

From: [redacted]
To: [redacted]
Date: 2/21/03 10:16AM
Subject: Re: Collection of Cell Site Location Data

[redacted] Thanks for the info. The question from the field stems from a disparity between the ELSUR guide produced by OEO and [redacted] analysis. It appears that an SA got hold of both these, noticed the differing opinions, and pointed that out to the CDC [redacted] I don't know if it was related to a specific case or not.

[redacted]

B-5 b5

I'll find out if there is a specific case which requires appropriate advisement, or whether this was just a question raised for interesting conversation between a SA and CDC. That will help to determine the priority for this.

Thanks.

[redacted]

>>> [redacted] 02/14/03 04:23PM >>>

[redacted]

B-5
b6
b7C
b5

Did the question from the field involve a use where they would not otherwise need to get a (d) order?

>>> [redacted] 02/14 2:16 PM >>>

[redacted]

B-5
b6
b7C
b5
B-5

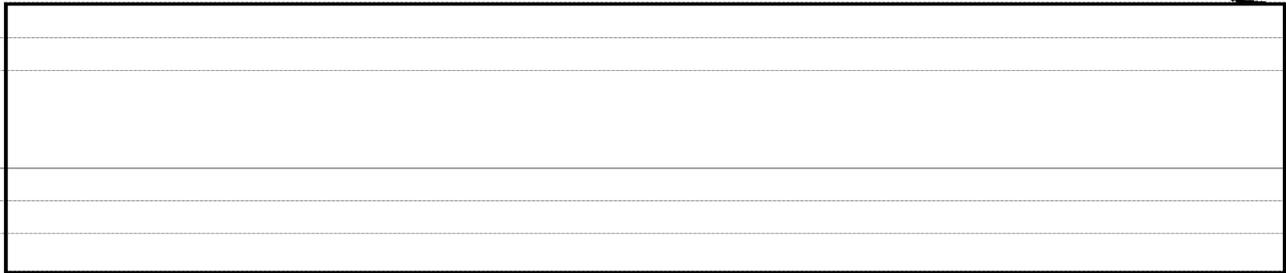
Thanks.

[redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 04-09-2013 BY NSICG J76J18T80

From:
To:
Date: 2/11/03 10:56AM
Subject: Electronic Surveillance Issue

b6
b7C
b7E



B-5

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 04-09-2013 BY NSICG J76J18T80

From: [redacted]
To: [redacted]
Date: 1/23/02 12:15PM
Subject: Re: CCIPS NEW PR/T&T [redacted] Interpretation

b6
b7C
b5
b7E

B5

[redacted] and [redacted] has advised CCIPS [redacted] of that.
We are in the process of putting together an analysis, but in general here are my thoughts:

[redacted]

b5

[redacted]

b5

see note ①

[redacted]

b5

B5

[redacted]

b5

B5

[redacted]

b5
b7E

B5

B5

B5 o/s

o/s L

o/s B5

B5

[Redacted]

b6
b7C
b5
b7E
B-E

>> [Redacted] 01/23/02 11:36AM >>>

[Redacted] Lets get [Redacted] comments before we change the ELSUR Guide. I read the opinion and agree with your assessment. Thanks [Redacted]

>>> [Redacted] 01/23 11:31 AM >>>

[Redacted] I've reviewed the CCIPS analysis and concur [Redacted] Has there been any additional discussion on this yet?

B-5

[Redacted] This will result in additional changes to the ELSUR manual. Unless advised to the contrary, I'll ensure these changes are made.

b5
b6
b7C
b7E

>> [Redacted] 01/17/02 06:27PM >>>

Attached is the most recent legal analysis issued by CCIPS to all AUSA/CTCs recommending that AUSAs [Redacted]

I have requested that CCIPS delay further dissemination of this opinion until we have had an opportunity to review it. They have not yet responded back.

[Redacted] AGC
Technology Law Unit
Office of the General Counsel
FEDERAL BUREAU OF INVESTIGATION
935 Pennsylvania Ave., N.W. Rm [Redacted]
Washington, D.C. 20535-0001
Tel. [Redacted]
Fax [Redacted]

[Redacted]

B5

b5
b6
b7C

Engineering Research Facility
Bldg. 27958A, Rm [Redacted]
Quantico, VA 22135
Tel [Redacted]
Fa [Redacted]

TDY Rochester RA
FBI, Room [Redacted]
100 State Street
Rochester, NY 14614
Tel [Redacted]
Fax [Redacted]

Pag [Redacted]
Internet E-mail with advance notice to [Redacted]@leo.gov

b6
b7C

CC: [Redacted]

U//FOUO

Operating a Cell Site Simulator, [redacted] to Locate a Cell Phone

b7E

Operation of a Cell Site Simulator (CSS) [redacted] requires different court orders under different circumstances. In order to determine which court order(s) is/are needed in a particular case, a "Cell Phone Location Quick Reference Guide" is attached as Appendix C. To the extent that a pen register order, or Rule 41 warrant is required, the emergency provisions for each are discussed above, as are the consent exceptions.

Attorney/client privileged

U//FOUO

9

*From - Emergency Authority Guide
2008*

[redacted]

b6
b7C

U//FOUO

Appendix C
[Cell Phone Location Quick Reference Guide]

Technique(s) To Be Used	Legal Process Needed	Legal Standard

b5
b7E

b5

b5

Note: the exceptions for the consent or implied consent of the subscriber, and the exigent circumstance exception to the Fourth Amendment are discussed above. These exceptions may be applicable for cell phone location, depending on the facts.

U//FOUO

Attorney/Client privileged

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 04-09-2013 BY NSICG J76J18T80

Date: 01/14/2002 09:28 am -0500 (Monday)
From: [redacted]
To: Ccips att: [redacted]
CC: [redacted]
Subject: please forward to CTC's

Attached is an analysis of the appropriate legal process for locating cell phones, in light of the changes enacted in the USA PATRIOT Act.



B-5

b5

B-5

The attached analysis will also be available soon in USA Book.

Feel free to contact [redacted] in the Computer Crime and Intellectual
Property Section, or [redacted] in the Office of Enforcement Operations if
you have any questions or comments.

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED

04-09-2013 BY NSICG J76J18T80

From: [redacted]
To: [redacted]
Date: 1/17/02 6:27PM
Subject: CCIPS NEW PR/T&T [redacted] Interpretation

b6
b7C
b5
b7E

Attached is the most recent legal analysis issued by CCIPS to all AUSA/CTCs recommending that [redacted]

B-5?

I have requested that CCIPS delay further dissemination of this opinion until we have had an opportunity to review it. They have not yet responded back.

[redacted] AGC
Technology Law Unit
Office of the General Counsel
FEDERAL BUREAU OF INVESTIGATION
935 Pennsylvania Ave., N.W. Rm [redacted]
Washington, D.C. 20535-0001

Tel [redacted]
Fax [redacted]

b6
b7C

Engineering Research Facility
Bldg. 27958A, Rm [redacted]
Quantico, VA 22135

Tel [redacted]
Fax [redacted]

TDY Rochester RA
FBI, Room [redacted]
100 State Street
Rochester, NY 14614

Tel [redacted]
Fax [redacted]

Pag [redacted]
Internet E-mail with advance notice to: [redacted]@leo.gov

~~execute such an order at one central point and not require the "use" of the device outside of the court's jurisdiction.~~

o/s

II. Collection of Cell Phone Location Information Directly by Law Enforcement

Law enforcement possesses electronic devices that allow agents to determine the location of certain cellular phones by the electronic signals that they broadcast. This equipment includes an antenna, an electronic device that processes the signals transmitted on cell phone frequencies, and a laptop computer that analyzes the signals and allows the agent to configure the collection of information. Working together, these devices allow the agent to identify the direction (on a 360 degree display) and signal strength of a particular cellular phone while the user is making a call. By shifting the location of the device, the operator can determine the phone's location more precisely using triangulation.

In order to use such a device the investigator generally must know the target phone's telephone number (also known as a Mobile Identification Number or MIN). After the operator enters this information into the tracking device, it scans the surrounding airwaves. When the user of that phone places or receives a call, the phone transmits its unique identifying information to the provider's local cell tower. The provider's system then automatically assigns the phone a particular frequency and transmits other information that will allow the phone properly to transmit the user's voice to the cell tower. By gathering this information, the tracking device determines which call (out of the potentially thousands of nearby users) on which to home in. While the user remains on the phone, the tracking device can then register the direction and signal strength (and therefore the approximate distance) of the target phone.

A. Use of Law Enforcement Cell Phone Tracking Devices Prior to the USA PATRIOT Act of 2001

In 1994, the Office of Enforcement Operations opined that investigators did not need to obtain any legal process in order to use cell phone tracking devices so long as they did not capture

the numbers dialed or other information "traditionally" collected using a pen/trap device. This analysis concluded that the "signaling information" automatically transmitted between a cell phone and the provider's tower does not implicate either the Fourth Amendment or the wiretap statute because it does not constitute the "contents" of a communication. Moreover, the analysis reasoned – prior to the 2001 amendments – that the pen/trap statute did not apply to the collection of such information because of the narrow definitions of "pen register" and "trap and trace device." Therefore, the guidance concluded, since neither the constitution nor any statute regulated their use, such devices did not require any legal authorization to operate.

B. The Pen/Trap Statute, As Amended By The USA PATRIOT Act of 2001

Although the analysis remains unchanged with respect to the Fourth Amendment and the wiretap statute, substantial amendments to the definitions of "pen register" and "trap and trace device" in the USA PATRIOT Act alter the applicability of the pen/trap statute. The new definitions, on their face, strongly suggest that the statute now governs the use of such devices. Where the old definition of "pen register" applied only to "numbers dialed or otherwise transmitted," "pen register" now means

a device or process which records or decodes dialing, routing, addressing, and signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted....

18 U.S.C. § 3127(3). "Signaling information" is a broader term that encompasses other kinds of non-content information used by a communication system to process communications. This definition appears to encompass all of the non-content information passed between a cell phone and the provider's tower.

Similarly, the USA PATRIOT Act broadened the definition of "trap and trace device." Where before the definition included only "the originating number of an instrument or device," the new definition covers "the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication...." 18 U.S.C. § 3127(4). Like the definition of "pen register," this broader definition appears to include

such information as the transmission of a MIN, which identifies the source of a communication.

Moreover, the scant legislative history that accompanied passage of the Act suggests Congress intended that the new definitions apply to all communications media, instead of focusing solely on traditional telephone calls. Although the House Report cannot definitively state the intent of both houses of Congress when passing the final bill, it does strongly suggest that Congress intended that the statute would apply to all technologies:

This section updates the language of the statute to clarify that the pen/register [sic] authority applies to modern communication technologies. Current statutory references to the target "line," for example, are revised to encompass a "line or other facility." Such a facility includes: *a cellular telephone number; a specific cellular telephone identified by its electronic serial number (ESN); an Internet user account or e-mail address; or an Internet Protocol (IP) address, port number, or similar computer network address or range of addresses.* In addition, because the statute takes into account a wide variety of such facilities, section 3123(b)(1)(C) allows applicants for pen register or trap and trace orders to submit a description of the communications to be traced using any of these or other identifiers.

Moreover, the section clarifies that orders for the installation of pen register and trap and trace devices may obtain *any* non-content information - "dialing, routing, addressing, and signaling information" - utilized in the processing and transmitting of wire or electronic communications....

This concept, that the information properly obtained by using a pen register or trap and trace device is non-content information, *applies across the board to all communications media ... ([and includes] packets that merely request a telnet connection in the Internet context).*

H.R. Rept 107-236, at 52-53 (emphasis added). Indeed, this last reference to a packet requesting a telnet session - a piece of information passing between machines in order to establish a communication session for the human user - provides a close analogy to the information passing between a cell phone and the nearest tower in the initial stages of a cell phone call.

Finally, the House Report recognizes that pen registers and trap and trace devices could include devices that collect information remotely. The Report states:

Further, *because the pen register or trap and trace 'device' is often incapable of being physically 'attached' to the target facility due to the nature of modern communication technology,* section 101 makes two other related changes.

First, in recognition of the fact that such functions are commonly performed today by software instead of physical mechanisms, the section allows the pen register or trap and trace device to be 'attached or applied' to the target facility [such as an ESN]. Likewise, the definitions of 'pen register' and 'trap and trace device' in section 3127 are revised to include an intangible 'process' (such as a software routine) which collects the same information as a physical device.

H.R. Rept 107-236, at 53 (emphasis added). Thus, the statutory text and legislative history strongly suggest that the pen/trap statute governs the collection of cell phone location information directly by law enforcement authorities.

C. The Inapplicability of CALEA's Prohibition on Collection Using Pen/Trap Authority

In passing CALEA in 1994, Congress required providers to isolate and provide to the government certain information relating to telephone communications. At the same time that it created these obligations, it created an exception: carriers shall not provide law enforcement with "any information that may disclose the physical location of the subscriber" in response to a pen/trap order. (A fuller quotation of the language appears, above, in Section I.B.). By its very terms, this prohibition applies only to information collected by a provider and not to information collected directly by law enforcement authorities. Thus, CALEA does not bar the use of pen/trap orders to authorize the use of cell phone tracking devices used to locate targeted cell phones.

D. Conclusion

The amended text of the pen/trap statute and the limited legislative history accompanying the 2001 amendments strongly suggest that the non-content information that passes between a cellular phone and the provider's tower falls into the definition of "dialing, routing, addressing, and signaling information" for purposes of the definitions of "pen register" and "trap and trace device." A pen/trap authorization is therefore the safest method of allowing law enforcement to collect such transmissions directly using its own devices.