

1 Jennifer Lynch (SBN 240701)
jlynch@eff.org
2 Mark Rumold (SBN 279060)
mark@eff.org
3 ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
4 San Francisco, CA 94110
Telephone: (415) 436-9333
5 Facsimile: (415) 436-9993

6 David L. Sobel (*pro hac vice*)
sobel@eff.org
7 ELECTRONIC FRONTIER FOUNDATION
1818 N Street, N.W.
8 Suite 410
Washington, DC 20036
9 Telephone: (202) 797-9009 x104
Facsimile: (202) 707-9066

10 Attorneys for Plaintiff
11 Electronic Frontier Foundation

12 **IN THE UNITED STATES DISTRICT COURT**
13 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**
14 **SAN FRANCISCO DIVISION**

15
16 ELECTRONIC FRONTIER FOUNDATION,)
17 Plaintiff,)
18 v.)
19 DEPARTMENT OF JUSTICE,)
20 Defendant.)
21)
22)
23)
24)
25 _____)

Case No. 3:10-cv-04892-RS
**THIRD DECLARATION OF
JENNIFER LYNCH IN SUPPORT OF
PLAINTIFF'S CROSS MOTION FOR
SUMMARY JUDGMENT AND
OPPOSITION TO DEFENDANT'S
MOTION FOR SUMMARY
JUDGMENT**

Date: May 31, 2012
Time: 1:30 p.m.
Place: Ctrm. 3, 17th Floor
Judge: Hon. Richard Seeborg

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1. I am an attorney of record for the plaintiff in this matter and a member in good standing of the California State Bar, and I am admitted to practice before this Court. I have personal knowledge of the matters stated in this declaration. If called upon to do so, I am competent to testify to all matters set forth herein.

2. Plaintiff Electronic Frontier Foundation (EFF) is a nonprofit corporation established under the laws of the Commonwealth of Massachusetts with offices in San Francisco, California and Washington, D.C. EFF is a donor-supported membership organization that works to inform policymakers and the general public about civil liberties issues related to technology and to act as a defender of those liberties. In support of its mission, EFF uses the Freedom of Information Act (FOIA) to obtain and disseminate information concerning the activities of federal agencies.

3. Attached hereto as Exhibit A is a true and correct copy of a letter dated April 26, 2012 and addressed to me from Valeree Villanueva, FOIA Specialist at the Department of Justice Office of Information Policy.

4. Attached hereto as Exhibit B are true and correct copies of responsive documents produced by the DEA.

I declare under penalty of perjury of the laws of the State of California that the foregoing is true and correct to the best of my knowledge and belief. Executed May 17, 2012 in San Francisco, California.

/s/ Jennifer Lynch
Jennifer Lynch

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

CERTIFICATE OF SERVICE

I hereby certify that on May 17, 2012, I electronically filed the foregoing document with the Clerk of the Court, using the CM/ECF system, which will send notification of such filing to the counsel of record in this matter who are registered on the CM/ECF system.

Executed on May 17, 2012, in San Francisco, California.

/s/ Jennifer Lynch

Jennifer Lynch

Exhibit A

Exhibit A



U.S. Department of Justice
Office of Information Policy
Suite 11050
1425 New York Avenue, NW
Washington, DC 20530-0001

Telephone: (202) 514-3642

APR 26 2012

Ms. Jennifer Lynch
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

Re: AG/11-00607 (F) DAG/11-00822 (F)
DAG/11-00387(F) OLP/11-00606 (F)
OLP/11-00608 (F) OLA/11-01068 (F)
VRB: VAV

Dear Ms. Lynch:

While processing your Freedom of Information Act (FOIA) requests dated September 28, 2010 for records created on or after January 1, 2006 pertaining to certain surveillance capabilities of the Department of Justice, the Drug Enforcement Agency (DEA) and Criminal Division referred documents, to this Office for processing and direct response to you on behalf of the Offices of the Attorney General, Deputy Attorney General, Legal Policy and Legislative Affairs. The DEA administrative tracking number is #10-00892-F and the Criminal Division administrative tracking number is #201000724F. For your information, the documents were received in this Office through a series of referrals between February and June 2011.

Please be advised that the Criminal Division referral, consisting of 362 pages, has been assigned file numbers DAG/11-00822 (F), OLP/11-00606 (F), and OLA/11-01068 (F). Additionally, the DEA referral, consisting of 278 pages, has been assigned file numbers AG/11-00607 (F), DAG/11-00387 (F), and OLP/11-00608 (F).

Upon review of the referred records, we determined that the documents contain information of interest to other Department components. Although we have completed initial consultations on the referred material, it is necessary for us to conduct additional consultations with Department components before final determinations can be made. I estimate that this process will be completed by May 29, 2012. Lastly, please be advised that much of this material is likely to be determined to be duplicative or not responsive to the subject of your requests.

I regret the necessity of this delay, but I assure you that your request will be processed as soon as possible. I understand that you have filed suit in the Northern District of California, Case No. 10-cv-04892.

Sincerely,

A handwritten signature in black ink, appearing to read "Valeree A. Villanueva".

Valeree A. Villanueva
FOIA Specialist

cc: Nicholas Cartier

Exhibit B

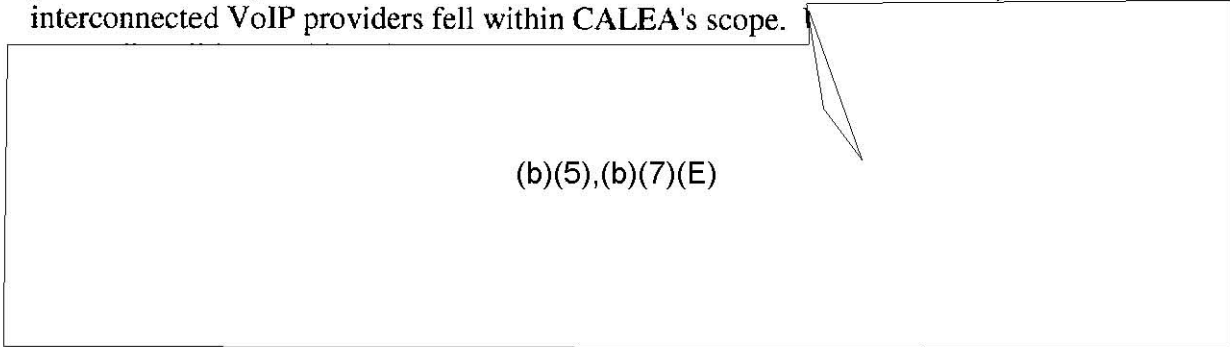
Exhibit B

(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 Drug Enforcement Administration Next Generation Wireless Strategy Status Report (DFN: 130-01)	Date FEB 23 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)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C)
Sent: Monday, July 20, 2009 5:59 PM
To: (b)(6),(b)(7)(C)
Cc:
Subject: RE: JMD Briefing on Going Dark
Attachments: doj-08-20-redacted.pdf

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

As we all know too well convergence is alive and well and is growing exponentially daily - as of February 11th, 2009, Apple reported more than 20,000 applications on their App Store (072009, <http://www.electronicpulp.net/2009/02/11/apples-iphone-app-store-now-hosts-20000-applications/>.)

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

I've also included the DOJ's IG Report on CALEA. Note the first paragraph where they highlight the following:

"Criminal organizations and individuals frequently use the telecommunication systems of the United States to further serious crimes, including terrorism, kidnapping, extortion, organized crime, drug trafficking, and public corruption. One of the most effective tools law enforcement agencies use to acquire evidence of these crimes is electronic surveillance techniques. **However, continuing advances in telecommunication technology have impaired and in some instances prevented law enforcement from conducting some types of authorized electronic surveillance.**" (8-20-08, DOJ IG Audit Redacted Report)

Please let me know if this helps or if you need anything further.

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

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

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

In March 2008, the U.S. Department of Justice (DOJ), Office of the Inspector General (IG) issued its Audit Report on the Implementation of the Communications Assistance for Law Enforcement Act (CALEA). In its executive summary, the report stated *"Criminal organizations and individuals frequently use the telecommunication systems of the United States to further serious crimes, including terrorism, kidnapping, extortion, organized crime, drug trafficking, and public corruption. One of the most effective tools law enforcement agencies use to acquire evidence of these crimes is electronic surveillance techniques. However, continuing advances in telecommunication technology have impaired and in some instances prevented law enforcement from conducting some types of authorized electronic surveillance."* (8-20-08, DOJ IG Audit Redacted Report).

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

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

Convergence is alive and well and is growing exponentially daily - as of February 11th, 2009, Apple reported more than 20,000 applications on their App Store.

<http://www.electronicpulp.net/2009/02/11/apples-iphone-app-store-now-hosts-20000-applications/>.

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

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

Today the ability to communicate on a mobile device can occur almost anywhere—yes in a house, yes on a boat, yes in a car, yes on a plane, and yes on a train. The variety and number of communication methods and devices continues to grow as support for ubiquitous broadband grows. Terms like Android, iPhone, App Store, Wi-Max, LTE, BlackBerry, and Skype are becoming familiar words in our national lexicon. Congress' mandate that the Federal Communications Commission (FCC) develop a National Broadband Plan and the FCC's own rule making proceeding on an Open Internet illustrate the emphasis and importance of broadband and emerging communication technology as national resources. Although these innovative technologies bring great promise to the well being, public safety and national security of the United States, they also bring challenges.

(b)(5),(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>

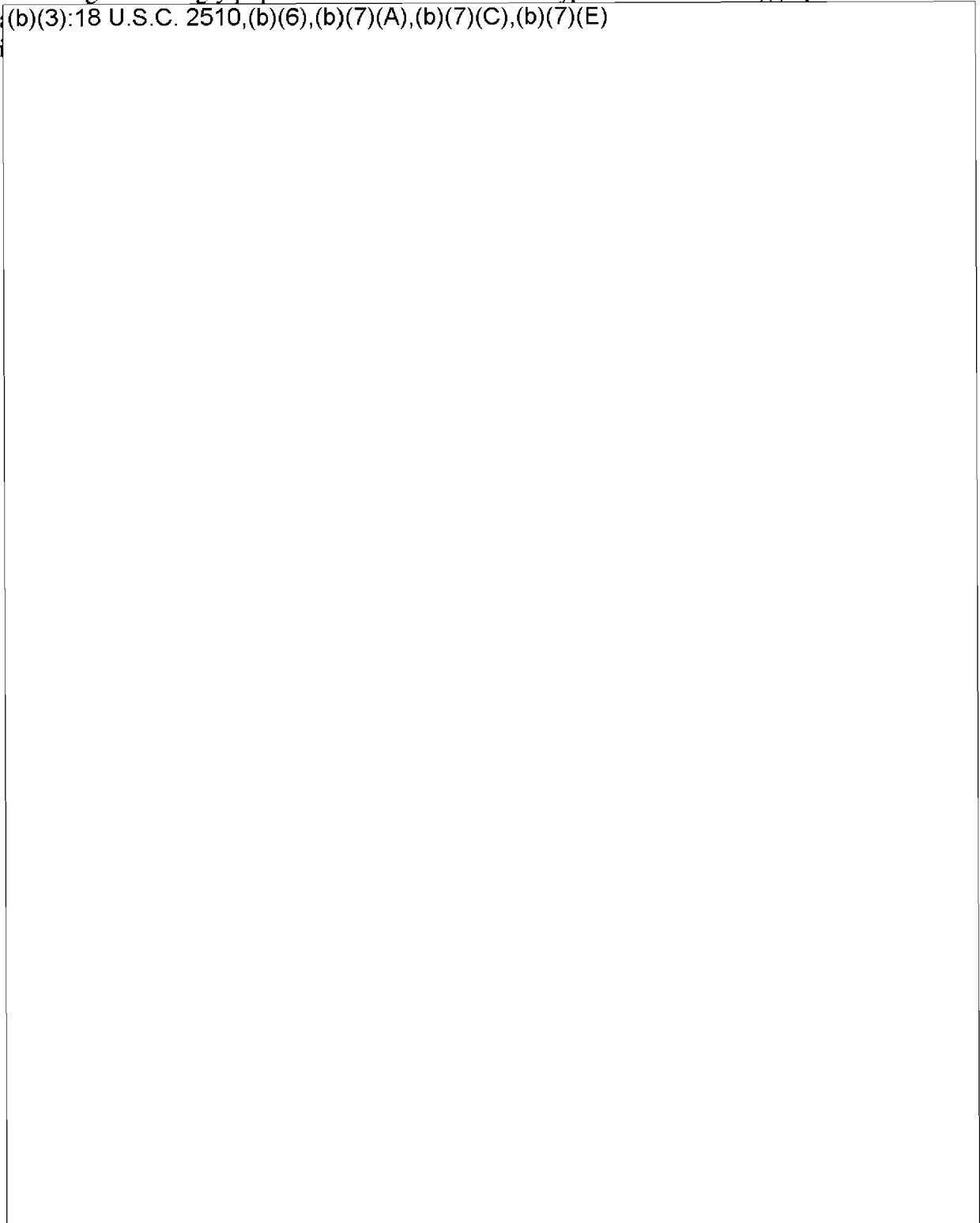
(b)(6),(b)(7)(C)

VOIP / SKYPE CASE EXAMPLES:

Skype is a VoIP service that allows users to chat, instant message, make or receive phone calls or transfer files worldwide over the Internet securely and free of charge. Dialogue is transmitted through a headset, speakers or a USB phone. A new Internet mobile phone service also allows Skype users to converse over the Internet using cell phones.

Launched in 2003, Skype is an efficient and reliable means of communication and is becoming increasingly popular in the United States. Skype is also becoming popular

(b)(3):18 U.S.C. 2510,(b)(6),(b)(7)(A),(b)(7)(C),(b)(7)(E)



(b)(7)(E)

VIRTUAL WORLDS AND ONLINE GAMING CASE EXAMPLES:

A virtual world is a computer-based simulated environment where users bit and interact via avatars, or graphical representations. The virtual world may depict a real world or a fantasy world. Users communicate through text-chat and real-time voiced-based chat. Virtual worlds provide versatility and anonymity and allow for covert communications. Voice-based chat is available through many virtual worlds using VoIP, such as Skype. Online role playing games like Second Life, are increasing in popularity. These games are completely online and require no gaming console, yet provide similar open VoIP, text messaging and IM communications. (b)(7)(E)

(b)(7)(E)

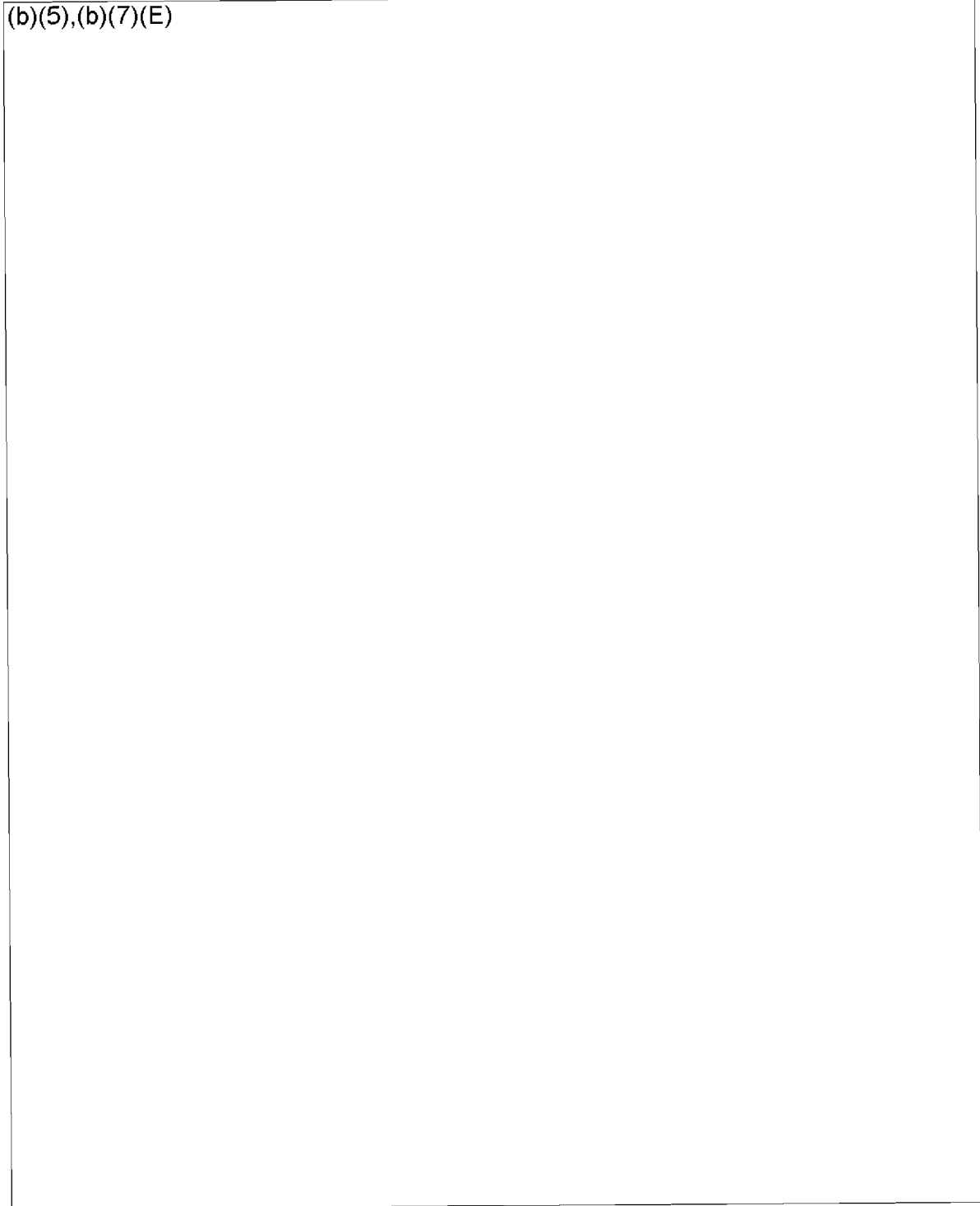
(b)(7)(E)

(b)(7)(D),(b)(7)(E)

VOIP / SKYPE CASE EXAMPLES:

Skype is a VoIP service that allows users to chat, instant message, make or receive phone calls or transfer files worldwide over the Internet securely and free of charge. Dialogue is transmitted through a headset, speakers or a USB phone. A new Internet mobile phone service also allows Skype users to converse over the Internet using cell phones. Launched in 2003, Skype is an efficient and reliable means of communication and is becoming increasingly popular in the United States. Skype is also becoming popular

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

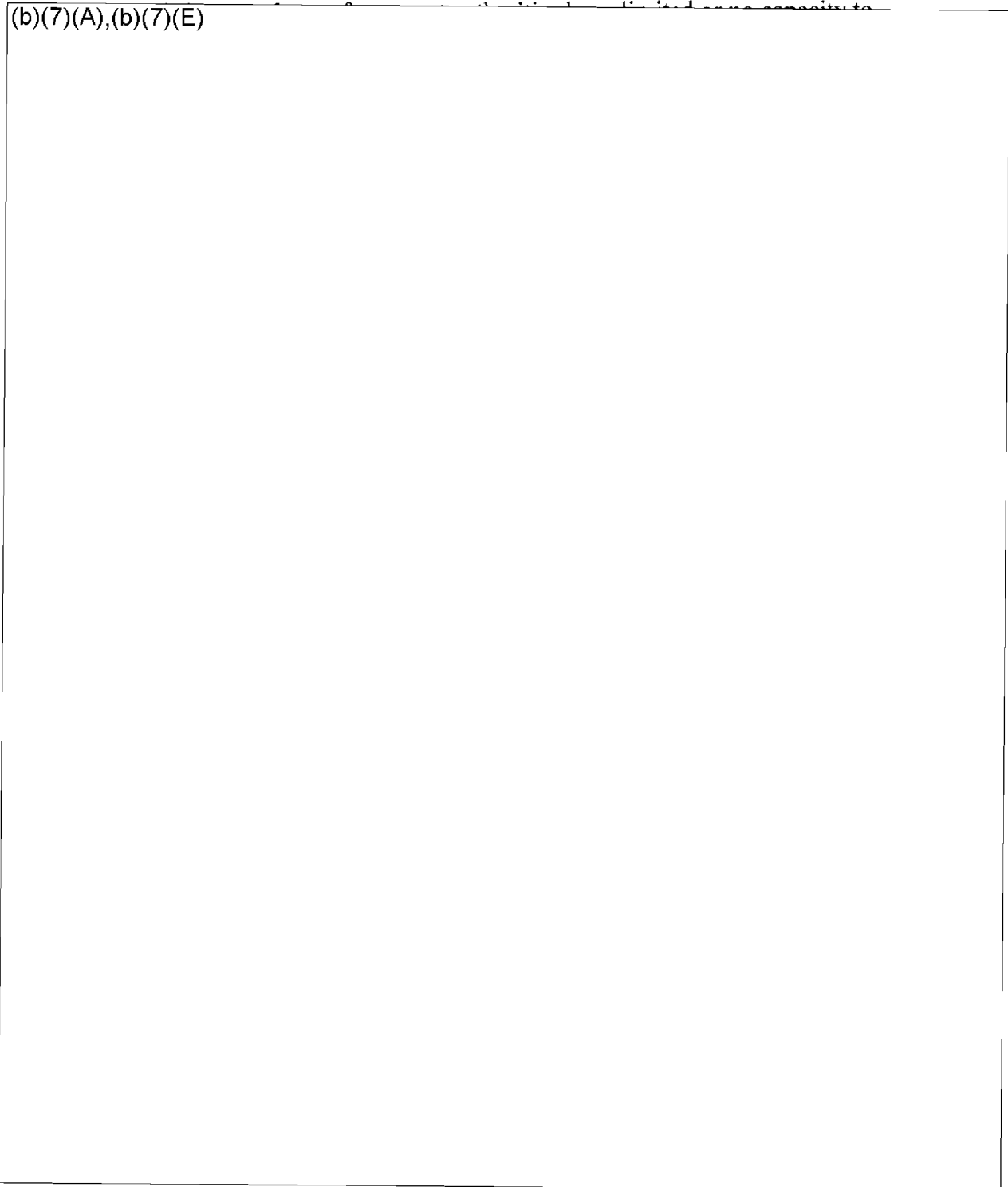


VOIP / SKYPE CASE EXAMPLES:

Skype is a VoIP service that allows users to chat, instant message, make or receive phone calls or transfer files worldwide over the Internet securely and free of charge. Dialogue is transmitted through a headset, speakers or a USB phone. A new Internet mobile phone service also allows Skype users to converse over the Internet using cell phones.

Launched in 2003, Skype is an efficient and reliable means of communication and is becoming increasingly popular in the United States. Skype is also becoming popular

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



VIRTUAL WORLDS AND ONLINE GAMING CASE EXAMPLES:

A virtual world is a computer-based simulated environment where users bit and interact via avatars, or graphical representations. The virtual world may depict a real world or a fantasy world. Users communicate through text-chat and real-time voiced-based chat. Virtual worlds provide versatility and anonymity and allow for covert communications. Voice-based chat is available through many virtual worlds using VoIP, such as Skype. Online role playing games like Second Life, are increasing in popularity. These games are completely online and require no gaming console, yet provide similar open VoIP, text messaging and IM communications.

(b)(7)(D),(b)(7)(E)

VIRTUAL WORLDS AND ONLINE GAMING CASE EXAMPLES:

A virtual world is a computer-based simulated environment where users bit and interact via avatars, or graphical representations. The virtual world may depict a real world or a fantasy world. Users communicate through text-chat and real-time voiced-based chat. Virtual worlds provide versatility and anonymity and allow for covert communications. Voice-based chat is available through many virtual worlds using VoIP, such as Skype. Online role playing games like Second Life, are increasing in popularity. These games are completely online and require no gaming console, yet provide similar open VoIP, text messaging and IM communications.

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

(b)(7)(E)

VIRTUAL WORLDS AND ONLINE GAMING CASE EXAMPLES:

A virtual world is a computer-based simulated environment where users bit and interact via avatars, or graphical representations. The virtual world may depict a real world or a fantasy world. Users communicate through text-chat and real-time voiced-based chat. Virtual worlds provide versatility and anonymity and allow for covert communications. Voice-based chat is available through many virtual worlds using VoIP, such as Skype. Online role playing games like Second Life, are increasing in popularity. These games are completely online and require no gaming console, yet provide similar open VoIP, text messaging and IM communications. (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(D),(b)(7)(E)

VOIP / SKYPE CASE EXAMPLES:

Skype is a VoIP service that allows users to chat, instant message, make or receive phone calls or transfer files worldwide over the Internet securely and free of charge. Dialogue is transmitted through a headset, speakers or a USB phone. A new Internet mobile phone service also allows Skype users to converse over the Internet using cell phones. Launched in 2003, Skype is an efficient and reliable means of communication and is becoming increasingly popular in the United States. Skype is also becoming popular

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



Rebtel Overview

Rebtel is a mobile VoIP call back service. With Rebtel you give them the phone number of a friend in another country, and we give you a local number for them. You then save this number on your mobile so you can call your friend whenever you want, for a fraction of your normal international rate. Now, if your friend also has Rebtel, you can call each other for absolutely free. First, call your friend on their Rebtel number. Then, ask your friend to call you back. Tell them to use the number shown on their phone screen. From there, stay on the line. In a few seconds your friend will join you back on the call.

Basic Info

Headquarters	Stockholm, Sweden
Year Established	2006
Call Type(s)	Mobile VoIP Call Back Service
Compatible Phones	You can use Rebtel from any cellular, VoIP or land-line telephone.
Availability	Rebtel service is available anywhere there is a cellular, landline or VoIP connection.
Free Calls	Rebtel users can make free calls to all Rebtel users.
Phone Number	With Rebtel there is no need for a new phone number as Rebtel uses your existing cellular, VoIP or land-line telephone to give you free and low cost calling. Rebtel works by taking your existing phone number and assigning it a Rebtel number that other Rebtel users can also use to call you for free. The only new number you will need is a Rebtel local access number that is provided to you when you sign-up.
Calling Rates	Rebtel offers low cost international calls and free in country calling to other Rebtel users
SMS	Rebtel allows you to initiate phone calls via SMS, but does not offer SMS services
Instant Messaging	Rebtel does not offer instant messaging services
Special Features	With Rebtel there is no need for a new phone number as Rebt uses your existing cellular, VoIP or land-line telephone to give you free and low cost calling. You can access their service via SMS, via the web (or via a mobile web browser) in addition to your VoIP, cellular or landline telephone.

The DEA conducts more Title III intercepts than any other law enforcement agency in the United States. As such, DEA has a significant interest in the impact emerging communication technologies will have on the future of lawful electronic surveillance, and our ability to successfully target the command and control of drug trafficking organizations that pose a significant threat to the security of our country.

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

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

(b)(2),(b)(5),(b)(6),(b)(7)(A),(b)(7)(C)

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

From: (b)(6),(b)(7)(C)
Sent: Friday, September 24, 2010 4:49 PM
To: Goggin, Wendy H.; Grubbs, Preston L.
Subject: RE: case eg's

I just inquired from TWG whether we had an example like this handy. It may be too late for the NYT article but as this proceeds those examples would be good to have.

From: Goggin, Wendy H.
Sent: Friday, September 24, 2010 4:26 PM
To: Grubbs, Preston L.; (b)(6),(b)(7)(C)
Subject: Re: case eg's

Although this an example where there was a work around solution. The best example is when a bad guy walks with all the money.

From: Grubbs, Preston L.
To: (b)(6),(b)(7)(C) Goggin, Wendy H.
Sent: Fri Sep 24 15:51:06 2010
Subject: RE: case eg's

Ok with me. No more specific information is necessary, correct. PLG

From: (b)(6),(b)(7)(C)
Sent: Friday, September 24, 2010 3:42 PM
To: Grubbs, Preston L.; Goggin, Wendy H.
Subject: FW: case eg's

Preston and Wendy,
I don't see any problem with this, do you? Thanks (b)(6),(b)(7)(C)

From: Sabol, Sherry E. [mailto:Sherry.Sabol@ (b)(2),(b)(6),(b)(7)(C)]
Sent: Friday, September 24, 2010 3:39 PM
To: (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)
Subject: FW: case eg's

(b)(6),(b)(7)(C) does DEA have any issue/objection to us providing the following to the NY Times as an example for Going Dark?

-
- (b)(7)(E)
-

In 2010, we investigated (b)(7)(E) Drug Trafficking Organization that used a peer-to-peer application (b)(7)(E)


- o Because peer-to-peer applications (b)(7)(E) they are difficult to intercept.

- o This forced DEA and FBI to use a risky, court-ordered entry at the target's office to install (b)(7)(E)
- o Eventually, we obtained an indictment and (b)(7)(E) (b)(7)(E) solution in this particular case created delays and prevented the interception of pertinent communications.

DEA SENSITIVE,
DO NOT RELEASE WITHOUT THE EXPRESS PERMISSION OF DEA'S OFFICE OF THE CHIEF COUNSEL

- 3.3 billion active cell phones on a planet of 6.6 billion people
 - fastest diffusion of any type of technology in history
- 2G capabilities and solutions do not work against Next Generation Wireless (NGW) technology
 - Circuit vs. Data
 - Public vs. Private Design

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



I-Phone

Multiple Carriers in 2010

- Currently serviced only through AT&T
- Multiple applications that facilitate voice and data communications.
 - Skype, Fring, Free SMS, Email, Facebook

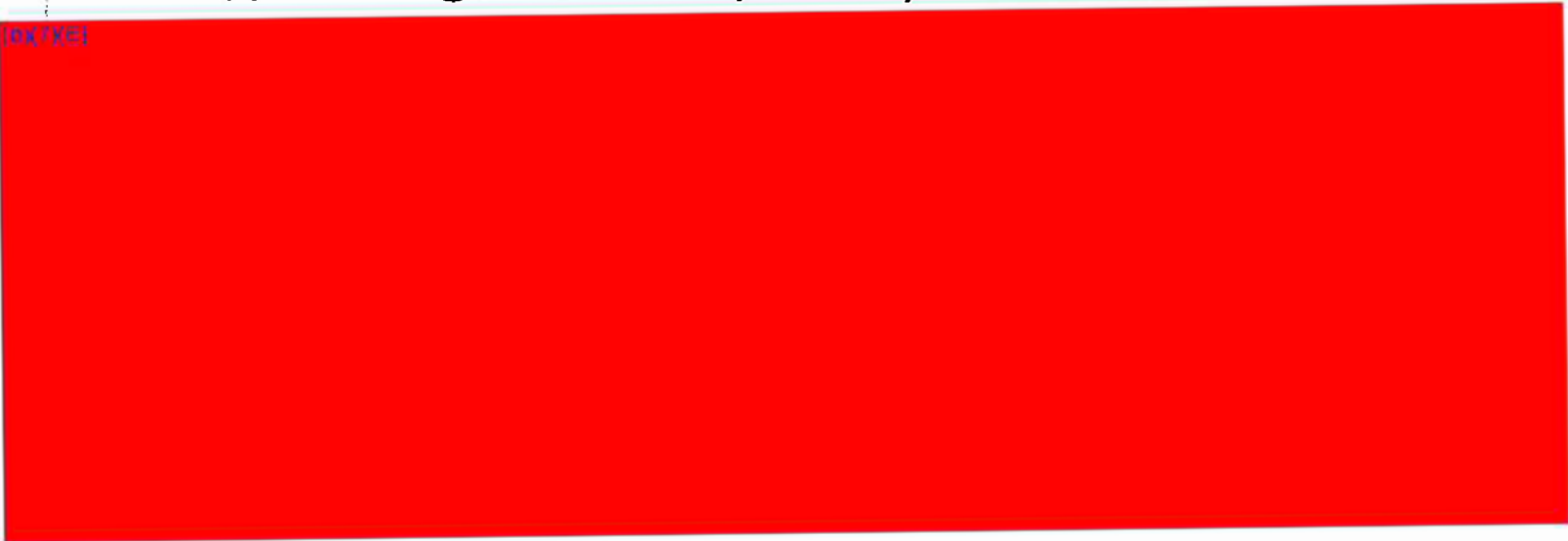
(b)(5), (b)(7)(E)




I-Phone

- A Smartphone manufactured by Apple Inc. and currently offered only through AT&T- (U.S.)
- Supports multiple applications through Apple iTunes that facilitate voice and data communications over the cellular and WiFi networks.
 - Skype, Fring, Free SMS, Email, Facebook

(b)(7)(C)



Facebook

- Exploiting social networking accounts allows law enforcement to obtain information to further an investigation, including associates (friends), email addresses, phone numbers, photos, credit card information, etc. 

(b)(7)(E)



- 2703c
- Preservation Letter
- 2703d
- Search Warrant

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

From: Goggin, Wendy H.
Sent: Friday, August 13, 2010 11:52 AM
To: (b)(6),(b)(7)(C)
Cc:
Subject: Fw: (b)(7)(E)

From: Caproni, Valerie E. <Valerie.Caproni@ic.fbi.gov>
To: Goggin, Wendy H.
Sent: Fri Aug 13 11:40:48 2010
Subject: RE: (b)(7)(E)

(b)(7)(E)

From: Goggin, Wendy H. [mailto:(b)(6),(b)(7)(C)]
Sent: Friday, August 13, 2010 11:35 AM
To: Caproni, Valerie E.
Subject: Re: (b)(7)(E)

(b)(7)(E)

From: Caproni, Valerie E. <Valerie.Caproni@ic.fbi.gov>
To: Goggin, Wendy H.
Sent: Fri Aug 13 08:50:54 2010
Subject: Re: (b)(7)(E)

(b)(7)(E)

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

as mentioned in a recent Washington Post

blog:

- 1) Kevin Bankston, senior staff attorney at the Electronic Frontier Foundation, took issue with the move. "This proposal is a drastic **anti-privacy, anti-security, anti-innovation** solution in search of a problem," he said. He noted that in an official 2009 review of **2,400 federal, state and local law enforcement applications for wiretap orders, "encryption was encountered during one state wiretap**, but did not prevent officials from obtaining the plain text of the communications."

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

-4-

Not responsive

19. DEA presentation on Narco-Terrorism – Special Operations Division Technology Issues:
Derick S. Maltz, Special Agent in Charge, Special Operations Division, DEA, and USA Russ
Dedrick (E/TN) gave a security presentation about the links between drug trafficking and terrorist
financing. (b)(7)(E)

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

Per DEA,
FBI, OIP

(b)(5)

Per OIP

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

phone

Questions should be directed to USA Russ Dedrick at

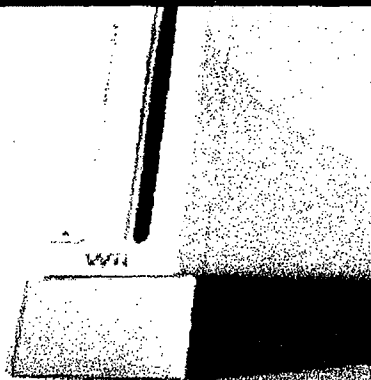
(b)(6),(b)(7)(C)

Not responsive

Gaming systems can be used for email communication.

(b)(7)(E)

GAME





Challenge: ID Spoofing

(b)(7)(E)



Law Enforcement Sensitive

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)



From: Sabol, Sherry E.
Sent: Monday, June 07, 2010 7:56 PM
To: [Redacted]
Cc: [Redacted]
Subject: Fw: [Redacted] Case Example [Redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-13-2011 BY 65179/DMH/BAW/STP/bls

b6
b7C
b7E

Sensitivity: ~~Confidential~~

From: (b)(6),(b)(7)(C)
To: Sabol, Sherry E.
Sent: Mon Jun 07 19:24:39 2010
Subject: RE: (b) Case Example ((b)(7)(E))

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-13-2011 BY 65179/DMH/BAW/STP/bls

Sherry and [Redacted]
Here is another (b)(7)(E) case example from

(b)(7)(E)

b6
b7C Per FBI

(b)(5),(b)(6),(b)(7)(A),(b)(7)(C),(b)(7)(D),(b)(7)(E),(b)(7)(F)

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

EFF/Lynch-765

file://D:\Going Dark\Fw [Redacted] Case Example [Redacted].htm

b7E 5/9/2011



b7E

Page 2 of 3

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

From: Sabol, Sherry E. [mailto:Sherry.Sabol@ic.fbi.gov]

Sent: Monday, June 07, 2010 2:33 PM

To: [Redacted]

Cc: [Redacted]

Subject: RE: [Redacted] Case Example [Redacted]

Sensitivity: Confidential

b6

b7C

b7E

Thank you. We may need something on ELSUR if you have it. If not, we'll go with what we have.
Sherry.

From: (b)(6),(b)(7)(C)

Sent: Monday, June 07, 2010 11:04 AM

To: Sabol, Sherry E.

Cc: [Redacted]

Subject: (b) Case Example (Data Retention-Preservation)

Sensitivity: Confidential

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-13-2011 BY 65179/DMH/BAW/STP/bls

b6

b7C

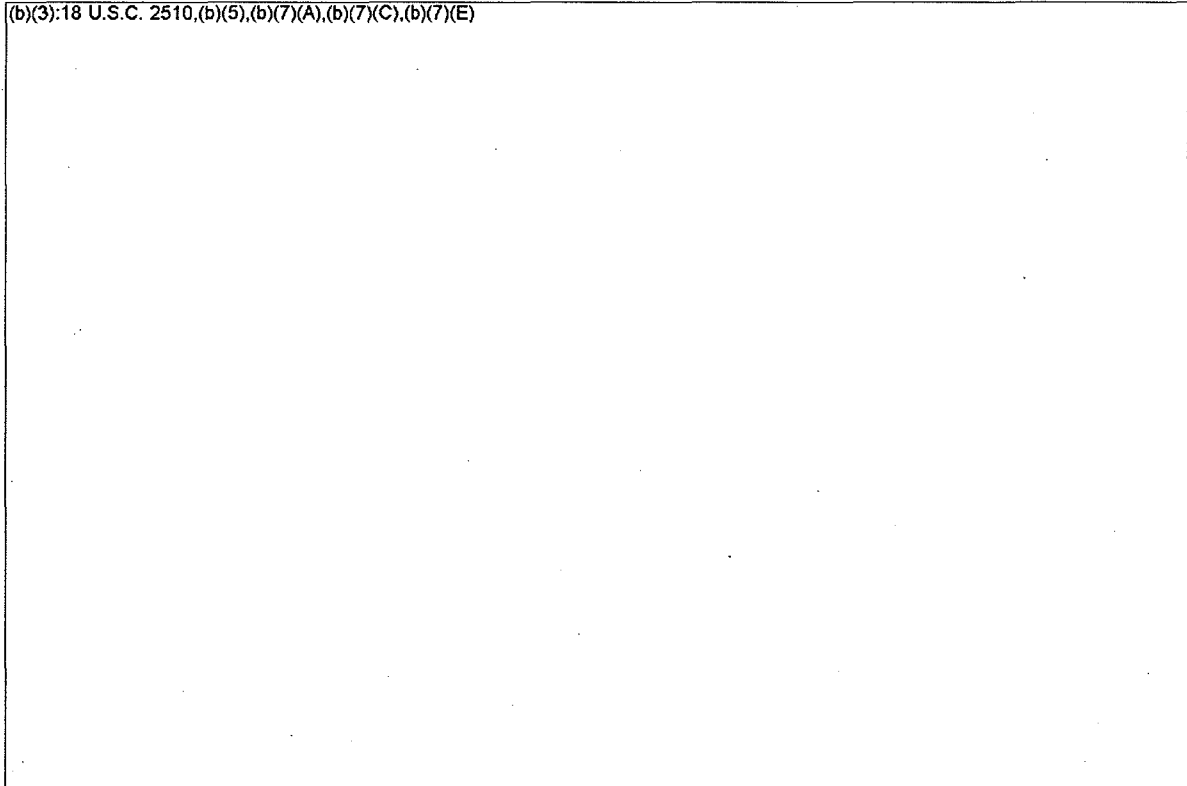
Per FBI

Sherry and [Redacted]

Here is a (b)(7)(E) case example that demonstrates the need for [Redacted]

(b)(6),(b)(7)(E)

(b)(3):18 U.S.C. 2510,(b)(5),(b)(7)(A),(b)(7)(C),(b)(7)(E)



EFF/Lynch-766

file://D:\Going Dark\Fw [Redacted] Case Example [Redacted].htm

b7E

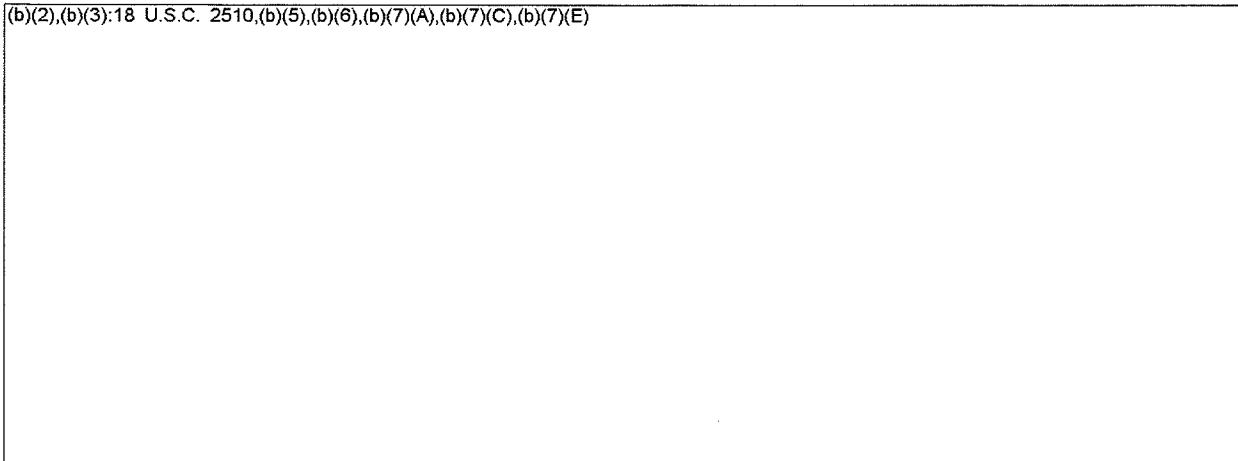
5/9/2011



b7E

Page 3 of 3

(b)(2),(b)(3):18 U.S.C. 2510,(b)(5),(b)(6),(b)(7)(A),(b)(7)(C),(b)(7)(E)



EFF/Lynch-767

b7E

5/9/2011