FCC Considers New Technology Mandates, Threatening Innovation and Privacy

September 19, 2007
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:

The Federal Communications Commission (FCC) is actively considering whether to adopt technology mandates that have the potential to significantly harm innovation and privacy on the Internet. Two ongoing proceedings -- one involving a small part of the ongoing Communications Assistance for Law Enforcement Act (CALEA) saga and one concerning E911 -- illustrate the danger.

(1) FCC Considers New Technology Mandates, Threatening Innovation and Privacy [1]

(2) FBI Continues to Extend CALEA Beyond Its Intended Scope [2]

(3) Location Awareness Mandates Raise Concerns [3]

(1) FCC Considers New Technology Mandates, Threatening Innovation and Privacy

The Federal Communications Commission (FCC) is actively considering whether to adopt technology mandates that have the potential to significantly harm innovation and privacy on the Internet. Two ongoing proceedings -- one involving a small part of the ongoing Communications Assistance for Law Enforcement Act (CALEA) saga and one concerning E911 -- illustrate the danger.

The Internet was not the primary target of either proceeding, but Internet and IP-based services would likely be squarely impacted by adverse FCC rules. In the CALEA proceeding, the FBI targeted a specific standard for wiretaps in the wireless telephone context, but the FBI made clear that it thought that whatever rules applied to wireless should apply also to wiretaps of broadband Internet access.

Congress enacted CALEA in 1994 to ensure that law enforcement would retain the capacity to conduct legal wiretapping on the public telephone network. Although the law explicitly excluded the Internet from its scope, regulators have been engaged in a long-running effort to extend the design mandates permitted under CALEA to Internet technology -- something that would have strong negative ramifications for innovators.

In the E911 proceeding, the main focus is also on wireless service, but the FCC also proposed to extend the same basic rules to voice-over Internet Protocol (VoIP) services.

Thus, in both proceedings, the FCC is considering seemingly narrow "technology mandates" that in fact could have very broad and harmful impacts. In isolation, each mandate may appear to be small, but taken together, these rules that could have a devastating impact on the ability of American technologists to innovate, and both could seriously harm privacy rights as well. It will be critical for Internet-focused companies and groups to pay close attention to both proceedings.

(2) FBI Continues to Extend CALEA Beyond Its Intended Scope

On July 25, CDT filed joint comments to the FCC on behalf of eight public interest and industry groups in the CALEA "deficiency proceeding" nominally aimed at challenging the CDMA2000 standard for compliance by wireless companies with their CALEA obligations. CALEA was originally

intended only to apply to the telephone network, and it specifically excluded application to the Internet. Last year the FCC overrode that exclusion and extended CALEA to certain Internet services.

The CDMA2000 standard applies to many of the leading U.S. wireless, some of which provide "Internet Protocol" based services including some access to the Internet. The FBI argued that the standard is deficient because it did not require the carrier to effectively listen in on their customers' communications to report certain information to law enforcement. Yet as CDT argued in its comments to the FCC, the FBI was seeking to impose on the carriers obligations far beyond what CALEA imposes on traditional telephone companies. The FBI also sought to impose an obligation of carriers to be able to report their customers' physical location at all times, also an obligation far beyond what is imposed in the traditional telephone network.

None of the points raised by the FBI concerns the type of basic surveillance capability that CALEA was intended to preserve in the traditional telephone network. Nevertheless, these are the kinds of features that the FBI is seeking to require be built into a wide range of devices, including basic laptop and other computers. The FCC, which under the original CALEA framework was supposed to play a balanced role between law enforcement and industry, has instead turned out to be the FBI's handmaiden in its attempted to redesign communications networks to serve its interests.

Overview of CALEA Developments by Professor Susan Crawford [4]

CDT Filing [5]

(3) Location Awareness Mandates Raise Concerns

On August 22, CDT filed joint comments to the FCC on behalf of itself, the Electronic Frontier Foundation and Sun Microsystems in the FCC's proceeding about extending e911 "auto-location" mandates to VoIP services.

For almost a decade, the FCC has been seeking to ensure that the 911 emergency system continues to function with a range of new technologies. The most critical initial issue concerned cell phones, which initially could not even make a call to 911 numbers. The FCC mandated that cell phones be able to call 911 and provide the geographic location of the caller.

In the current e911 proceeding at the FCC, the FCC is considering what level of location accuracy it should impose on wireless carriers. But the Commission is also asking whether it should also impose on VoIP services the same rules that it imposes on wireless carriers. In its comments to the Commission, CDT argued that the technology that underlies VoIP is radically different than the cellular telephone network, and that imposing wireless rules onto Internet services would effectively prohibit the marketing of some Internet services, because the services would not be able to meet the same standards for "automatic" location determination that the Commission was considering for wireless.

CDT urged that the FCC not constrain the development of VoIP and other emerging communications technologies. Instead, it is critical that the public learn that the 911 capabilities of different technologies will be different, and that to call 911 using some VoIP services may require the user to provide the location information.

CDT Filing [6]

-
- location

Copyright © 2013 by Center for Democracy & Technology.
The content throughout this website that originates with 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/fcc-considers-new-technology-mandates-threatening-innovation-and-privacy

Links:
[1] https://www.cdt.org/1
[2] https://www.cdt.org/2
[3] https://www.cdt.org/3
[4] http://scrawford.blogware.com/blog/_archives/2007/8/16/3162684.html
[5] http://www.cdt.org/digi_tele/20070725caleacomments.pdf
[6] http://www.cdt.org/privacy/20070822e911-comments.pdf