Written Statement of the
American Civil Liberties Union

Laura W. Murphy
Director, Washington Legislative Office

Christopher Calabrese
Legislative Counsel

Before U.S. House Committee on the Judiciary
Subcommittee on Crime, Terrorism and Homeland Security

February 17, 2011

Going Dark: Lawful Electronic Surveillance in the Face of New Technologies

Chairman Sensenbrenner, ranking member Scott and members of the Committee, On behalf of the American Civil Liberties Union ("ACLU"), America's oldest and largest civil liberties organization, and its more than half a million members, countless additional supporters and activists, and 53 affiliates nationwide, we write to oppose any expansion of the Communication Assistance to Law Enforcement Act (CALEA). The original CALEA law, passed in 1994, was aimed at making surveillance of telephones simpler by building wiretap capacity into every telephone switch network.

While no formal legislative proposal exists, some reports have suggested law expanding this law to the internet and internet communications providers. Such an expansion would raise serious concerns for privacy, innovation and human rights around the globe. Further, evidence in the public record does little to support the need for any expansion.

Background

Details regarding a proposed expansion to CALEA have largely come from two articles in the *New York Times*.[1] The first, dated September 27, 2010, states:

> Federal law enforcement and national security officials are preparing to seek sweeping new regulations for the Internet, arguing that their ability to wiretap criminal and terrorism suspects is "going dark" as people increasingly communicate online instead of by telephone.
>
> Essentially, officials want Congress to require all services that enable communications — including encrypted e-mail transmitters like BlackBerry, social networking Web sites like Facebook and software that allows direct "peer to peer" messaging like Skype — to be technically capable of complying if served with a wiretap order. The mandate would include being able to intercept and unscramble encrypted messages.[2]

The article describes the proposal in more detail as consisting of three related requirements:

- Communications services that encrypt messages must have a way to unscramble them.
- Foreign-based providers that do business inside the United States must install a domestic office capable of performing intercepts.
- Developers of software that enables peer-to-peer communication must redesign their service to allow interception.[3]

Put another way, this proposal is aimed at requiring companies to re-engineer their communications software so that it has a surveillance backdoor that can be effortlessly accessed by law enforcement. Also, one of the core security protections of the internet – encryption – must be weakened by building in an eavesdropping capacity for a third party who is not privy to the communication.

---

[1] Charlie Savage, *U.S. Tries to Make It Easier to Wiretap the Internet*, NEW YORK TIMES, September 27, 2010.
[2] *Id.*
[3] *Id.*

The scope of such a proposal is striking. A significant percentage of all software designed for the internet is aimed at communicating in some way. Email, instant message, Skype, posts on social networking sites – all are communications methods. Gaming consoles allow conversation among multiple players. Also, less obvious software – like word processing programs that allow log in from anywhere with internet access – can be used to communicate. Encryption is ubiquitous across the web for authenticating the validity and security of communications. Moreover, this is not just a design mandate for the U.S. – foreign governments will certainly demand similar access.

Details in the CALEA articles raise broad concerns.

1. Privacy invasions

The essence of a CALEA expansion would be the building of a surveillance back door into every online communication. A real world analogy helps to explain why this is so problematic. Imagine if the government required every home to be built with cameras and microphones pre-installed. It would provide little reassurance to know that the government would have to get a search warrant to turn those cameras on. We understand intuitively that government surveillance of private activities would be much too easy.

In addition, this proposal would switch the burden for surveillance from the government to companies (and through them to their customers, the American people). Every customer would be paying to have surveillance capability pre-installed and ready to go at a moment's notice. As a practical matter the cost to law enforcement of surveillance has provided real privacy protection by forcing law enforcement to determine if investigations are practical and appropriate uses of resources.

Perhaps most importantly, this proposal is a dramatic expansion of a dangerous idea – that the private sector should be responsible for building the government's surveillance infrastructure. We rely on others – often private companies – to provide the vast majority of services and goods we consume every day. CALEA was an expansion of private sector surveillance to phone service. We have already seen similar problematic expansions of this idea in banking and air travel.[4] The internet is a large and growing presence in our lives – it is deeply troubling to imagine it as the subject of easy and pervasive government scrutiny.

2. Human rights around the world

An expansion of CALEA by the United States would set an international standard. If the U.S. builds backdoors into internet communications devices, other governments – many of them repressive regimes like China and Iran – will want similar access. We have already seen the pivotal role that new technologies like Twitter and Facebook can play in promoting change. Both of these technologies are frequently cited as important ingredients in the Green Revolution in Iran and the recent mass protests in Egypt.

[4] See 49 CFR Parts 1540, 1544 and 1560 (Secure Flight Program Rules) and 31 CFR Part 103 (Financial Crimes Enforcement Network Rules).

In fact, internet freedom is a key objective of U.S. foreign policy. In a January 2010 speech, Secretary of State Hillary Clinton said:

> President Obama held a town hall meeting with an online component to highlight the importance of the internet. In response to a question that was sent in over the internet, he defended the right of people to freely access information, and said that the more freely information flows, the stronger societies become. He spoke about how access to information helps citizens hold their own governments accountable, generates new ideas, encourages creativity and entrepreneurship. The United States belief in that ground truth is what brings me here today.
>
> Because amid this unprecedented surge in connectivity, we must also recognize that these technologies are not an unmitigated blessing. These tools are also being exploited to undermine human progress and political rights. … And technologies with the potential to open up access to government and promote transparency can also be hijacked by governments to crush dissent and deny human rights.
>
> In the last year, we've seen a spike in threats to the free flow of information. China, Tunisia, and Uzbekistan have stepped up their censorship of the internet. In Vietnam, access to popular social networking sites has suddenly disappeared. … So while it is clear that the spread of these technologies is transforming our world, it is still unclear how that transformation will affect the human rights and the human welfare of the world's population.[5]

It would be ironic and saddening if these technologies – created and introduced in the United States – were converted from tools for freedom to tools of oppression with the assistance of misguided U.S. policies.

3. Effect on security and innovation

In addition to these core civil liberties concerns, the ACLU believes that the internet is one of the greatest tools for exercising an individual's constitutional rights. Any proposal that threatens the robustness of the internet – as this proposal does – is a matter of significant concern.

A wide array of security experts have stated that any weakening of encryption standards would almost certainly make internet communications less secure. Professor Steven Bellovin of Columbia University recently described the problem very clearly:

> Cryptography, it turns out, is far more complex than one would think. It isn't enough to have an unbreakable cipher; one has to use the cipher precisely correctly, in a stylized exchange of messages known as a cryptographic protocol. If the protocol is designed

[5]Secretary of State Hillary Clinton, *Remarks on Internet Freedom* delivered at the Newseum in Washington DC January 10, 2010. http://www.state.gov/secretary/rm/2010/01/135519.htm

incorrectly, it's often possible for an attacker to read encrypted messages even if the underlying cipher remains secure.

…

The administration's proposal would add a third party to communications: the government. This demands a much more complicated protocol. … Many previous attempts to add such features have resulted in new, easily exploited security flaws rather than better law enforcement access. In other words, instead of helping the government, the schemes created new opportunities for serious misuse. … The odds on everyone getting this right are exceedingly low; others have created security flaws when trying. [6]

It's not just the government that uses these back doors; they can be exploited by bad actors as well. In 2005 hackers took advantage of a similar law in Greece to hack into mobile communications system and listen to the calls of high government officials including those of the Prime Minister.[7]

The proposal would also substantially stifle innovation. Dozens of new technologies have arisen since 1994 – from instant messaging, to video game systems, to Skype. Today almost any document or technology accessible via the internet allows communications. Imagine if, when all of these technologies were created, each had to comply with law enforcement rules – or, worse, be pre-approved by law enforcement. Many of these technologies might never have gotten off the ground.

4. <u>There is no proof this system is necessary</u>

The number of wiretap orders the government seeks every year is a matter of public record and that record does not support this level of privacy invasion. The 2009 Wiretap Report (which describes all federal, state and local Title III wiretap orders – the only orders at issue here) listed only 32 wiretap orders for computers and only one encrypted communication.[8] In the case of that encrypted communication, law enforcement was able to gain access to the clear text of the communication.[9]

The government already has the legal authority to demand assistance of anyone – from a landlord to an internet service provider – in executing a wiretap order.[10] A company that refused to comply with a lawful Title III order could be held in contempt of court. On its face, this entire, wide-ranging proposal is aimed at easing very few orders in a situation where the

---

[6] Steven Bellovin, *The Worm and the Wiretap*, SMBlog, October 16, 2010. http://www.cs.columbia.edu/~smb/blog/2010-10/2010-10-16.html

[7] Vassilis Prevelakis and Diomidis Spinellis, *The Athens Affair,* IEEE Spectrum, July 2007 http://spectrum.ieee.org/telecom/security/the-athens-affair/0

[8] The Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral or Electronic Communications (2009 Wiretap Report), April 2010. See table 6. http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2009/Table6.pdf

[9] 2009 Wiretap Report pg. 5 http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2009/2009Wiretaptext.pdf

[10] 18 U.S.C. 2511(2)(a)(ii).

government already has substantial power to compel compliance. There must be more effective and less invasive alternatives.

Conclusion

The Obama administration has failed to demonstrate the pressing law enforcement need for such a massive change to our laws. Moreover, the proposal would weaken the internet, stifle innovation, harm privacy, and create major new security vulnerabilities. Because the balance of harms weighs heavily against the proposal and because of the absence of any profound justification for such a change, we urge Congress to reject the Obama administration's proposal to expand CALEA to internet communications devices.