
FBI Seeks New Mandates on Communications Technologies

February 24, 2011

Tags: Array

Policy Posts are in-depth analyses on current tech policy issues from CDT experts. Sign up to receive the latest Policy Posts here:

- (1) [FBI Seeks New Mandates On Communications Technologies](#)
- (2) [Background On Communications Assistance for Law Enforcement Act \(CALEA\)](#)
- (3) [Extending CALEA Could Undermine Cybersecurity and Threaten Innovation](#)
- (4) [Any New CALEA Mandates Should Be Matched with Stronger Privacy Protections](#)
- (5) [Congress Steps In](#)

1) FBI Seeks New Mandates on Communications Technologies

The Federal Bureau of Investigation is seeking new technology mandates that would make it easier for law enforcement and national security officials to conduct surveillance of new communications services. While nothing has yet been proposed, the New York Times has reported that the FBI wants to amend the Communications Assistance for Law Enforcement Act (CALEA) to require that a range of companies re-design their services.

When CALEA was adopted in 1994, it covered a handful of telecommunications companies using switching equipment made by a handful of manufacturers. The technologies and services the FBI now apparently wants to bring under CALEA are much more diverse. Some were developed in garages and others in college dorm rooms. They take advantage of the unique, decentralized design of the Internet. It would be very disruptive if they had to follow the centralized model of the traditional telephone system.

The FBI, calling its program "Going Dark," argues that it could lose the ability to conduct surveillance. There is no doubt that communications technologies have changed dramatically recent years, that some communications are more difficult to intercept than are others, and that the FBI has a legitimate concern that criminals and terrorists will gravitate to communications technologies that are difficult to surveil. However, taken as a whole, the digital revolution has made more information available to the FBI than ever before and government surveillance goes up almost every year. In 2009, the most recent year for which statistics are available, federal and state law enforcement placed a record 2,376 wiretaps. On average, 3,763 communications were intercepted in each of these wiretaps. Far from "Going Dark" as a result of advances in technology, the FBI and other law enforcement agencies are experiencing a boon in electronic surveillance.

In response to the FBI's concerns, the Obama Administration has commenced an inter-agency review to determine what, if any, legislation should be proposed. The results of that review could be provided to Congress soon.

[U.S. Tries to Make It Easier to Wiretap the Internet, The New York Times, September 27, 2010](#) [1]

[Gregory Nojeim, New Wiretapping Mandates Could Harm Privacy, Innovation and Security, The Hill, October 1, 2010](#) [2]

2) Background on Communications Assistance for Law Enforcement Act (CALEA)

Congress enacted CALEA in 1994 in response to law enforcement concerns that wiretaps would be more difficult in digital telephone networks than they had been in the analog phone system. Discrete technical problems had arisen, including the inability to acquire forwarded calls and a lack of capacity in cellular systems to accommodate multiple taps. The earliest FBI proposal to deal with

these concerns, floated in the early 1990s, would have given the Attorney General broad authority to dictate design standards. Congress rejected this heavy-handed approach as “not practical... [nor] justified to meet any law enforcement need,” as indicated in the House report on CALEA. Instead, Congress insisted that the FBI detail its technological challenges so Congress could tailor a solution to fit the problem.

As enacted, CALEA required telecommunications carriers to reconfigure their switching equipment to provide four basic capabilities. Carriers had to be able to isolate expeditiously the content of targeted communications, isolate expeditiously the call identifying information, provide this content and other information to law enforcement in useful form, and do it unobtrusively to protect the secrecy of the wiretap and the privacy of others’ communications.

CALEA was supposed to “preserve the government’s ability... to intercept communications” (emphasis supplied) according to the House report on the legislation. However, the FBI convinced the FCC to mandate specific and costly features that gave the government capabilities beyond those that had been available in older phone systems. Thus, contrary to Congress’ intent, CALEA was used to enhance rather than merely preserve government surveillance capabilities.

In 2004, the FBI filed a petition with the FCC asking that the agency extend CALEA to a wide range of Internet services. Ultimately, the FCC found that broadband Internet access and interconnected VoIP (Voice Over Internet Protocol) services were “substantial replacement[s]” for local telephone service, and, on that basis, the FCC extended CALEA to these services. Again, a statute intended to preserve capabilities was used to expand them, covering technology that did not even exist in 1994.

[The FBI's Public CALEA Page, Featuring Statutory Text and Legislative History](#) [3]

[CDT's Background Page on CALEA](#) [4]

[CDT's Policy Post on the Extension of CALEA Mandates to the Internet, June 13, 2006](#) [5]

3) Extending CALEA Could Undermine Cybersecurity and Threaten Innovation

Ironically, as Congress debates how to strengthen cybersecurity, the changes to CALEA that the FBI reportedly seeks might actually weaken security and put more communications at risk of exploitation by hackers, identity thieves, foreign governments, and malicious insiders. Re-architecting a communications service to create a new point of access at which the FBI could conduct surveillance also creates a vulnerability that others can exploit.

The FBI’s proposal is aimed at the application layer of the Internet, where the most dynamic innovation is occurring. It could seriously stifle innovation if the government has to pre-clear new services, or if they have to be built to a government standard. The next great communications application might never come to market. Some current applications, particularly those that allow encrypted computer-to-computer communications (P2P communications), could be precluded altogether.

The FBI proposal also poses global issues. The world is watching what the United States does in terms of facilitating lawful surveillance. Countries with poor human rights records will point to new U.S. technology mandates to justify controlling what their populations see and hear on the Internet. Already, the United Arab Emirates has (wrongly) cited CALEA as precedent for the technology mandates it has sought to impose on companies doing business in the UAE. Others, seeing new technology mandates adopted in the U.S., may impose similar or more stringent requirements. Secretary of State Clinton, who spoke so eloquently about Internet freedom in the wake of the protests that led Egyptian president Hosni Mubarak to step down, would be poorly positioned to object if the U.S. had imposed such mandates in the U.S.

Through the Digital Privacy and Security Working Group (DPSWG), CDT has convened a broad range of interested parties to bring these concerns to the attention of government officials and members of

Congress. Industry associations and NGOs issued joint statement proposing principles against which any legislation to extend CALEA should be measured. They emphasize that before any extension of CALEA is considered, the FBI should first specify the surveillance problems that it believes need to be addressed and work to resolve them without new technology mandates.

[NGO and Industry Association Statement of Concern about Expansion of CALEA, February 15, 2011](#) [6]

4) Any New CALEA Mandates Should Be Matched with Stronger Privacy Protections

In support of its effort to expand CALEA, the FBI says that it is not seeking new surveillance authorities, just changes in the law to facilitate compliance with surveillance orders issued under current authority. The problem is that the privacy standards currently governing exercise of existing surveillance authorities are woefully out of date, allowing the government to access sensitive information without a warrant. The key statute, ECPA, was drafted in 1986, before the World Wide Web and social networking existed, before email and cellular telephones were widely used, and before the mass movement from desktop computing to cloud computing got underway.

ECPA's privacy rules reflect the technology of 1986. For example, when ECPA was drafted, electronic storage was expensive and providers discarded email shortly after the user downloaded it to his or her computer, or after a few months if it was not downloaded. As a result, ECPA treats emails stored with a provider for more than 180 days as if they were abandoned and makes them available to the government with a mere subpoena. As another example, ECPA specifies no standard for law enforcement access to location information generated by cellular telephones and other mobile devices.

A broad coalition of telecommunications and technology firms, privacy groups spanning the political spectrum, former DOJ officials, and academics have come together under the banner of Digital Due Process to propose changes to ECPA to address these problems.

As a practical matter, both legal standards and technological difficulty limit surveillance and protect privacy. When technology mandates lessen the technological impediments to surveillance, stronger legal standards must compensate. Before it considers new CALEA mandates, Congress should update ECPA to bring legal standards governing surveillance into the 21st century.

[ECPA reform proposals made by the Digital Due Process coalition](#) [7]

[FBI strategy document showing that "Going Dark" initiative seeks changes to surveillance statutes, including the Wiretap Act and ECPA, May 27, 2009 \(pp. 38-40\)](#) [8]

5) Congress Steps In

On February 17, 2011, at a hearing before the House Judiciary Committee Subcommittee on Crime, Terrorism and National Security, FBI General Counsel Valerie Caproni indicated that the Administration hoped to give Congress a proposal in the near future. An interagency process involving the FBI/DOJ, the Department of Commerce, the White House, and intelligence agencies is underway to determine the parameters of that proposal. It will be up to Congress to balance privacy, innovation, cybersecurity, and surveillance needs as it contemplates new legislation.

Ms. Caproni's testimony suggested some limits on the changes the FBI might seek. First, she indicated that FBI's "Going Dark" problem pertained only to communications sought in real time, not to stored communications. Second, she indicated that "fundamental changes in encryption technology" will not be sought. Third, she recognized that some impediments to the government's ability to conduct surveillance will have to be addressed with individually tailored solutions, not with broadly applicable mandates. Still, her testimony suggested that the FBI, at least, seeks new powers of undefined scope, potentially reaching a wide range of services.

Interestingly, Ms. Caproni's testimony highlighted what could be an alternative approach: she called for Congress to support establishment of a Domestic Communications Assistance Center (DCAC) that would leverage research and development efforts of Federal, State and local law enforcement agencies with respect to electronic surveillance capabilities. The Justice Department's FY 2012 budget request seeks \$15 million for the DCAC. While the FBI may seek design mandates on top of the research capability, the DCAC seems a cost-effective alternative to extension of CALEA mandates. The DCAC is not be a silver bullet that solves all surveillance challenges, but it would help address the needs of state and local law enforcement without the negatives associated with new technology mandates. Funding for the DCAC was endorsed by each of the other witnesses, Dr. Susan Landau, a former Distinguished Engineer at Sun Microsystems, and Chief Michael Marshall, the President of the International Association of Chiefs of Police.

Prompted by Dr. Landau's testimony, Subcommittee members focused much of their attention on whether solutions to the FBI's surveillance challenges would negatively impact cybersecurity. These concerns may come into sharp focus when a legislative proposal is made.

The Senate has not yet conducted similar hearings, but Judiciary Committee Chairman Patrick Leahy (D-VT) indicated in a January 11, 2011 speech that the Committee's work may include re-visiting CALEA in this Congress.

["Going Dark" Hearing, Witness Statements and Video Webcast, February 17, 2011](#) [9]

[DOJ FY 2012 Budget Request Seeking \\$15 Million for New Communications Center, February, 2011](#) [10]

-
- [tech mandates](#)
- [fbi](#)
- [calea](#)

Copyright © 2013 by Center for Democracy & Technology. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. [Details](#).

Source URL: <https://www.cdt.org/policy/fbi-seeks-new-mandates-communications-technologies>

Links:

[1] <http://www.nytimes.com/2010/09/27/us/27wiretap.html>

[2] <http://thehill.com/blogs/congress-blog/homeland-security/122073-new-wiretapping-mandates-could-harm-privacy-innovation-and-security>

[3] <http://www.askcalea.net/calea/>

[4] <http://www.cdt.org/report/calea-background>

[5] <http://www.cdt.org/policy/court-upholds-imposition-technical-design-mandates-internet>

[6] http://www.cdt.org/pr_statement/statement-concern-about-expansion-calea

[7] <http://www.digitaldueprocess.org>

[8] http://www.eff.org/files/20110207_FBI_Going_Dark_Release_Part_1.pdf

[9] http://judiciary.house.gov/hearings/hear_02172011.html

[10] <http://www.justice.gov/jmd/2012factsheets/docs/fy12-national-security.pdf>