

FBI plans new Net-tapping push

FBI has drafted legislation that would require Internet service providers to create wiretapping hubs for police surveillance

By [Global Research](#)

Global Research, July 13, 2006

[CNET News.com](#) 13 July 2006

Region: [USA](#)

Theme: [Police State & Civil Rights](#)

By [Declan McCullagh](#)

Staff Writer, CNET News.com

The FBI has drafted sweeping legislation that would require Internet service providers to create wiretapping hubs for police surveillance and force makers of networking gear to build in backdoors for eavesdropping, CNET News.com has learned.

FBI Agent Barry Smith distributed the proposal at a private meeting last Friday with industry representatives and indicated it would be introduced by Sen. Mike DeWine, an Ohio Republican, according to two sources familiar with the meeting.

The draft bill would place the FBI's Net-surveillance push on solid legal footing. At the moment, it's ensnared in a [legal challenge](#) from universities and some technology companies that claim the Federal Communications Commission's broadband surveillance directives exceed what Congress has authorized.

The FBI claims that expanding the 1994 [Communications Assistance for Law Enforcement Act](#) is necessary to thwart criminals and terrorists who have turned to technologies like voice over Internet Protocol, or VoIP.

"The complexity and variety of [communications technologies](#) have dramatically increased in recent years, and the lawful intercept capabilities of the federal, state and local law enforcement community have been under continual stress, and in many cases have decreased or become impossible," according to a summary accompanying the draft bill.

Complicating the political outlook for the legislation is an [ongoing debate](#) over allegedly illegal surveillance by the National Security Administration—punctuated by [several lawsuits](#) challenging it on constitutional grounds and an [unrelated proposal](#) to force Internet service providers to record what Americans are doing online. One source, who asked not to be identified because of the sensitive nature of last Friday's meeting, said the FBI viewed its CALEA expansion as a top congressional priority for 2007.

Breaking the legislation down

The 27-page proposed CALEA amendments seen by CNET News.com would:

- Require any manufacturer of "routing" and "addressing" hardware to offer upgrades or other "modifications" that are needed to support Internet wiretapping. Current law does require that of telephone switch manufacturers—but not makers of routers and [network](#)

[address translation](#) hardware like Cisco Systems and 2Wire.

- Authorize the expansion of wiretapping requirements to “commercial” Internet services including instant messaging if the FCC deems it to be in the “public interest.” That would likely sweep in services such as in-game chats offered by Microsoft’s Xbox 360 gaming system as well.
- Force Internet service providers to sift through their customers’ communications to identify, for instance, only VoIP calls. (The language requires companies to adhere to “processing or filtering methods or procedures applied by a law enforcement agency.”) That means police could simply ask broadband providers like AT&T, Comcast or Verizon for wiretap info—instead of having to figure out what VoIP service was being used.
- Eliminate the current legal requirement saying the Justice Department must publish a public “notice of the actual number of communications interceptions” every year. That notice currently also must disclose the “maximum capacity” required to accommodate all of the legally authorized taps that government agencies will “conduct and use simultaneously.”

[Jim Harper](#), a policy analyst at the free-market Cato Institute and member of a Homeland Security advisory board, said the proposal would “have a negative impact on Internet users’ privacy.”

“People expect their information to be private unless the government meets certain legal standards,” Harper said. “Right now the Department of Justice is pushing the wrong way on all this.”

Neither the FBI nor DeWine’s office responded to a request for comment Friday afternoon.

DeWine has relatively low approval ratings—[47 percent](#), according to SurveyUSA.com—and is enmeshed in a fierce battle with a Democratic challenger to retain his Senate seat in the November elections. DeWine is a member of a Senate Judiciary [subcommittee](#) charged with overseeing electronic privacy and antiterrorism enforcement and is a former prosecutor in Ohio.

A panel of the U.S. Court of Appeals in Washington, D.C., [decided 2-1 last month](#) to uphold the FCC’s extension of CALEA to broadband providers, and it’s not clear what will happen next with the lawsuit. Judge Harry Edwards wrote in his dissent that the majority’s logic gave the FCC “unlimited authority to regulate every telecommunications service that might conceivably be used to assist law enforcement.”

The organizations behind the lawsuit say Congress never intended CALEA to force broadband providers—and networks at corporations and universities—to build in central surveillance hubs for the police. The list of organizations includes Sun Microsystems, Pulver.com, the American Association of Community Colleges, the Association of American Universities and the American Library Association.

If the FBI’s legislation becomes law, it would derail the lawsuit because there would no longer be any question that Congress intended CALEA to apply to the Internet.

[Copyright](#) ©1995-2006 CNET Networks, Inc. All rights reserved.

The original source of this article is CNET News.com
Copyright © Global Research, CNET News.com, 2006

[Comment on Global Research Articles on our Facebook page](#)

[Become a Member of Global Research](#)

Articles by: [Global Research](#)

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca