency.

An order issued by the Federal Communications Commission in August and first published in the Federal Register of October 13 extends the requirement of the 1994 legislation to cover broadband Internet access services, including wireless and voice-over-IP (VoIP) Internet telephony services.

The far-ranging implications of this are highlighted in an appeal being prepared by lawyers for the American Council on Education. The largest association of universities and colleges is preparing to appeal the order before the United States Court of Appeals for the District of Columbia Circuit. According to the *New York Times*, the universities do not question the government's right to implement wiretaps but are appealing on the grounds of cost—in excess of $7 billion, according to estimates by some professionals. But the cost is itself indicative of the extent of the threat to privacy and democratic rights contained in the order.

Universities provide Internet access from hundreds of buildings across campuses and entire cities, including lounges, dorms, classrooms, laboratories, libraries and other areas that offer either wired or wireless Internet access.

Universities already comply with requests by law enforcement officials who produce court orders requiring wiretaps. At present, this requires them to work with campus officials to single out specific sites and install the equipment needed to carry out surveillance. The new legislation requires universities to have every Internet access point send all communications to a network operations center, where the data packets could be put together into a single package for delivery to a law enforcement agency.

If this is done, then the government will no longer require the collaboration of campus officials to monitor the activities of students or staff. The technology will be in place for automatic surveillance from a remote location without the knowledge of either the individuals being monitored or the institution itself.

Beyond the university campus, the order extends the 1994 wiretap provisions to Internet service providers, libraries, airports providing wireless services and municipalities that either provide Internet access to residents or plan to build their own Internet access networks, such as Philadelphia or San Francisco.

As well as extending CALEA to broadband Internet access providers, the order states, "We conclude that CALEA applies to providers of 'interconnected VoIP services,' which include those VoIP services that: (1) enable real-time, two-way voice communications; (2) require a broadband connection from the user's location; (3) require IP-compatible customer premises question; and (4) permit users to receive calls from and terminate calls to the PSTN [public switched telephone network]."

This poses huge compliance problems for companies providing so-called peer-to-peer (P2P) services, where communications are not routed through a central server. Though the legislation requires compliance only from systems that allow connection to the PSTN, it nevertheless requires that on such systems, all calls be wiretappable, not just those interacting with the phone

system.

This would potentially require P2P telephone service companies such as Skype to re-engineer its system to make customers wiretappable because it offers the SkypeIn and SkypeOut paid services that permit customers to receive calls from and make them to the traditional phone system. Skype is the best known of such services, which was recently purchased by eBay for $2.6 billion. The service registers well over 3 million users online at any one time.

The expansion of CALEA to cover VoIP services is the latest in a long line of attacks on democratic rights and civil liberties carried out on the basis of the supposed “war on terror.”

When CALEA was set up in 1994, it explicitly differentiated between telecommunications and Internet services. CALEA originally carried a complete exemption for all “information services.” This was in part a response to broad-based criticisms on civil liberties grounds and concerns that to place such requirements on an emerging technology would stifle innovation and leave American capitalism unable to compete against its rivals.

As the Internet emerged as a mass medium, however, there were increasing attempts by police and intelligence agencies services to undermine such a separation. The terrorist attacks of 2001 provided the political climate in which this could finally be achieved. It was demanded that all such concerns be put aside in the interests of the “war on terror.”

On September 13, 2001, just two days after the attacks on New York and Washington, the Senate approved the Combating Terrorism Act, which among other things extended the powers of the FBI and other police agencies to spy on the Internet using new technology to monitor e-mail messages as they pass through Internet service providers.

Previous laws on telephone wiretapping made it relatively easy for the police to obtain the records of incoming and outgoing phone calls, a procedure called “trap and trace,” resulting in a list of all numbers called from or calling to a target location. A much higher standard of evidence must be met to get an actual wiretap that records the substance of telephone conversations.

In the past, the monitoring of Internet traffic was limited to this more restrictive standard, but with the Combating Terrorism Act, Internet monitoring was treated the same as a trap-and-trace, although the information obtained goes far beyond a simple list of phone numbers.

The expansion of CALEA to require that any institution providing broadband Internet services must implement the technical means to facilitate such spying on an automatic basis is an ominous warning of things to come. The FCC’s own press release describes the ruling as “the first step to apply CALEA obligations to new technologies and services that are increasingly used as a substitute for conventional services.”