(b)(5),(b)(7)(E)

(b)(5),(b)(7)(E)

in March 2004, DOJ, FBI, and DEA petitioned the Federal Communications Commission (FCC) to confirm that CALEA's requirements applied to Broadband Internet Access providers and certain Voice over Internet Protocol (VoIP) providers. In August 2005, the FCC ruled that Broadband Internet Access providers and interconnected VoIP providers fell within CALEA's scope.

(b)(5),(b)(7)(E)

There are currently over 250 million cellular phone users and 220 million broadband

Memorandum

Subject	Date
Drug Enforcement Administration Next Generation Wireless Strategy Status Report (DFN: 130-01)	FEB 2 3 2010

To

Preston L. Grubbs
Assistant Administrator
Operational Support Division

PLG 02/24/10

(b)(6),(b)(7)(C)

Deputy Assistant Administrator
Office of Investigative Technology

(b)(7)(E)

The information provided below outlines the efforts made by the Office of Investigative Technology (ST), in coordination with other DEA components, in furtherance of the DEA NGW Strategy.

INDUSTRY / TECHNOLOGY STRATEGY: (b)(7)(E) **meet the challenge of conducting electronic surveillance on emerging technologies. The Office of Investigative Technology (ST) will engage the law enforcement community and communications industry to obtain the support, resources, and knowledge to enable DEA to meet future electronic surveillance challenges.**

Accomplishments:

- (b)(7)(E)
-

(b)(7)(A),(b)(7)(E)

- Throughout 2009, ST personnel attended workshops and conferences with other federal, state, and local law enforcement agencies to address and make efforts to resolve ongoing or developing legal and/or technical issues with the major communications providers. During these workshops, ST provided a presentation on emerging communication.

(b)(7)(E)

(b)(5),(b)(6),(b)(7)(C),(b)(7)(E)

Communications can be encrypted by third party providers who do not maintain encryption keys and/or allow different encryption keys to be generated every communication. Encrypted communications can be accomplished through a managed service such as BlackBerry or an unmanaged service like Skype.[1]

(b)(5),(b)(7)(E)

[1] Washington Post Jan 19, 2010: Skype constitutes 12% of all international calling minutes (**Report: Skype Now Accounts For 12% Of All International Calling Minutes** (Robin Wauters))

(b)(5),(b)(7)(E)

Communications can be encrypted by third party providers who do not maintain encryption keys and/or allow different encryption keys to be generated every communication. Encrypted communications can be accomplished through a managed service such as BlackBerry or an unmanaged service like Skype.[1]

(b)(5),(b)(7)(E)

[1] Washington Post Jan 19, 2010: Skype constitutes 12% of all international calling minutes (**Report: Skype Now Accounts For 12% Of All International Calling Minutes** (Robin Wauters))

(b)(5),(b)(6),(b)(7)(C),(b)(7)(E)

September 27th, 2010 Government Seeks Back Door Into All Our Communications

Commentary by Seth Schoen

The *New York Times* reported this morning on a Federal government plan to put government-mandated back doors in *all communications systems, including all encryption software*. The *Times* said the Obama administration is *drafting a law that would impose a new "mandate" that all communications services be "able to intercept and unscramble encrypted messages" — including ordering "[d]evelopers of software that enables peer-to-peer communication [to] redesign their service to allow interception".*

Throughout the 1990s, EFF and others fought the "crypto wars" to ensure that the public would have the right to strong encryption tools that protect our privacy and security — with no back doors and no intentional weaknesses. We fought in court and in Congress to protect privacy rights and challenge restrictions on encryption, and to make sure the public could use encryption to protect itself. In a 1999 decision in the EFF-led Bernstein case, the Ninth Circuit Court of Appeals observed that

[w]hether we are surveilled by our government, by criminals, or by our neighbors, it is fair to say that never has our ability to shield our affairs from prying eyes been at such a low ebb. The availability and use of secure encryption may offer an opportunity to reclaim some portion of the privacy we have lost. Government efforts to control encryption thus may well implicate not only the First Amendment rights of cryptographers intent on pushing the boundaries of their science, but also the constitutional rights of each of us as potential recipients of encryption's bounty.

For a decade, the government backed off of attempts to force encryption developers to weaken their products and include back doors, and the crypto wars seemed to have been won. (Indeed, journalist Steven Levy declared victory for the civil libertarian side in 2001.) In the past ten years, even as the U.S. government has sought (or simply taken) vastly expanded surveillance powers, it never attempted to ban the development and use of secure encryption.

Now the government is again proposing to do so, following in the footsteps of regimes like the United Arab Emirates that have recently said some privacy tools are *too secure* and must be kept out of civilian hands.

As the Internet security community explained years ago, intentionally weakening security and including back doors is a recipe for disaster. "Lawful intercept" systems built under current laws have already been abused for unlawful spying by governments and criminals. Trying to force technology developers to include back doors is a recipe for disaster for our already-fragile on-line security and privacy. And like the COICA Internet censorship bill, it takes a page from the world's most repressive regimes' Internet-control playbook. This is exactly the wrong message for the U.S. government to be sending to the rest of the world.

The crypto wars are back in full force, and it's time for everyone who cares about privacy to stand up and defend it: no back doors and no bans on the tools that protect our communications.

https://www.eff.org/deeplinks/2010/09/government-seeks

(b)(6),(b)(7)(C)

3C - 7

EMERGING TRENDS IN THE TELECOMMUNICATIONS INDUSTRY

(b)(7)(E)

In order to keep abreast of the emerging trends in the telecommunications industry, DEA formed the Telecommunications Working Group (TWG). The TWG is responsible for identifying emerging trends in the telecom industry and how these trends will affect DEA, specifically our electronic surveillance capabilities. DEA management is often asked by Congressional staffers and budget personnel to identify specific instances where emerging technology prohibits DEA from the successful completion of our mission. Field personnel were recently solicited by the TWG regarding emerging technologies that had been encountered in the field that have affected enforcement operations. The following are examples that have been provided by field personnel as of July 25, 2006. The examples have been grouped by specific technology, for example (b)(7)(E) etc., and contain the point of contact regarding the specific investigation that was affected. Many of these investigations are ongoing therefore this information is to be controlled accordingly.

(b)(7)(A),(b)(7)(E)