Statement of Concern about Expansion of CALEA

February 15, 2011

Recently, FBI officials have indicated that the Obama Administration may seek legislation to expand the scope of the Communications Assistance for Law Enforcement Act (CALEA) to a broad array of Internet communications technologies. Currently, this 1994 law requires telecommunications carriers to design wiretapping capabilities into their networks, and the FCC extended these requirements to providers of broadband Internet access and interconnected VoIP services in 2005. Clearly, lawful electronic surveillance plays an important role in enabling government agencies to fulfill their obligations to stop crime and to protect national security. These goals, however, must be reconciled with other important societal values, including cybersecurity, privacy, free speech, innovation and commerce.

These threshold questions should be answered before consideration of any proposal to expand CALEA:

(1) **What specific problems must be addressed?** As it was required to do when it proposed the original CALEA, the FBI must first identify the particular services or technologies most in need of additional surveillance capability and the frequency with which they thwart authorized government surveillance.

(2) **Have alternatives to a CALEA-like mandate been pursued sufficiently?** After the specifics have been identified, alternative approaches to surveillance needs that do not involve technology mandates should be considered. Industry may voluntarily adopt practices that obviate some problems; others may be addressed by providing extra resources for the FBI to acquire additional expertise and for assisting state and local law enforcement.

(3) **What is the narrowest, effective approach?** Only after addressing the first two elements could changes that are narrowly targeted be considered. Generalized or overbroad mandates would be difficult to implement, likely to foster avoidable litigation, and certain to have unintended results.

After these threshold questions are answered, policy makers should measure any proposal to extend the scope of CALEA mandates against all of the following principles:

Preserve trust: Consumer and business trust in the confidentiality of Internet communications is essential to online commerce, privacy and free speech. Changes to products and services that could undermine users' trust in the privacy and security of their communications should be avoided.

Safeguard cybersecurity: Requiring redesign of Internet communications technologies to facilitate surveillance would make them less secure and produce vulnerabilities exploitable by others, including foreign entities, perpetrators of economic espionage, malicious insiders, hackers and identity thieves, thus undermining cybersecurity goals.

Protect innovation and competitiveness: Extending CALEA mandates to Internet communications applications could stifle innovation, delay or prevent cutting-edge communication technologies from coming to market, and give foreign competitors an advantage over U.S. companies. Any requirement of governmental approval of such technology or applications before release must be rejected for the same reasons.

Anticipate resultant international demands: New U.S. surveillance requirements could spur other countries to impose new mandates that are equally burdensome or worse, thereby undermining efforts to resist such demands by other countries.

Don't compromise encryption: Strong encryption is a foundation for data security, Internet commerce and personal communication. There should be no new requirements or restrictions that would introduce vulnerabilities or weaken the protection afforded by encryption and related security technologies.

Avoid unfunded mandates: The costs of implementing any new proposals should be borne by the government.

Protect privacy and promote accountability: Stronger technical capabilities resulting from extension or expansion of CALEA should be matched with stronger privacy protections such as enhanced judicial oversight, transparency, and audits to promote government accountability.

American Library Association
Association of Research Libraries
Americans for Tax Reform's DigitalLiberty.Net
Business Software Alliance
Center for Democracy & Technology
Center for Financial Privacy and Human Rights
Competitive Enterprise Institute
Computer and Communications Industry Association
EDUCAUSE
NetCoalition
Software and Information Industry Association
TechAmerica
TechFreedom
U.S. Public Policy Council for the Association of Computing Machinery