

The Internet and Law Enforcement Surveillance:

Law Enforcement Concerns Can Be Addressed Without Regulation, Which Would Stifle Innovation, Raise Costs, Risk Security

March 19, 2004



There is nothing untappable about packet or Internet technology. Packet services currently available for voice and data are tappable at one or more points in the networks, and service providers are quite willing to work with law enforcement to satisfy interception orders quickly and fully. But the Internet is different from the traditional telephone network, and government agencies should not expect that surveillance will be carried out on the Internet the same way it is carried out in the circuit-switched telephone network. The digital revolution has produced many means of communication and it is not reasonable to require that all of them identify communications and route traffic the same way that the telephone network does.

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
<http://www.cdt.org>

Yet the Justice Department and the FBI are trying to force the diversity of services available over the Internet into a single format resembling the telephone network. On March 10, 2004, DOJ and FBI filed a Joint Petition for Expedited Rulemaking with the Federal Communications Commission asking the FCC (a) to declare that providers of broadband access and "Voice over IP" (or Voice on the Net) services are covered by the Communications Assistance for Law Enforcement Act ("CALEA"), and (b) to create a regulatory process under which new communications protocols, applications, or services must be reviewed and approved by the FBI before they can be deployed.

CALEA was adopted in 1994 in response to law enforcement concerns that wiretaps would be more difficult in digital telephone networks than they had been with the analog phone system. CALEA required "telecommunications carriers" to design basic wiretap capabilities into their networks. As it was implemented, the CALEA statute gave the FBI very precise design control over telephone switching software. The FBI was able to convince the FCC to mandate very specific features, including – at substantial cost to carriers – features that gave the government capabilities going beyond those that had been available in older phone systems. Thus CALEA was used to enhance rather than merely preserve government surveillance capabilities.

The CALEA statute applies only to telecommunications common carriers. It does not apply to "information services." Congress realized that the Internet was fundamentally different from the telephone system and Congress chose not to apply CALEA to the Internet and "information services" carried over it. VoIP, email, Instant Messaging and other forms of Internet communications are information services and thus are not covered by CALEA. Although ISPs and Internet application providers must (and do) comply with interception orders under the wiretap laws, they have not had to design their networks and services to meet FBI specifications.

The Joint Petition seeks to alter the balance initially struck in CALEA, and asks the FCC to extend CALEA to cover broadband Internet access generally and VoIP services specifically. Moreover, the Joint Petition asks the FCC to create a system under which any new technology that might replace a range of existing communications technologies must be reviewed and approved by the FBI before deployment.

Such a prior-review requirement would destroy the United States' ability to innovate on the Internet, and would in effect overturn the critical decisions of the FCC over the years that facilitated the rise of the Internet as a mass communications medium. The changes that the FBI seeks are not necessary to allow law enforcement to carry out court-ordered interceptions. The Internet and technology industries are working hard to meet the needs of law enforcement, and the imposition of the sweeping regulatory regime advocated by the Joint Petition is not necessary to provide law enforcement with the ability to carry out its investigations. Surveillance features built in to satisfy government demands could undermine the openness and security of the Internet.

For more information, contact Jim Dempsey (jdempsey@cdt.org), Lara Flint (lflint@cdt.org) or John Morris (jmorris@cdt.org) at (202) 637-9800.