

**21st Century Investigations
And Motions Practice**

*Just Because You're Paranoid
Doesn't Mean They Aren't Watching You*

**AFPD Amy Baggio
June 2011**

PowerPoint Slides

BIG BROTHER



IS WATCHING YOU

21st Century Investigations & Motions Practice

Just Because You're Paranoid Doesn't Mean They Aren't Watching You

AFPD Amy Baggio
June 2011

Today's Discussion

- Modern Methods Used By Law Enforcement For Evidence Gathering
 - Administrative Subpoenas
 - Pen Registers/Trap & Trace Devices
 - Cell Phone Data
 - Pole Cameras
 - GPS Vehicle Trackers'
 - Computer Monitoring (Internet; email)
 - Wiretaps

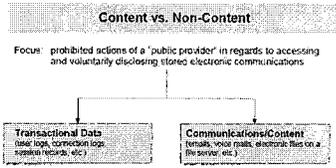
Today's Discussion

- What Showing The Government Must Make To Gather This Info
- Challenges To Law Enforcement Practices And The Evidence

Stored Communications Act

Content vs. Non-Content

Focus: prohibited actions of a "public provider" in regards to accessing and voluntarily disclosing stored electronic communications



© 2011 CANADIAN PUBLIC UNIVERSITY MODULE 1: EDPF 134

Stored Communications Act

- What is it?
- What does it cover?
- What are the standards?
 - See Kerr, *A User's Guide To The Stored Communications Act And A Legislator's Guide To Amending It*, 72 Geo. Wash. L. Rev. 1208 (August 2004) (included in materials)

Administrative Subpoenas

Administrative Subpoenas

- What are they?
- Requests for production of information, documents, etc. issued by an investigating agency.

Administrative Subpoenas

- DO NOT EQUAL
 - Grand Jury Subpoenas
 - Trial Subpoenas (i.e., FRCP 16, 41)



Administrative Subpoenas: Types

- **Agency Subpoenas**– Investigators empowered by statute to use subpoenas to investigate certain types of offenses
 - 21 USC § 876 – DEA can issue if specific & articulable facts make relevant to drug investigation

Administrative Subpoenas: Types

- **Data-Type Subpoenas**– Business required to keep certain records and make available to investigators
- 18 USC § 2709 (part of SCA)– communications providers must maintain certain records which are subject to subpoena
 - 335 separate authorizations for Executive Branch officials



Administrative Subpoenas

- What Court Involvement Is There?
- NONE!
- Exception: Motion To Quash
 - *Peters v. U.S.*, 853 F.2d 692 (9th Cir. 1988)



Administrative Subpoenas

- On Whom Are They Served?
 - Usually third parties/businesses with less interest in contesting subpoena validity
- Can The Third Party Disclose To Its Customer The Fact Of The Subpoena?
 - Usually not in criminal investigations

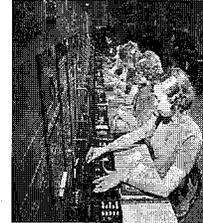


Administrative Subpoenas

- What Information Do Agents Learn?
 - Phone Records
 - Employment Records
 - Bank Records
 - Internet Records

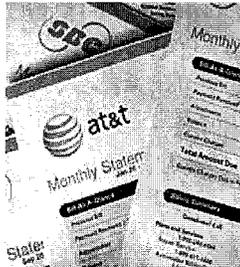
Administrative Subpoenas

- **Training Focus:**
**Phone Records and
Administrative
Subpoenas**



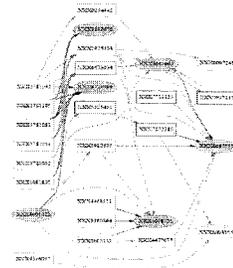
Administrative Subpoenas: Phone Records Focus

- What information is contained in your phone records?
 - Subscriber / Billing Information
 - Incoming / Outgoing Calls
 - CSLI



Common Call Analysis

- Government collects and compares all numbers dialed to create associations and to link to particular events

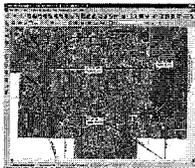


Cell Site Location Information (CSLI)

■ **Must Read:** MJ Smith (SD TX) testimony to Congress (included in materials) <http://judiciary.house.gov/hearings/pdf/Smith100624.pdf>

■ 3rd Circuit—Only circuit decision re: CSLI, 620 F.3d 304 (3d Cir. 2010)

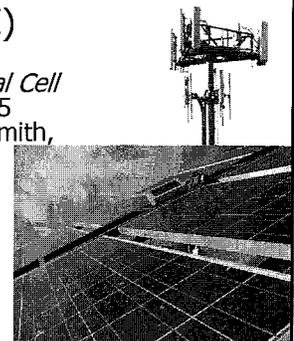
–Issued not per admin subpoena, but court order on less than PC under SCA (18 USC 2703(d))



Cell Site Location Information (CSLI)

■ **Must Read:** *In re application for Historical Cell Data*, 2010 WL 4286365 (S.D.Tex. 10/29/10) (Smith, J.)

–Discussion of evolving CSLI technology



Administrative Subpoenas

- How to Analyze:
 - What information are they getting?
 - Argue 4th implicated:
 - Location information implicates privacy
 - Records info implicates privacy interest (such as info beyond what one would expect in bill)
 - Does examination of compiled info to create associations or impute involvement based on calls at time/place cross line of mere recordkeeping into content?

Administrative Subpoenas

- Collective findings obtained from administrative subpoenas often used in application for Pen Registers / Trap & Trace Orders, among other things

Pen Registers and Trap & Trace Devices

Pen Registers / Trap & Trace

- What do they do?
 - Pens – Real time disclosure of numbers dialed out to a phone

 - Trap & Trace – Real time disclosure of numbers calling in to a phone

Pen Registers / Trap & Trace

- “Given a pen register’s limited capabilities... [the] argument that its installation and use constituted a ‘search’ necessarily rests upon a claim that he had a ‘legitimate expectation of privacy’ regarding the numbers he dialed on his phone. This claim must be rejected.”



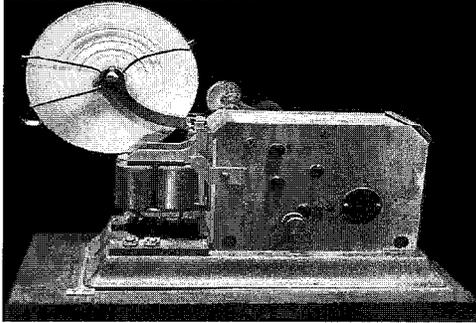
- *Smith v. Maryland*, 442 U.S. 735 (1979)

Pen Registers / Trap & Trace

- *Smith* reasoning, 1979 –
 - “a law enforcement official could not even determine from the use of a pen register whether a communication existed.”
 - “disclose only the telephone numbers that have been dialed...”
 - do NOT disclose any communication “nor whether the call was even completed”

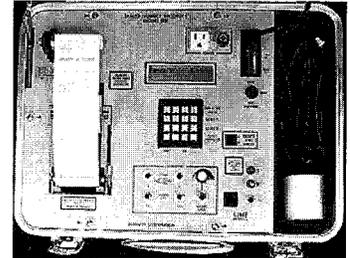


1850s Pen Register



20th Century Pen Register

- Evolution of technology = Increase in data conveyed by Pen



21st Century Pen Register

- Modern-day Pens disclose:
 - Numbers in/out
 - "Cut Through" Numbers
 - Duration
 - Whether call connected
 - If went to voicemail
 - If oral or text
 - CSLI
- Is this content?



Pen Registers / Trap & Trace

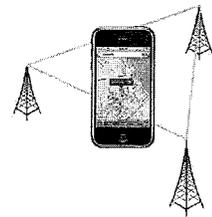
- How Does Law Enforcement Get This Information?
 - Pen / T&T Court Order
 - Standard - Offer Proof That The Information Is Relevant To An Ongoing Criminal Investigation
 - Less than probable cause (per *Smith*, no PC necessary)

Pen Registers / Trap & Trace

- | | |
|--|---|
| <ul style="list-style-type: none"> ■ 20th Century Pens in <i>Smith</i>: <ul style="list-style-type: none"> - Number Dialed Out | <ul style="list-style-type: none"> ■ 21st Century Data Collected: <ul style="list-style-type: none"> - Number Dialed Out/In - Cut Through Numbers - Whether Call Is Completed - Whether Call Went To Voicemail - Whether Call Was Voice Or Text Communication |
|--|---|

Pen Registers / Trap & Trace

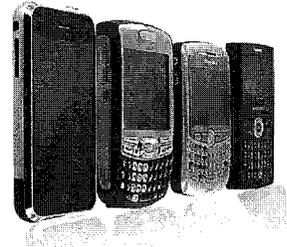
- Plus... 21st Century Data Collected:
 - Location Of Cell Tower
 - At Call Inception
 - At Call Completion
 - See *US v. Maynard*, 615 F.3d 544 (D.C. Cir 2010) (GPS case)
 - MJ Smith decision, 10/29/10 (historical CSLI)



Pen Registers / Trap & Trace

- How to Analyze:
 - What information are they getting?
 - Argue the information involves a search or an expectation of privacy, such as:
 - “Cut Through” numbers reveal content
 - Location information implicates privacy

Cell Phone / SmartPhone Data



Phone Data

- Estimated 277,000,000 cellular phones being used in US
- Eight primary service providers:
 - ATT, Verizon, Cingular, CellularOne, Nextel, T-Mobile, Sprint, and USCellular
- Plus, many more specialty and pre-paid service carriers (such as Cricket & GoATT)

Phone Data

- GPS precision locators activated and tracked remotely



– Did they get a warrant?

– 18 USC 3117(b) – “precision tracking device” requires PC & court order

Phone Data

- GPS precision locators activated and tracked remotely



- Gov’t makes real time versus historical distinction
- Gov’t then seeks without warrant under 18 USC 2703 as service record
- Newsweek, *The Snitch In Your Pocket* (2/19/10), “thousands of requests per month”

Phone Data

- Instant Messaging Service
 - What is this?
 - How do they get this info?

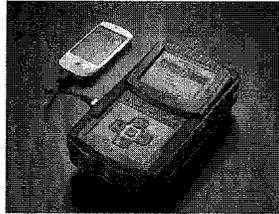


- Search warrant?

- Should this require a Wiretap?

Instant Access?

- UFED – Michigan police utilize in traffic stops since 2008
- Works on 3000 different phones, extracts data in 90 seconds



cellebrite
mobile data secured

"UNPARALLELED ACCESS TO PHONE MEMORY"

UFED Physical Pro provides access to data inaccessible by logical methods:

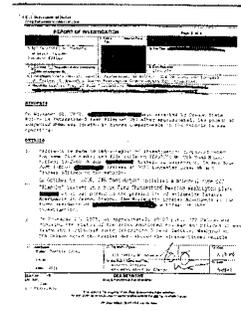
- Phone user lock code
- Deleted data including: deleted call history, text messages, images, phonebook entries and videos
- Access to internal application data
- Phone internal data including: IMSI history, past SIM cards used, past user lock code history



cellebrite
mobile data secured

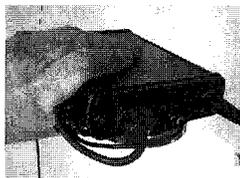
GPS Vehicle Trackers

GPS Vehicle Trackers



GPS Vehicle Trackers

- "Slap On" GPS Vehicle Trackers
 - Real Time?
 - Does It Matter?



GPS Vehicle Trackers

- Request discovery:
 - Make
 - Model
 - Instructional Information



GPS Vehicle Trackers

- "newer devices are placed in the engine compartment and hardwired to the car's battery so they don't run out of juice."

<http://www.wired.com/threatlevel/2010/10/fbi-tracking-device/#ixzz13ygw5yNI>

- Seizure?



GPS Vehicle Trackers

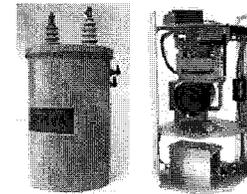
- Circuit Split – So Raise & Preserve!
 - 7th-9th Circuits: No warrant required
 - *US v. Pinedo-Moreno*, 591 F.3d 1212 (9th Cir. 2010)(installed on private property)
 - See also *Kozinski dissent, denial from rehearing*
 - *US v Marquez*, 605 F.3d 604 (8th Cir 2010)(citing *Knotts*)
 - *US v Cuevas-Perez*, 2011 WL 1585072 (7th Cir. Apr. 28, 2011)(surveillance limited 60 hours, one trip)
 - D.C. Circuit: Warrant required because 24 hour per day monitoring of location invades privacy
 - *US v. Maynard*, 615 F.3d 544 (D.C.Cir. 2010)

Pole Cameras

Pole Camera

- What are they?

Devices installed on utility poles, using either constant video or still photography



Pole Cameras

- What court authorization is needed?
- NONE! *US v. McIver*, 186 F.3d 1119 (9th Cir. 1999)
- Exception: when camera is pointed at place where have reasonable expectation of privacy, like inside motel room. *US v. Nerber*, 222 F.3d 597(9th Cir. 2000) but see *US v. Larios*, 593 F.3d 82 (1st Cir. 2010) (defendant had no reasonable expectation of privacy based on fleeting time in agent's hotel room)

Mobile Police Cameras

- "License Plate Reader"
- Currently employed in New York



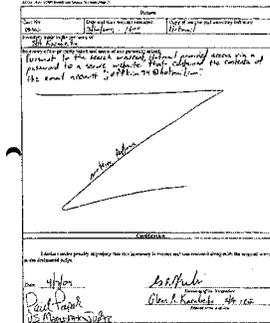
Computers

E-MAIL

- Is it like a letter, or like a phone number dialed out?
- Fourth Amendment?

E-MAIL

- Stored Communications Act – 18 U.S.C. § 2703
 - Less than 180 days old = PC warrant needed; courts split on whether notice is required to subscriber
 - More than 180 days old = subpoena or court order needed; notice required but can be delayed



E-MAIL

“Much of the reluctance to apply traditional notions of third party disclosure to the e-mail context seems to stem from a fundamental misunderstanding of the lack of privacy we all have in our e-mails. Some people seem to think that they are as private as letters, phone calls, or journal entries. The blunt fact is, they are not.”



– *In re Application of US for a Search Warrant*, 665 F.Supp.2d 1210, 1224 (D. Or. 2009).

E-MAIL

Compare In re Application of US for a Search Warrant, 665 F.Supp.2d 1210, 1224 (D. Or. 2009) with *United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008):

“The privacy interests in [mail and email] are identical.”

Sixth Circuit - E-MAIL

- *US v. Warshak*, 631 F.3d 266, 285-86 (6th Cir. 2010) – “Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection.”
- *City of Ontario v. Quon*, 130 S.Ct. 2619 (2010) as “implying that ‘a search of an individual’s personal e-mail account’ would be just as intrusive as ‘a wiretap on his home phone line.’”



E-MAIL

- *Warshak*, continued –
 - Officers entitled to good faith exception for relying on SCA
 - Law enforcement now on notice: can’t rely on SCA post Warshak
 - “Of course, after today’s decision, the good-faith calculus has changed, and a reasonable officer may no longer assume that the Constitution permits warrantless searches of private emails.” 631 F.3d at 289 n.17.

Computer Surveillance

■ Computer and Internet Protocol Address Verifier (CIPAV)

- IP address,
- MAC address,
- open ports,
- running programs,
- operating system
- web browser, and
- last visited URL

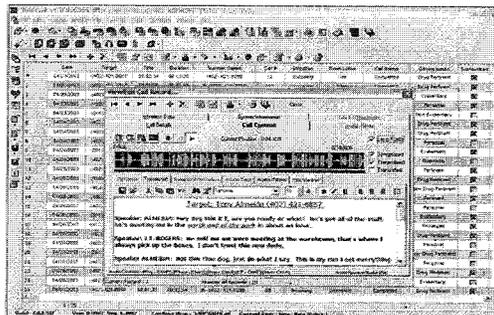


Wiretaps

The Road To A Wiretap

- Admin Subpoenas – association and event involvement by phone, banking records
 - No PC, no court order
- Trash Pulls - creepy
 - No PC, no court order
- Vehicle GPS – at place & time of relevance
 - No PC, no order
- Physical Surveillance / Informants
 - No PC, no order
- Pen Register/Trap & Trace – additional proof of associations and location
 - No PC, court orders if info “relevant”
- Search Warrants – for phone information, such as location, text messages, photos, etc.
 - PC, court orders

21st Century Wire Tap



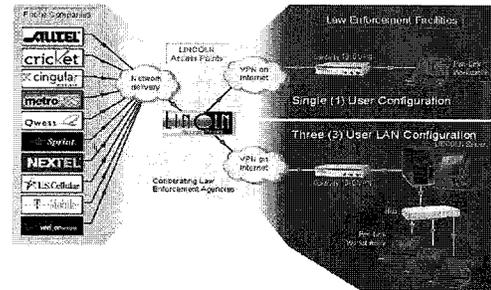
Wire Taps

- Info provided by wiretaps varies by service provider after service of court order



- Packets of information normalized using software which allows analysis, location plotting, etc.

Sample Data Normalization



Wire Taps

- Federal law provides for sealing, often on equivalent of permanent basis, such that user never knows his phone was tapped
- Civil litigation: "Hand Off Procedure"

Wiretaps

- Federal Wiretaps – Watch for technical compliance because statutory remedy for technical failure is suppression
- Different From Warrants – Government Needs To Prove:
 - Probable Cause **PLUS**
 - Necessity – "Full and complete statement" of investigation –
 - *This should include disclosure of informants but often does not*

Putting Concepts Into Practice

How To Analyze

- Paragraph by paragraph analysis of wiretap application / search warrant application / etc.
- Aggressive discovery demands
- Piece together what evidence they have, how they got it, and formulate suppression motion by articulating information as covered by a reasonable expectation of privacy

How To Litigate

- Distinguish bad prior law by changes in technology
- Go back to basic Fourth Amendment concepts in articulating position
- Don't be intimidated by overwhelming amounts of discovery or by new technology
- Ask for help

BIG BROTHER

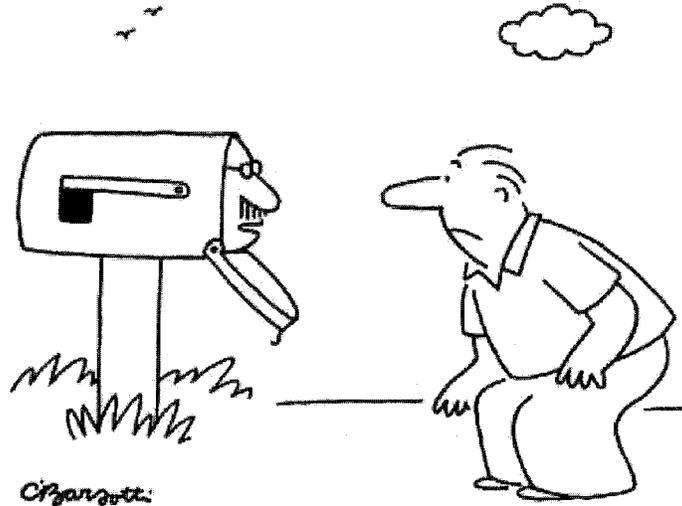


21st Century
Investigations &
Motions Practice

Just Because
You're Paranoid
Doesn't Mean
They Aren't
Watching You

Written Materials

**21st Century Investigations & Motions Practice
Written Materials**



"It's O.K., I'm with the government."

Charles Barsotti (8/13/1990)

Return to N

“There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time.”

George Orwell, *NINETEEN EIGHTY-FOUR* (1949).

“Every man should know that his conversations, his correspondence, and his personal life are private.”

Lyndon Johnson, Remarks (March 10, 1967).

“Some day soon, we may wake up and find we’re living in Oceania.”

United States v. Pineda-Morena, 617 F.3d 1120 (9th Cir. Aug.12, 2010)
(Kozinski, J., dissenting from denial of rehearing en banc)

Examples Of Modern Day Surveillance Tools

- Wiretaps – real-time monitoring of telephone communications or bugging of locations (*compare*: body wire)
- “Slap On” GPS trackers – small device attached to vehicle to provide location info
- Precision locators– remote activation and monitoring of GPS location of a particular cell phone
- Pen Registers – Originally, device that provides real time disclosure of numbers dialed out on a monitored telephone; now more information sought and provided
- Trap and Trace Devices – Identical to Pen Register, but discloses numbers calling in to a monitored telephone
- CIPAV – “Computer internet protocol address verifier”, FBI spyware that infiltrates a person’s computer, gathers IP address, MAC address, open ports, last visited URL, and more, and sends this information to the FBI server in eastern Virginia. After initial transfer of data, CIPAV then continues to monitor user’s internet use, including logging of IP address with which every other computer user connects
- Pole Cameras – Stationary cameras installed on utility poles outside a residence and recording either by video or fixed number of still images per minute
- Reverse Peephole Viewer – Also called a “door scope”, this is a small device which when held to peephole of door exterior will provide enlarged view of interior of room
- Administrative Subpoena – This simple tool provides a wealth of information. Subpoenas on phone companies result in disclosure of data about who you call, when you call them, whether you spoke or left a message, and more. Subpoenas on internet service providers disclose who pays the bill and can prove when a file was downloaded to a particular computer. Agents use subpoenas for bank records, online purchases, anything. No court involvement, and one may never know the subpoena was ever served – only the issuing agent and the third party receiving it. That’s power.

Why This Is So Important

The government’s sophistication in gathering evidence about its citizenry grows by the day. Many of the statutes supposedly authorizing information-gathering are antiquated – some over fifty-years old – and were not intended for the use currently employed by our government. Case law is similarly behind the times, allowing us the opportunity to distinguish previous holdings based on more limited technologies.

In defending the rights of our clients, and in turn the rights of every person, we are obligated to stay abreast of the government’s investigative methods and to master the supposed statutory authorizations on which law enforcement rely. Only through mastery of these complicated areas of the law can we challenge the use of ever-more-invasive technologies increasingly reminiscent of life in a police state.

Primary Electronic Surveillance Laws

Statutory authorizations for electronic surveillance and information collection are complicated and often strewn among a number of chapters within the code. Below are *some* of the primary statutes on which law enforcement rely:

A. *Electronic Communications Privacy Act* – (ECPA) Pub. L. 99-508, Oct. 21, 1986, 100 Stat. 1848, 18 U.S.C. § 2510, et. seq. The ECPA is codified in different provisions of the US Code. Due to its complexity, this statute is best considered in reference to its three Titles, their application, and scope:

	Application	Scope
Title I–Wiretap Act	interception of communications <i>in transmission</i>	Almost exclusively traditional phone and cell phone conversations, plus covers “bugging,” or installation of stationary listening devices

	(real time)	Limited protection for e-mail users due to narrow definition of “interception”
Title II–Stored Communications Act: 18 USC 2703 (a) =contents in storage (b)=contents held remotely (c)=records	accessing of <i>stored</i> electronic communications and subscriber records (non real-time)	Both cell phone telephone companies and email service providers. Applies to communications in “electronic storage” or “remote computing storage” by “electronic communications service (ECS).” According to legislative history, ECS=telephone companies AND electronic mail companies.
Title III–Pen Register Act	Pen registers/trap & race which record phone numbers or addressing (real time) information	USA Patriot Act expands to include “all dialing, routing, addressing, or signaling information.” Includes email addressing and phone information.

B. *Wire and Electronic Communications Interception and Interception of Oral Communications Act, 18 USC 2510-2520, formerly known as Title III Wiretap Act* – Government must establish PC that crime is, or is about to be, committed **and** that wiretap is necessary because traditional law enforcement techniques are not likely to be successful or are too dangerous.

C. *Foreign Intelligence Surveillance Act (FISA), 50 USC 1801 et seq.* – Using secret FISA Court applications and process, government can physically and electronically surveil person who is “foreign power” or “agent of a foreign power” or a “lone wolf” (individual engaging in or preparing for act of terrorism). Surveillance includes physical searches of residences or other locations, real time monitoring of phones or internet use. To obtain ex parte FISA order, government must establish PC that person is engaged in conduct that “may be” criminal if target is present in US lawfully, but if person is illegal alien, no showing of criminal activity is needed. Proceedings remain sealed.

Government may utilize surveillance even without a court order (Executive Branch decision alone) if (1) the monitoring is a year or less; (2) the activity involves foreign intelligence information by foreign powers or their agents and (3) there is no substantial likelihood that surveillance will capture communications of US citizen.

D. *Communications Assistance for Law Enforcement Act (CALEA, which in 1994 amended 1986's ECPA), 47 USC 1001-1010 and 18 USC §2703 (amending SCA)* – requires companies that provide communications services (like phone or internet) to utilize a communications system that will allow government a basic level of access.

E. Other Federal Electronics Laws – This area of search and seizure jurisprudence is one of the fastest changing in our practice. The following chart is an attempt to break down the authorization required for specific types of government surveillance and information gathering. Because of the lack of precedent and the multiple possible interpretations, practitioners are strongly encouraged to engage in their own research. The categories in order are:

1. Tracking devices
2. Phones
3. Emails
4. Basic User / Subscriber Information
5. Pole Cameras
6. Instant Messaging
7. Administrative Subpoenas

Electronic Surveillance Chart¹

Electronic Surveillance Type	Authorization Required	Statutory Cite
1. Tracking Devices		
A. GPS precision locators—cell site data on cell phones (real time movement)	Warrant, maybe. Conflicting case law.	Meets definition of “tracking device” under 18 U.S.C. § 3117(b) and government cannot use pen/trap device to obtain cell site data though <i>it is</i> information that pen/trap can technically provide, just not real time. <i>See e.g., In the Matter of an Application of the United States</i> , 384 F.Supp. 2d 562, No. M 05-1093(JO)(E.D.N.Y. Aug. 25, 2005). This case was the first opinion on this topic—most subsequent courts seem to agree that the government must have probable cause to obtain cell site data. District courts split on issue though, rapidly developing area of law. Government handbook discusses split.
B. GPS precision locators—placed on vehicles	None	Circuits split, based on different 4th A. protections 8 th Cir: No warrant – <i>US v Marquez</i> , 605 F.3d 604 (8th Cir 2010) – No warrant required, citing <i>US v. Knotts</i> ,

¹Thanks to Federal Defender law clerk Caitlin Overland for her help in creating this chart in its original form in 2010.

Electronic Surveillance Type	Authorization Required	Statutory Cite
		<p>460 US 276 (1983) 9th Circuit says not a “search” – No reasonable expectation of privacy in underside of vehicle outside curtilage of home. Government can affix tracking device—not a search. <i>US v. Pineda-Moreno</i>, 591 F.3d 1212 (9th Cir. 2010), rehearing en banc denied, 2010 WL 3169573 (Kozinski, J., dissenting from denial of rehearing en banc) (“There is something creepy and un-American about such clandestine and underhanded behavior. To those of us who have lived under a totalitarian regime, there is an eerie feeling of deja-vu.”).</p> <p><i>And compare</i> D.C. Circuit: Warrant required for GPS vehicle tracker because 24 hour per day monitoring of location invades right to privacy. <i>US v. Maynard</i>, 615 F3d 544 (D.C.Cir. 2010)</p> <p>Most recent: <i>US v Cuevas-Perez</i>, 2011 WL 1585072 (7th Cir. Apr. 28, 2011)(distinguishes <i>Maynard</i> on grounds that vehicle surveillance limited to 60 hours and one trip)</p> <p>Lesson: PRESERVE YOUR ISSUE and argue under both 4th Amendment theories</p> <p><u>GPS vehicle trackers under 18 U.S.C. § 3117?</u> <i>In re Application for an Order Authorizing the Extension and Use of Pen Register Device, etc.</i>, 2007 WL 397129, No. 07-SW-034-GGH, (E.D.Cal. Feb. 1, 2007) (unpublished opinion), held:</p> <p>“The tracking device statute, 18 U.S.C. § 3117, does not specify the standard an applicant must meet to install a tracking device. The Supreme Court has acknowledged that the standard for installation of a tracking device is unresolved, and has reserved ruling on the issue until it is squarely presented by the facts of a case. <i>See United States v. Karo</i>, 468 U.S. 705, 718 n. 5 (1984). The amendment to Rule 41 does not</p>

Electronic Surveillance Type	Authorization Required	Statutory Cite
		<p>resolve this issue or hold that such warrants may issue only on a showing of probable cause. Instead, it simply provides that if probable cause is shown, the magistrate judge must issue the warrant. And the warrant is only needed if the device is installed (for example, in the trunk of the defendant's car) or monitored (for example, while the car is in the defendant's garage) in an area in which the person being monitored has a reasonable expectation of privacy.”</p>
<p>2. Phones</p>		
<p>A. Trap and trace cell phone information</p>	<p>Court order</p>	<p>18 U.S.C. § 3122 (application for order)</p> <p>18 U.S.C. § 3123 (procedure for issuance of order)</p> <p>18 U.S.C. § 3127 (applies to trap/trace for cell phones based on broad definition)</p> <p>Violations of pen register law do not fall under exclusionary rule. <i>United States v. Forrester</i>, 512 F.3d 500, 512 (9th Cir. 2008). Need to articulate as constitutional violation, not statutory violation.</p>
<p>B. Pen register phone information</p>	<p>Court order</p>	<p>18 U.S.C. § 3122 (application for order)</p> <p>18 U.S.C. § 3123 (procedure for issuance of order)</p> <p>No expectation of privacy in numbers dialed out. <i>Smith v. Maryland</i>, 442 U.S. 735 (1979).</p> <p><i>See also In re U.S. for Orders (1) Authorizing Use of Pen Registers and Trap and Trace Devices</i>, 515 F.Supp.2d 325, 338 (E.D.N.Y. 2007) (access to numbers dialed after number connects violates Fourth Amendment and distinguishing <i>Smith</i>: “The evolution</p>

Electronic Surveillance Type	Authorization Required	Statutory Cite
		of technology and the potential degree of intrusion changes the [<i>Smith</i>] analysis.”).
C. Wiretap recordings on various cell phones	Wiretap order	18 U.S.C. § 2510 et seq.
D. Text messages on phones not seized/not in government possession--phone number known by government	<p><i>Stored for less than 180 days:</i> Warrant</p> <p><i>Stored more than 180 days:</i> warrant or; admin subpoena with notice or; 2703(d) Court order</p>	<p>18 U.S.C. § 2703 (a)-(d)</p> <p>No exclusionary rule for violations of Stored Communications Act (SCA).</p> <p>But, the Ninth Circuit has seemingly extended stored communications to require Wiretap protections based on the <i>Theofel</i> opinion. Seems to have made SCA partially irrelevant.</p>
E. Data stored in phones seized during traffic stops--substantially contemporaneous search or; data recovery post arrest	<p>Search incident to arrest or;</p> <p>Warrant</p>	<p><i>United States v. Park</i>, No. CR 05-375 SI, 2007 WL 1521573 (N.D.Cal. May 23, 2007) (unpublished) (proposition that cell phones are analogous to “possessions within an arrestee’s” control that may be searched absent a warrant only if search is “substantially contemporaneous” to arrest. (<i>citing United States v. Chadwick</i>, 433 U.S. 1 (1977))).</p>
3. Emails		
A. Contemporaneous Email Interception		Narrow interpretation of “interception” means even contemporaneous interception typically only falls under Stored Communication Act, and doesn’t get afforded Wiretap protection.

Electronic Surveillance Type	Authorization Required	Statutory Cite
		<i>See e.g., United States v. Scarfo</i> , 180 F.Supp.2d 572, 581 (D.N.J. 2001) (holding that technique used by government in recording keystrokes on computer to decipher password did not violate Wiretap statute).
B.1 Sent Emails —Majority of Circuits		
i. Unopened email (in electronic storage less than 180 days)	Search Warrant	18 U.S.C. 2703(a)
ii. Unopened email (in electronic storage more than 180 days)	Subpoena with notice or; 2703(d) order with notice or; search warrant	18 U.S.C. 2703(a)-(b) <i>Compare US v. Warshak</i> , 631 F.3d 266 (6 th Cir. 2010) (expectation of privacy in email) <i>and In the Matter of Application of the USA for a Search Warrant for Contents of Electronic Mail...</i> , 665 F.Supp.2d 1210 (D. Or. 2009) (Mosman, J.) (no expectation of privacy in email).
iii. Opened emails, other content files being stored or processed	Subpoena with notice or; 2703(d) order with notice or; search warrant	18 U.S.C. 2703(a)-(b)
iv. Noncontent records	2703(d) order or; search warrant	18 U.S.C. 2703(c)(1)
v. Basic subscriber information, session logs, IP addresses	Subpoena; or 2703(d) order; or search warrant	18 U.S.C. 2703(c)(2)

Electronic Surveillance Type	Authorization Required	Statutory Cite
B.2 Sent Emails–9th Circuit <i>See Theofel v. Farey-Jones</i> , 359 F.3d 1066 (9th Cir. 2004)		
i. Unexpired emails stored for 180 days or less	Search warrant	18 U.S.C. 2703(a)
ii. Unexpired emails stored for more than 180 days	Subpoena with notice or 2703(d) order with notice or; search warrant	18 U.S.C. 2703(a)-(b)
iii. Files remotely stored or processed	Subpoena with notice or; 2703(d) order with notice or: search warrant	18 U.S.C. 2703(b)
iv. Noncontent records	2703(d) order or; search warrant	18 U.S.C. 2703(c)(1)
v. Basic subscriber information, session logs, IP addresses	Subpoena; or 2703(d) order; or search warrant	18 U.S.C. 2703(c)(2)
4. Basic User Information		
Telephone user/subscriber info	Administrative subpoena	
5. Pole Camera		
A. Pole camera external surveillance–generally	Nothing	<i>United States v. McIver</i> , 186 F.3d 1119 (9th Cir. 1999) citing <i>Katz v United States</i> (warrant not required if defendant did not have reasonable expectation of privacy in public area.)

Electronic Surveillance Type	Authorization Required	Statutory Cite
<p>B. Pole camera external surveillance – vicinity of residence</p>	<p><u>Circuit Split:</u> Nothing <i>or</i>; warrant</p>	<p><i>United States v. Vankesteren</i>, 553 F.3d 286 (4th Cir. 2009) (camera installed to record defendant’s open field does not implicate 4th)</p> <p><i>United States v. Jackson</i>, 213 F.3d 1269 (10th Cir. 2000) (No reasonable expectation of privacy because cameras were incapable of viewing inside house...any passerby could easily observe same thing).</p> <p><i>United States v. Cuevas-Sanchez</i>, 821 F.2d 248 (5th Cir. 1987) (video surveillance of home constituted search, warrant required).</p> <p>No 9th Circuit Opinion specifically on use of pole cameras near homes, but positive citations of <i>Cuevas-Sanchez</i>. See <i>United States v. Nerber</i>, 222 F.3d 597 (9th Cir. 2000) <i>but compare</i> <i>US v. Larios</i>, 593 F.3d 82 (1st Cir. 2010) (defendant failed to establish reasonable expectation of privacy based on fleeting time in agent’s hotel room)</p>
<p>6. Instant Messaging</p>		
<p>A. Standard Instant Messaging (no video, voice, etc, just text)– Contemporaneous interception</p>	<p>Wiretap order(?)</p>	<p>Ninth Circuit case analogizes IM chat to private call for purposes of consent by one party. <i>United States v. Meek</i>, 366 F.3d 705, 711 (9th Cir. 2004).</p> <p>“Nor should a private chat be subject to fewer protections than a phone call merely because the words are written.” Comment, Nicholas Matlatch, <i>Who Let the Katz Out? How the ECPA and SCA Fail to Apply to Modern Digital Communications and How Returning to the Principles of Katz v. United States Will Fix It</i>, 18 Comm Law Conspectus 421, 452-53 (2010) (discussing why private IM conversations should be afforded the same protections as private phone calls)</p>

Electronic Surveillance Type	Authorization Required	Statutory Cite
<p>B. Enhanced Instant Messaging (including voice, video, etc)– contemporaneous interception</p>	<p>Wiretap order (?)</p>	<p>Seems to depend on which component gets intercepted and when. Again, limited law on subject.</p> <p>See Comment, Nicholas Matlatch, <i>Who Let the Katz Out? How the ECPA and SCA Fail to Apply to Modern Digital Communications and How Returning to the Principles of Katz v. United States Will Fix It</i>, 18 Comm Law Conspectus 421, 453-54 (2010).</p>
<p>C. Instant Message Records</p>	<p>Presumably falls under Stored Communications Act–see circuit split discussion on emails.</p>	<p>See Comment, Nicholas Matlatch, <i>Who Let the Katz Out? How the ECPA and SCA Fail to Apply to Modern Digital Communications and How Returning to the Principles of Katz v. United States Will Fix It</i>, 18 Comm Law Conspectus 421 (2010).</p>
<p>7. Administrative Subpoenas</p>		
	<p>Agent Issued (no court review absent motion to quash)</p>	<p>Several sources in federal law, including:</p> <p>21 U.S.C. 876 (subpoenas issued during controlled substance investigations)</p> <p>– See <i>Hell's Angels Motorcycle Corp. v. McKinley</i>, 360 F.3d 930 (9th Cir. 2004) (Hell’s Angels lack expectation of privacy to challenge §876 subpoena for records previously seized pursuant to state search warrant); <i>United States v. Plunk</i>, 153 F.3d 1011, 1020 (9th Cir.1998), amended by, 161 F.3d 1195 (9th Cir.1998), abrogated on other grounds by, <i>United States v. Hankey</i>, 203 F.3d 1160, 1169 and n. 7 (9th Cir.2000) (defendant lacked standing to challenge 876 administrative subpoena served on third party phone company because no expectation of privacy in telephone records).</p> <p>Recipient of subpoena must move to quash: See <i>Peters v. U.S.</i>, 853 F.2d 692 (9th Cir. 1988) (successfully</p>

Electronic Surveillance Type	Authorization Required	Statutory Cite
		<p>quashing INS subpoena as beyond statutory authority); but rarely granted: <i>Amato v. US</i>, 450 F.3d 46 (1st Cir. 2006); <i>In re Admin Subpoena</i>, 289 F.3d 843 (6th Cir. 2001),</p> <p>18 U.S.C. 3486 (administrative subpoenas in certain health care fraud, child abuse, and Secret Service protection cases)</p> <p>5 U.S.C.App.(III) 6 (Inspector General investigations)</p> <p>Plus, authority for subpoenas involving certain “international terrorism” investigations: 18 U.S.C. 2709 (communications provider records); 12 U.S.C. 3414 (financial institution records); 50 U.S.C. 436 (same); 15 U.S.C. 1681v (credit agency records); 15 U.S.C. 1681u (same).</p>

The Sword And The Shield:

As noted in *Kyllo v. United States*, 553 U.S. 27, 34, 40 (2001), “police technology [can] erode the privacy guaranteed by the Fourth Amendment” and courts must “take the long view, from the original meaning of the Fourth Amendment forward.” The *Kyllo* decision is a gold mine in terms of powerful language about the advances of technology and the need to protect rights under the Fourth Amendment. *See also U.S. v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010) (reviewing Fourth Amendment law vis-a-vis improved government surveillance tactics, esp. GPS tracker, distinguishing *United States v. Knotts*, 460 U.S. 276 (1983) (use of a beeper device to aid in tracking a suspect to his drug lab not a search), and finding continuous GPS monitoring infringes on privacy interests). Judge Kozinski’s dissent from denial of rehearing en banc in *Pineda-Moreno* (bad 9th decision holding installation of GPS on vehicle not a “search”) provides a powerful articulation of the tension between Fourth Amendment protections and advances in government surveillance. 617 F.3d 1120. Because of the ever-evolving techniques used by law enforcement, our best shield may be a return to basic Fourth Amendment jurisprudence combined with a sword of distinguishing bad cases by delineating the differences in technology then, with technology employed now.

To adequately understand what the government did to obtain evidence in our clients’ cases, we can employ more detailed requests for discovery, review the documents carefully to

understand substantively what information was provided, and then raise an objection to obtaining that information in terms of a protected interest.

So:

1. Move for specific discovery of administrative subpoenas, physical and electronic surveillance done during course of investigation – and watch for pretext stops – which are sometimes based on other surreptitious investigations and evidence gathering law enforcement does not want to disclose;
2. Carefully review the statutory authority relied on by law enforcement for that particular means of evidence collection;
3. Have they gone beyond the statutory authority, even by a bit ,by virtue of advancing technologies or more aggressive use of existing technology or by laziness?;
4. Move to suppress the evidence! Or, if that evidence is used to establish probable cause for a warrant or to obtain a wiretap, move to suppress the resulting warrant or wiretap.
5. Remember: Not much case law out there, and the bad stuff is based on old notions of government technology and antiquated ideas of the types of information provided by third parties.

Sources and Resources

Dept. of Justice, Office of Legal Education, Exec. Office for United States Attorneys *Searching and Seizing Computers And Obtaining Electronic Evidence In Criminal Investigations*, (2009) available at <http://www.justice.gov/criminal/cybercrime/ssmanual/ssmanual2009.pdf> (complete statement of federal government policy and how-to manual for obtaining electronic evidence)

Daniel Solove, *Reconstructing Electronic Surveillance Law*, 72 Geo. Wash. L. Rev. 1264, 1279 (2004) (detailed discussion of evolution of federal surveillance law).

Michael Isikoff, *The Snitch In Your Pocket*, Newsweek, Mar. 1, 2010, available at <http://www.newsweek.com/id.233965> (upon government request, Sprint activated GPS in citizens' cell phones eight million times in 2009).

Electronic Frontier Foundation (www.eff.org) – nonprofit devoted to “defending your digital rights”; provides research materials and has acted as amicus in electronic evidence litigation. See particularly, Electronic Frontier Foundation, *Privacy: Stored Communications Act - Internet Law Treatise*, <http://ilt.eff.org/index.php/Privacy: Stored Communications Act> (discussion of SCA)

In re Timberlinebominfo MySpace account, FBI request for CIPAV warrant, available at http://www.wired.com/images_blogs/threatlevel/files/timberline_affidavit.pdf.

Congressional Research Service, *Administrative Subpoenas in Criminal Investigations: A Brief Legal Analysis* (March 2006) available at <http://www.fas.org/spp/crs/intel/RL33321.pdf> (lengthy discussion of types of administrative subpoenas and uses in criminal investigations).

National Conference of State Legislatures, *Electronic Surveillance Laws* (last updated April 2009) available at <http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/ElectronicSurveillanceLaws/tabid/13492/Default.aspx> (comprehensive state-by-state chart of surveillance statutes)

In re §2703(d) Order, 2011 WL 900120 (E.D.Va. Mar.11, 2011) (Buchanan, J.)

In the matter of the Application of the US for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 620 F.3d 304 (3d Cir. 2010).

Primary Electronic
Evidence Statutes
(including full text)

Individual Privacy: Challenges Grow as Technology Flourishes

Applicable Statutes

Table of Contents

Stored Wire and Electronic Communications Act.....	2
18 USC § 2701. Unlawful access to stored communications	2
18 USC § 2702. Voluntary disclosure of customer communications or records.....	3
18 USC § 2703. Required disclosure of customer communications or records.....	5
18 USC § 2704. Backup preservation	8
18 USC § 2705. Delayed notice	10
Pen Registers and Trap and Trace Devices	12
18 USC § 3121. General prohibition on pen register and trap and trace device use; exception.....	12
18 USC § 3122. Application for an order for a pen register or a trap and trace device.....	13
18 USC § 3123. Issuance of an order for a pen register or a trap and trace device	14
18 USC § 3124. Assistance in installation and use of a pen register or a trap and trace device	16
18 USC § 3125. Emergency pen register and trap and trace device installation	17
18 USC § 3126. Reports concerning pen registers and trap and trace devices	18
§ 3127. Definitions for chapter	19
Wire and Electronic Communications Interception and Interception of Oral Communications.....	20
18 USC § 2510. Definitions	20
18 USC § 2511. Interception and disclosure of wire, oral, or electronic communications prohibited ..	23
Prospective amendment:.....	27
18 USC § 2515. Prohibition of use as evidence of intercepted wire or oral communications.....	27
§ 2516. Authorization for interception of wire, oral, or electronic communications.....	28
18 USC § 2517. Authorization for disclosure and use of intercepted wire, oral, or electronic communications.....	32
18 USC § 2518. Procedure for interception of wire, oral, or electronic communications.....	34
18 USC § 2519. Reports concerning intercepted wire, oral, or electronic communications.....	39
All Writs Act.....	40
§ 1651. Writs	40
Rule 41 of the Federal Rules of Criminal Procedure	41
Search and Seizure	41
9th Circuit <i>en banc</i> CDT Opinion.	45

Stored Wire and Electronic Communications Act

18 USC § 2701. Unlawful access to stored communications

(a) Offense. Except as provided in subsection (c) of this section whoever--

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

(b) Punishment. The punishment for an offense under subsection (a) of this section is--

(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State--

(A) a fine under this title or imprisonment for not more than 5 years, or both, in the case of a first offense under this subparagraph; and

(B) a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph; and

(2) in any other case--

(A) a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section.

(c) Exceptions. Subsection (a) of this section does not apply with respect to conduct authorized--

(1) by the person or entity providing a wire or electronic communications service;

(2) by a user of that service with respect to a communication of or intended for that user; or

(3) in section 2703, 2704 or 2518 of this title [18 USCS § 2703, 2704, or 2518].

18 USC § 2702. Voluntary disclosure of customer communications or records

(a) Prohibitions. Except as provided in subsection (b) or (c)--

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service--

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

(b) Exceptions for disclosure of communications. A provider described in subsection (a) may divulge the contents of a communication--

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title [18 USCS § 2517, 2511(2)(a), or 2703];

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A [18 USCS § 2258A];

(7) to a law enforcement agency--

(A) if the contents--

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or

(B) [Deleted]

(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

(c) Exceptions for disclosure of customer records. A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))--

(1) as otherwise authorized in section 2703 [18 USCS § 2703];

- (2) with the lawful consent of the customer or subscriber;
- (3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;
- (4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency;
- (5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A [18 USCS § 2258A]; or
- (6) to any person other than a governmental entity.

(d) Reporting of emergency disclosures. On an annual basis, the Attorney General shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report containing--

- (1) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (b)(8); and
- (2) a summary of the basis for disclosure in those instances where--
 - (A) voluntary disclosures under subsection (b)(8) were made to the Department of Justice; and
 - (B) the investigation pertaining to those disclosures was closed without the filing of criminal charges.

18 USC § 2703. Required disclosure of customer communications or records

(a) Contents of wire or electronic communications in electronic storage. A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of wire or electronic communications in a remote computing service.

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection--

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity--

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title [18 USCS § 2705].

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service--

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) Records concerning electronic communication service or remote computing service.

(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity--

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure;

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section

2325 of this title [18 USCS § 2325]); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the--

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number), of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) Requirements for court order. A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) No cause of action against a provider disclosing information under this chapter. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter [18 USCS §§ 2701 et seq.].

(f) Requirement to preserve evidence.

(1) In general. A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention. Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

(g) Presence of officer not required. Notwithstanding section 3105 of this title [18 USCS § 3105], the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter [18 USCS §§ 2701 et seq.] requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

18 USC § 2704. Backup preservation

(a) Backup preservation.

(1) A governmental entity acting under section 2703(b)(2) [18 USCS § 2703(b)(2)] may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of such subpoena or court order, such service provider shall create such backup copy as soon as practicable consistent with its regular business practices and shall confirm to the governmental entity that such backup copy has been made. Such backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.

(2) Notice to the subscriber or customer shall be made by the governmental entity within three days after receipt of such confirmation, unless such notice is delayed pursuant to section 2705(a) [18 USCS § 2705(a)].

(3) The service provider shall not destroy such backup copy until the later of--

(A) the delivery of the information; or

(B) the resolution of any proceedings (including appeals of any proceeding) concerning the government's subpoena or court order.

(4) The service provider shall release such backup copy to the requesting governmental entity no sooner than fourteen days after the governmental entity's notice to the subscriber or customer if such service provider--

(A) has not received notice from the subscriber or customer that the subscriber or customer has challenged the governmental entity's request; and

(B) has not initiated proceedings to challenge the request of the governmental entity.

(5) A governmental entity may seek to require the creation of a backup copy under subsection (a)(1) of this section if in its sole discretion such entity determines that there is reason to believe that notification under section 2703 of this title [18 USCS § 2703] of the existence of the subpoena or court order may result in destruction of or tampering with evidence. This determination is not subject to challenge by the subscriber or customer or service provider.

(b) Customer challenges.

(1) Within fourteen days after notice by the governmental entity to the subscriber or customer under subsection (a)(2) of this section, such subscriber or customer may file a motion to quash such subpoena or vacate such court order, with copies served upon the governmental entity and with written notice of such challenge to the service provider. A motion to vacate a court order shall be filed in the court which issued such order. A motion to quash a subpoena shall be filed in the appropriate United States district court or State court. Such motion or application shall contain an affidavit or sworn statement--

(A) stating that the applicant is a customer or subscriber to the service from which the contents of electronic communications maintained for him have been sought; and

(B) stating the applicant's reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this chapter [18 USCS §§ 2701 et seq.] in some other respect.

(2) Service shall be made under this section upon a governmental entity by delivering or mailing by registered or certified mail a copy of the papers to the person, office, or department specified in the notice which the customer has received pursuant to this chapter [18 USCS §§ 2701 et seq.]. For the purposes of this section, the term "delivery" has the meaning given that term in the Federal Rules of Civil Procedure.

(3) If the court finds that the customer has complied with paragraphs (1) and (2) of this subsection, the court shall order the governmental entity to file a sworn response, which may be filed in camera if the governmental entity includes in its response the reasons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the parties' initial allegations and response, the court may conduct such additional proceedings as it deems appropriate. All such proceedings shall be completed and the motion or application decided as soon as practicable after the filing of the governmental entity's response.

(4) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the governmental entity are maintained, or that there is a reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order such process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not a reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the provisions of this chapter [18 USCS §§ 2701 et seq.], it shall order the process quashed.

(5) A court order denying a motion or application under this section shall not be deemed a final order and no interlocutory appeal may be taken therefrom by the customer.

18 USC § 2705. Delayed notice

(a) Delay of notification.

(1) A governmental entity acting under section 2703(b) of this title [18 USCS § 2703(b)] may--

(A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title [18 USCS § 2703(b)] for a period not to exceed ninety days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or

(B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title [18 USCS § 2703(b)] for a period not to exceed ninety days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.

(2) An adverse result for the purposes of paragraph (1) of this subsection is--

(A) endangering the life or physical safety of an individual;

(B) flight from prosecution;

(C) destruction of or tampering with evidence;

(D) intimidation of potential witnesses; or

(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(3) The governmental entity shall maintain a true copy of certification under paragraph (1)(B).

(4) Extensions of the delay of notification provided in section 2703 [18 USCS § 2703] of up to ninety days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) of this section.

(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first-class mail to, the customer or subscriber a copy of the process or request together with notice that--

(A) states with reasonable specificity the nature of the law enforcement inquiry; and

(B) informs such customer or subscriber--

(i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;

(ii) that notification of such customer or subscriber was delayed;

(iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and

(iv) which provision of this chapter [18 USCS §§ 2701 et seq.] allowed such delay.

(6) As used in this subsection, the term "supervisory official" means the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney's headquarters or regional office.

(b) Preclusion of notice to subject of governmental access. A governmental entity acting under section 2703 [18 USCS § 2703], when it is not required to notify the subscriber or customer under section 2703(b)(1) [18 USCS § 2703(b)(1)], or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is

directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in--

- (1) endangering the life or physical safety of an individual;
- (2) flight from prosecution;
- (3) destruction of or tampering with evidence;
- (4) intimidation of potential witnesses; or
- (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

Pen Registers and Trap and Trace Devices

18 USC § 3121. General prohibition on pen register and trap and trace device use; exception

(a) In general. Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title [18 USCS § 3123] or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

(b) Exception. The prohibition of subsection (a) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service--

(1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or

(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or

(3) where the consent of the user of that service has been obtained.

(c) Limitation. A government agency authorized to install and use a pen register or trap and trace device under this chapter [18 USCS §§ 3121 et seq.] or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications.

(d) Penalty. Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both.

18 USC § 3122. Application for an order for a pen register or a trap and trace device

(a) Application.

(1) An attorney for the Government may make application for an order or an extension of an order under section 3123 of this title [18 USCS § 3123] authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter [18 USCS §§ 3121 et seq.], in writing under oath or equivalent affirmation, to a court of competent jurisdiction.

(2) Unless prohibited by State law, a State investigative or law enforcement officer may make application for an order or an extension of an order under section 3123 of this title [18 USCS § 3123] authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter [18 USCS §§ 3121 et seq.], in writing under oath or equivalent affirmation, to a court of competent jurisdiction of such State.

(b) Contents of application. An application under subsection (a) of this section shall include--

(1) the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and

(2) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

18 USC § 3123. Issuance of an order for a pen register or a trap and trace device

(a) In general.

(1) Attorney for the Government. Upon an application made under section 3122(a)(1) [18 USCS § 3122(a)(1)], the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. The order, upon service of that order, shall apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order. Whenever such an order is served on any person or entity not specifically named in the order, upon request of such person or entity, the attorney for the Government or law enforcement or investigative officer that is serving the order shall provide written or electronic certification that the order applies to the person or entity being served.

(2) State investigative or law enforcement officer. Upon an application made under section 3122(a)(2) [18 USCS § 3122(a)(2)], the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court, if the court finds that the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

(3) (A) Where the law enforcement agency implementing an ex parte order under this subsection seeks to do so by installing and using its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public, the agency shall ensure that a record will be maintained which will identify--

(i) any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network;

(ii) the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information;

(iii) the configuration of the device at the time of its installation and any subsequent modification thereof; and

(iv) any information which has been collected by the device.

To the extent that the pen register or trap and trace device can be set automatically to record this information electronically, the record shall be maintained electronically throughout the installation and use of such device.

(B) The record maintained under subparagraph (A) shall be provided ex parte and under seal to the court which entered the ex parte order authorizing the installation and use of the device within 30 days after termination of the order (including any extensions thereof).

(b) Contents of order. An order issued under this section--

(1) shall specify--

(A) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;

(B) the identity, if known, of the person who is the subject of the criminal investigation;

(C) the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of an order authorizing installation and use of a trap and trace device under subsection (a)(2), the geographic limits of the order; and

(D) a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates; and

(2) shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device under section 3124 of this title [18 USCS § 3124].

(c) Time period and extensions.

(1) An order issued under this section shall authorize the installation and use of a pen register or a trap and trace device for a period not to exceed sixty days.

(2) Extensions of such an order may be granted, but only upon an application for an order under section 3122 of this title [18 USCS § 3122] and upon the judicial finding required by subsection (a) of this section. The period of extension shall be for a period not to exceed sixty days.

(d) Nondisclosure of existence of pen register or a trap and trace device. An order authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that--

(1) the order be sealed until otherwise ordered by the court; and

(2) the person owning or leasing the line or other facility to which the pen register or a trap and trace device is attached, or applied, or who is obligated by the order to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

18 USC § 3124. Assistance in installation and use of a pen register or a trap and trace device

(a) Pen registers. Upon the request of an attorney for the government or an officer of a law enforcement agency authorized to install and use a pen register under this chapter [18 USCS §§ 3121 et seq.], a provider of wire or electronic communication service, landlord, custodian, or other person shall furnish such investigative or law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such assistance is directed by a court order as provided in section 3123(b)(2) of this title [18 USCS § 3123(b)(2)].

(b) Trap and trace device. Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to receive the results of a trap and trace device under this chapter [18 USCS §§ 3121 et seq.], a provider of a wire or electronic communication service, landlord, custodian, or other person shall install such device forthwith on the appropriate line or other facility and shall furnish such investigative or law enforcement officer all additional information, facilities and technical assistance including installation and operation of the device unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such installation and assistance is directed by a court order as provided in section 3123(b)(2) of this title [18 USCS § 3123(b)(2)]. Unless otherwise ordered by the court, the results of the trap and trace device shall be furnished, pursuant to section 3123(b) or section 3125 of this title [18 USCS § 3123(b) or 3125], to the officer of a law enforcement agency, designated in the court order, at reasonable intervals during regular business hours for the duration of the order.

(c) Compensation. A provider of a wire or electronic communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

(d) No cause of action against a provider disclosing information under this chapter. No cause of action shall lie in any court against any provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with a court order under this chapter [18 USCS §§ 3121 et seq.] or request pursuant to section 3125 of this title [18 USCS § 3125].

(e) Defense. A good faith reliance on a court order under this chapter [18 USCS §§ 3121 et seq.], a request pursuant to section 3125 of this title [18 USCS § 3125], a legislative authorization, or a statutory authorization is a complete defense against any civil or criminal action brought under this chapter [18 USCS §§ 3121 et seq.] or any other law.

(f) Communications assistance enforcement orders. Pursuant to section 2522 [18 USCS § 2522], an order may be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act [47 USCS §§ 1001 et seq.].

18 USC § 3125. Emergency pen register and trap and trace device installation

(a) Notwithstanding any other provision of this chapter [18 USCS §§ 3121 et seq.], any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that--

(1) an emergency situation exists that involves--

(A) immediate danger of death or serious bodily injury to any person;

(B) conspiratorial activities characteristic of organized crime;

(C) an immediate threat to a national security interest; or

(D) an ongoing attack on a protected computer (as defined in section 1030 [18 USCS § 1030]) that constitutes a crime punishable by a term of imprisonment greater than one year;

that requires the installation and use of a pen register or a trap and trace device before an order authorizing such installation and use can, with due diligence, be obtained, and

(2) there are grounds upon which an order could be entered under this chapter [18 USCS §§ 3121 et seq.] to authorize such installation and use;

may have installed and use a pen register or trap and trace device if, within forty-eight hours after the installation has occurred, or begins to occur, an order approving the installation or use is issued in accordance with section 3123 of this title [18 USCS § 3123].

(b) In the absence of an authorizing order, such use shall immediately terminate when the information sought is obtained, when the application for the order is denied or when forty-eight hours have lapsed since the installation of the pen register or trap and trace device, whichever is earlier.

(c) The knowing installation or use by any investigative or law enforcement officer of a pen register or trap and trace device pursuant to subsection (a) without application for the authorizing order within forty-eight hours of the installation shall constitute a violation of this chapter [18 USCS §§ 3121 et seq.].

(d) A provider of a wire or electronic service, landlord, custodian, or other person who furnished facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

18 USC § 3126. Reports concerning pen registers and trap and trace devices

The Attorney General shall annually report to Congress on the number of pen register orders and orders for trap and trace devices applied for by law enforcement agencies of the Department of Justice, which report shall include information concerning--

- (1) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;
- (2) the offense specified in the order or application, or extension of an order;
- (3) the number of investigations involved;
- (4) the number and nature of the facilities affected; and
- (5) the identity, including district, of the applying investigative or law enforcement agency making the application and the person authorizing the order.

§ 3127. Definitions for chapter

As used in this chapter [18 USCS §§ 3121 et seq.]--

(1) the terms "wire communication", "electronic communication", "electronic communication service", and "contents" have the meanings set forth for such terms in section 2510 of this title [18 USCS § 2510];

(2) the term "court of competent jurisdiction" means--

(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that--

(i) has jurisdiction over the offense being investigated;

(ii) is in or for a district in which the provider of a wire or electronic communication service is located;

(iii) is in or for a district in which a landlord, custodian, or other person subject to subsections [subsection] (a) or (b) of section 3124 of this title [18 USCS § 3124] is located; or

(iv) is acting on a request for foreign assistance pursuant to section 3512 of this title [18 USCS § 3512]; or

(B) a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device;

(3) the term "pen register" means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business;

(4) the term "trap and trace device" means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication;

(5) the term "attorney for the Government" has the meaning given such term for the purposes of the Federal Rules of Criminal Procedure; and

(6) the term "State" means a State, the District of Columbia, Puerto Rico, and any other possession or territory of the United States.

Wire and Electronic Communications Interception and Interception of Oral Communications

18 USC § 2510. Definitions

As used in this chapter [18 USCS §§ 2510 et seq.]--

(1) "wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce;

(2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication;

(3) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States;

(4) "intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.[];

(5) "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than--

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

(b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal;

(6) "person" means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation;

(7) "Investigative or law enforcement officer" means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter [18 USCS §§ 2510 et seq.], and any attorney authorized by law to prosecute or participate in the prosecution of such offenses;

(8) "contents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;

(9) "Judge of competent jurisdiction" means--

(a) a judge of a United States district court or a United States court of appeals; and

(b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire, oral, or electronic communications;

(10) "communication common carrier" has the meaning given that term in section 3 of the Communications Act of 1934 [47 USCS § 153];

(11) "aggrieved person" means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed;

(12) "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include--

- (A) any wire or oral communication;
 - (B) any communication made through a tone-only paging device;
 - (C) any communication from a tracking device (as defined in section 3117 of this title [18 USCS § 3117]); or
 - (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;
- (13) "user" means any person or entity who--
- (A) uses an electronic communication service; and
 - (B) is duly authorized by the provider of such service to engage in such use;
- (14) "electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;
- (15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;
- (16) "readily accessible to the general public" means, with respect to a radio communication, that such communication is not--
- (A) scrambled or encrypted;
 - (B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;
 - (C) carried on a subcarrier or other signal subsidiary to a radio transmission;
 - (D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or
 - (E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;
- (17) "electronic storage" means--
- (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
 - (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication;
- (18) "aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception;
- (19) "foreign intelligence information", for purposes of section 2517(6) of this title [18 USCS § 2517(6)], means--
- (A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against--
 - (i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
 - (ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
 - (iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
 - (B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to--
 - (i) the national defense or the security of the United States; or
 - (ii) the conduct of the foreign affairs of the United States;
- (20) "protected computer" has the meaning set forth in section 1030 [18 USCS § 1030]; and

(21) "computer trespasser"--

(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and

(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.

18 USC § 2511. Interception and disclosure of wire, oral, or electronic communications prohibited [Caution: See prospective amendment note below.]

(1) Except as otherwise specifically provided in this chapter [18 USCS §§ 2510 et seq.] any person who--

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when--

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or

(e) (i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b)-(c), 2511(2)(e), 2516, and 2518 of this chapter [18 USCS §§ 2511(2)(a)(ii), 2511(2)(b)-(c), 2511(2)(e), 2516, and 2518], (ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, (iii) having obtained or received the information in connection with a criminal investigation, and (iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation, shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2)

(a) (i) It shall not be unlawful under this chapter [18 USCS §§ 2510 et seq.] for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or

electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 [50 USCS § 1801] if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with--

(A) a court order directing such assistance or a court order pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978 [50 USCS § 1881c] signed by the authorizing judge, or

(B) a certification in writing by a person specified in section 2518(7) of this title [18 USCS § 2518(7)] or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required,

setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished an order or certification under this subparagraph, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520 [18 USCS § 2520]. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or certification under this chapter [18 USCS §§ 2510 et seq.].

(iii) If a certification under subparagraph (ii)(B) for assistance to obtain foreign intelligence information is based on statutory authority, the certification shall identify the specific statutory provision and shall certify that the statutory requirements have been met.

(b) It shall not be unlawful under this chapter [18 USCS §§ 2510 et seq.] for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 [47 USCS §§ 151 et seq.] of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter [18 USCS §§ 2510 et seq.] for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter [18 USCS §§ 2510 et seq.] for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934 [47 USCS § 605 or 606], it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 [50 USCS § 1801], as authorized by that Act [50 USCS §§ 1801 et seq.].

(f) Nothing contained in this chapter or chapter 121 or 206 of this title [18 USCS §§ 2510 et seq., or 2701 et seq., or 3121 et seq.], or section 705 of the Communications Act of 1934 [47 USCS § 605], shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance

with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 [50 USCS § 1801], and procedures in this chapter or chapter 121 or 206 of this title [18 USCS §§ 2510 et seq., or 2701 et seq., or 3121 et seq.] and the Foreign Intelligence Surveillance Act of 1978 [50 USCS §§ 1801 et seq.] shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act [50 USCS § 1801], and the interception of domestic wire, oral, and electronic communications may be conducted.

(g) It shall not be unlawful under this chapter [18 USCS §§ 2510 et seq.] or chapter 121 of this title [18 USCS §§ 2701 et seq.] for any person--

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

(ii) to intercept any radio communication which is transmitted--

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

(IV) by any marine or aeronautical communications system;

(iii) to engage in any conduct which--

(I) is prohibited by section 633 of the Communications Act of 1934 [47 USCS § 553]; or

(II) is excepted from the application of section 705(a) of the Communications Act of 1934 [47 USCS § 605(a)] by section 705(b) of that Act [47 USCS § 605(b)];

(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or

(v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

(h) It shall not be unlawful under this chapter [18 USCS §§ 2510 et seq.]--

(i) to use a pen register or a trap and trace device (as those terms are defined for the purposes of chapter 206 (relating to pen registers and trap and trace devices) of this title) [18 USCS §§ 3121 et seq.]; or

(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.

(i) It shall not be unlawful under this chapter [18 USCS §§ 2510 et seq.] for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if--

(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

(II) the person acting under color of law is lawfully engaged in an investigation;

(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

(IV) such interception does not acquire communications other than those transmitted to or from the

computer trespasser.

(3)

(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication--

(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title [18 USCS § 2511(2)(a) or 2517];

(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

(4) (a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

(b) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted--

(i) to a broadcasting station for purposes of retransmission to the general public; or

(ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls,

is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

(5) (a) (i) If the communication is--

(A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter [18 USCS §§ 2510 et seq.] is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or

(B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter [18 USCS §§ 2510 et seq.] is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain,

then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction.

(ii) In an action under this subsection--

(A) if the violation of this chapter [18 USCS §§ 2510 et seq.] is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title [18 USCS § 2520], the Federal Government shall be entitled to appropriate injunctive relief; and

(B) if the violation of this chapter [18 USCS §§ 2510 et seq.] is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under

section 2520 [18 USCS § 2520], the person shall be subject to a mandatory \$ 500 civil fine.

(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than \$ 500 for each violation of such an injunction.

Prospective amendment:

Amendment of para. (2)(a)(ii)(A), effective Dec. 31, 2012. Act July 10, 2008, P.L. 110-261, Title IV, § 403(b)(2)(C), 122 Stat. 2474, provides that effective 12/31/2012, as provided by § 403(b)(2)(C) of such Act, which appears as a note to this section, except as provided in section 404 [50 USCS § 1801 note], section 2511(2)(a)(ii)(A) of title 18, United States Code [para. (2)(a)(ii)(A) of this section], is amended by striking 'or a court order pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978'.

18 USC § 2515. Prohibition of use as evidence of intercepted wire or oral communications

Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter [18 USCS §§ 2510 et seq.].

§ 2516. Authorization for interception of wire, oral, or electronic communications

(1) The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division or National Security Division specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter [18 USCS § 2518] an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of--

(a) any offense punishable by death or by imprisonment for more than one year under sections 2122 and 2274 through 2277 of title 42 of the United States Code (relating to the enforcement of the Atomic Energy Act of 1954), section 2284 of title 42 of the United States Code (relating to sabotage of nuclear facilities or fuel), or under the following chapters of this title: chapter 10 [18 USCS §§ 175 et seq.] (relating to biological weapons)[,] chapter 37 [18 USCS §§ 791 et seq.] (relating to espionage), chapter 55 [18 USCS §§ 1201 et seq.] (relating to kidnapping), chapter 90 [18 USCS §§ 1831 et seq.] (relating to protection of trade secrets), chapter 105 [18 USCS §§ 2151 et seq.] (relating to sabotage), chapter 115 [18 USCS §§ 2381 et seq.] (relating to treason), chapter 102 [18 USCS §§ 2101 et seq.] (relating to riots), chapter 65 [18 USCS §§ 1361 et seq.] (relating to malicious mischief), chapter 111 [18 USCS §§ 2271 et seq.] (relating to destruction of vessels), or chapter 81 [18 USCS §§ 1621 et seq.] (relating to piracy);

(b) a violation of section 186 or section 501(c) of title 29, United States Code (dealing with restrictions on payments and loans to labor organizations), or any offense which involves murder, kidnapping, robbery, or extortion, and which is punishable under this title;

(c) any offense which is punishable under the following sections of this title: section 37 [18 USCS § 37] (relating to violence at international airports), section 43 [18 USCS § 43] (relating to animal enterprise terrorism), section 81 [18 USCS § 81] (arson within special maritime and territorial jurisdiction), section 201 [18 USCS § 201] (bribery of public officials and witnesses), section 215 [18 USCS § 215] (relating to bribery of bank officials), section 224 [18 USCS § 2224] (bribery in sporting contests), subsection (d), (e), (f), (g), (h), or (i) of section 844 [18 USCS § 844] (unlawful use of explosives), section 1032 [18 USCS § 1032] (relating to concealment of assets), section 1084 [18 USCS § 1032] (transmission of wagering information), section 751 [18 USCS § 751] (relating to escape), section 832 [18 USCS § 832] (relating to nuclear and weapons of mass destruction threats), section 842 [18 USCS § 842] (relating to explosive materials), section 930 [18 USCS § 930] (relating to possession of weapons in Federal facilities), section 1014 [18 USCS § 1014] (relating to loans and credit applications generally; renewals and discounts), section 1114 [18 USCS § 1114] (relating to officers and employees of the United States), section 1116 [18 USCS § 1116] (relating to protection of foreign officials), sections 1503, 1512, and 1513 [18 USCS §§ 1503, 1512, and 1513] (influencing or injuring an officer, juror, or witness generally), section 1510 [18 USCS § 1510] (obstruction of criminal investigations), section 1511 [18 USCS § 1511] (obstruction of State or local law enforcement), section 1591 [18 USCS § 1591] (sex trafficking of children by force, fraud, or coercion), section 1751 [18 USCS § 1751] (Presidential and Presidential staff assassination, kidnapping, and assault), section 1951 [18 USCS § 1951] (interference with commerce by threats or violence), section 1952 [18 USCS § 1952] (interstate and foreign travel or transportation in aid of racketeering enterprises), section 1958 [18 USCS § 1958] (relating to use of interstate commerce

facilities in the commission of murder for hire), section 1959 [18 USCS § 1959] (relating to violent crimes in aid of racketeering activity), section 1954 [18 USCS § 1954] (offer, acceptance, or solicitation to influence operations of employee benefit plan), section 1955 [18 USCS § 1955] (prohibition of business enterprises of gambling), section 1956 [18 USCS § 1956] (laundering of monetary instruments), section 1957 [18 USCS § 1957] (relating to engaging in monetary transactions in property derived from specified unlawful activity), section 659 [18 USCS § 659] (theft from interstate shipment), section 664 [18 USCS § 664] (embezzlement from pension and welfare funds), section 1343 [18 USCS § 1343] (fraud by wire, radio, or television), section 1344 [18 USCS § 1344] (relating to bank fraud), section 1992 [18 USCS § 1992] (relating to terrorist attacks against mass transportation), sections 2251 and 2252 [18 USCS §§ 2251 and 2252] (sexual exploitation of children), section 2251A [18 USCS § 2251A] (selling or buying of children), section 2252A [18 USCS § 2252A] (relating to material constituting or containing child pornography), section 1466A [18 USCS § 1466A] (relating to child obscenity), section 2260 [18 USCS § 2260] (production of sexually explicit depictions of a minor for importation into the United States), sections 2421, 2422, 2423, and 2425 [18 USCS §§ 2421, 2422, 2423, and 2425] (relating to transportation for illegal sexual activity and related crimes), sections 2312, 2313, 2314, and 2315 [18 USCS §§ 2312, 2313, 2314, and 2315] (interstate transportation of stolen property), section 2321 [18 USCS § 2321] (relating to trafficking in certain motor vehicles or motor vehicle parts), section 2340A [18 USCS § 2340A] (relating to torture), section 1203 [18 USCS § 1203] (relating to hostage taking), section 1029 [18 USCS § 1029] (relating to fraud and related activity in connection with access devices), section 3146 [18 USCS § 3146] (relating to penalty for failure to appear), section 3521(b)(3) [18 USCS § 3521(b)(3)] (relating to witness relocation and assistance), section 32 [18 USCS § 32] (relating to destruction of aircraft or aircraft facilities), section 38 [18 USCS § 38] (relating to aircraft parts fraud), section 1963 [18 USCS § 1963] (violations with respect to racketeer influenced and corrupt organizations), section 115 [18 USCS § 115] (relating to threatening or retaliating against a Federal official), section 1341 [18 USCS § 1341] (relating to mail fraud), a felony violation of section 1030 [18 USCS § 1030] (relating to computer fraud and abuse), section 351 [18 USCS § 351] (violations with respect to congressional, Cabinet, or Supreme Court assassinations, kidnapping, and assault), section 831 [18 USCS § 831] (relating to prohibited transactions involving nuclear materials), section 33 [18 USCS § 33] (relating to destruction of motor vehicles or motor vehicle facilities), section 175 [18 USCS § 175] (relating to biological weapons), section 175c (relating to variola virus), section 956 [18 USCS § 956] (conspiracy to harm persons or property overseas), [section] a felony violation of section 1028 [18 USCS § 1028] (relating to production of false identification documentation), section 1425 [18 USCS § 1425] (relating to the procurement of citizenship or nationalization unlawfully), section 1426 [18 USCS § 1426] (relating to the reproduction of naturalization or citizenship papers), section 1427 [18 USCS § 1427] (relating to the sale of naturalization or citizenship papers), section 1541 [18 USCS § 1541] (relating to passport issuance without authority), section 1542 [18 USCS § 1542] (relating to false statements in passport applications), section 1543 [18 USCS § 1543] (relating to forgery or false use of passports), section 1544 [18 USCS § 1544] (relating to misuse of passports), or section 1546 [18 USCS § 1546] (relating to fraud and misuse of visas, permits, and other documents);

(d) any offense involving counterfeiting punishable under section 471, 472, or 473 of this title [18 USCS § 471, 472, or 473];

(e) any offense involving fraud connected with a case under title 11 or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States;

(f) any offense including extortionate credit transactions under sections 892, 893, or 894 of this title [18 USCS § 892, 893, or 894];

(g) a violation of section 5322 of title 31, United States Code (dealing with the reporting of currency

transactions), or section 5324 of title 31, United States Code (relating to structuring transactions to evade reporting requirement prohibited);

(h) any felony violation of sections 2511 and 2512 [18 USCS §§ 2511 and 2512] (relating to interception and disclosure of certain communications and to certain intercepting devices) of this title;

(i) any felony violation of chapter 71 (relating to obscenity) of this title [18 USCS §§ 1460 et seq.];

(j) any violation of section 60123(b) (relating to destruction of a natural gas pipeline), section 46502 (relating to aircraft piracy), the second sentence of section 46504 (relating to assault on a flight crew with dangerous weapon), or section 46505(b)(3) or (c) (relating to explosive or incendiary devices, or endangerment of human life, by means of weapons on aircraft) of title 49;

(k) any criminal violation of section 2778 of title 22 (relating to the Arms Export Control Act);

(l) the location of any fugitive from justice from an offense described in this section;

(m) a violation of section 274, 277, or 278 of the Immigration and Nationality Act (8 U.S.C. 1324, 1327, or 1328) (relating to the smuggling of aliens);

(n) any felony violation of sections 922 and 924 of title 18, United States Code [18 USCS §§ 922 and 924] (relating to firearms);

(o) any violation of section 5861 of the Internal Revenue Code of 1986 [26 USCS § 5861] (relating to firearms); or

(p) a felony violation of section 1028 [18 USCS § 1028] (relating to production of false identification documents), section 1542 [18 USCS § 1542] (relating to false statements in passport applications), section 1546 [18 USCS § 1546] (relating to fraud and misuse of visas, permits, and other documents), section 1028A [18 USCS § 1028A] (relating to aggravated identity theft) of this title or a violation of section 274, 277, or 278 of the Immigration and Nationality Act [8 USCS § 1324, 1327, or 1328] (relating to the smuggling of aliens); [or]

(q) any criminal violation of section 229 [18 USCS § 229] (relating to chemical weapons) or section 2332, 2332a, 2332b, 2332d, 2332f, 2332g, 2332h[,] 2339, 2339A, 2339B, 2339C, or 2339D of this title [18 USCS § 2332, 2332a, 2332b, 2332d, 2332f, 2332g, 2332h, 2339, 2339A, 2339B, 2339C, or 2339D] (relating to terrorism);

(r) any criminal violation of section 1 (relating to illegal restraints of trade or commerce), 2 (relating to illegal monopolizing of trade or commerce), or 3 (relating to illegal restraints of trade or commerce in territories or the District of Columbia) of the Sherman Act (15 U.S.C. 1, 2, 3); or

(s) any conspiracy to commit any offense described in any subparagraph of this paragraph.

(2) The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire, oral, or electronic communications, may apply to such judge for, and such judge may grant in conformity with section 2518 of this chapter [18 USCS § 2518] and with the applicable State statute an order authorizing, or approving the interception of wire, oral or electronic communications by investigative or law enforcement officers having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of the commission of the offense of murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses.

(3) Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and

such judge may grant, in conformity with section 2518 of this title [18 USCS § 2518], an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of any Federal felony.

18 USC § 2517. Authorization for disclosure and use of intercepted wire, oral, or electronic communications

(1) Any investigative or law enforcement officer who, by any means authorized by this chapter [18 USCS §§ 2510 et seq.], has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.

(2) Any investigative or law enforcement officer who, by any means authorized by this chapter [18 USCS §§ 2510 et seq.], has obtained knowledge of the contents of any wire, oral, or electronic communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties.

(3) Any person who has received, by any means authorized by this chapter [18 USCS §§ 2510 et seq.], any information concerning a wire, oral, or electronic communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter [18 USCS §§ 2510 et seq.] may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof.

(4) No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter [18 USCS §§ 2510 et seq.] shall lose its privileged character.

(5) When an investigative or law enforcement officer, while engaged in intercepting wire, oral, or electronic communications in the manner authorized herein, intercepts wire, oral, or electronic communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter [18 USCS §§ 2510 et seq.]. Such application shall be made as soon as practicable.

(6) Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter [18 USCS §§ 2510 et seq.], has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or foreign intelligence information (as defined in subsection (19) of section 2510 of this title [18 USCS § 2510]), to assist the official who is to receive that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.

(7) Any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents or derivative evidence to a foreign investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure, and foreign investigative or law enforcement officers may use or disclose such contents or derivative evidence to the extent such use or disclosure is appropriate to the proper performance of their official duties.

(8) Any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents or derivative evidence to any appropriate Federal, State, local, or foreign government official to the extent that such contents or derivative evidence reveals a threat of actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power, within the United States or elsewhere, for the purpose of preventing or responding to such a threat. Any official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information, and any State, local, or foreign official who receives information pursuant to this provision may use that information only consistent with such guidelines as the Attorney General and Director of Central Intelligence shall jointly issue.

18 USC § 2518. Procedure for interception of wire, oral, or electronic communications

(1) Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under this chapter [18 USCS §§ 2510 et seq.] shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) except as provided in subsection (11), a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and

(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction), if the judge determines on the basis of the facts submitted by the applicant that--

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter [18 USCS § 2516];

(b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;

(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being

used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

(4) Each order authorizing or approving the interception of any wire, oral, or electronic communication under this chapter [18 USCS §§ 2510 et seq.] shall specify--

- (a) the identity of the person, if known, whose communications are to be intercepted;
- (b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;
- (c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;
- (d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and
- (e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

An order authorizing the interception of a wire, oral, or electronic communication under this chapter [18 USCS §§ 2510 et seq.] shall, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance. Pursuant to section 2522 of this chapter [18 USCS § 2522], an order may also be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act [47 USCS §§ 1001 et seq.].

(5) No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Such thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter [18 USCS §§ 2510 et seq.], and must terminate upon attainment of the authorized objective, or in any event in thirty days. In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter [18 USCS §§ 2510 et seq.] may be conducted in whole or in part by Government personnel, or by an individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.

(6) Whenever an order authorizing interception is entered pursuant to this chapter [18 USCS §§ 2510 et seq.], the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.

(7) Notwithstanding any other provision of this chapter [18 USCS §§ 2510 et seq.], any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that--

(a) an emergency situation exists that involves--

- (i) immediate danger of death or serious physical injury to any person,
- (ii) conspiratorial activities threatening the national security interest, or
- (iii) conspiratorial activities characteristic of organized crime,

that requires a wire, oral, or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and

(b) there are grounds upon which an order could be entered under this chapter [18 USCS §§ 2510 et seq.] to authorize such interception,

may intercept such wire, oral, or electronic communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of this chapter [18 USCS §§ 2510 et seq.], and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application.

(8) (a) The contents of any wire, oral, or electronic communication intercepted by any means authorized by this chapter [18 USCS §§ 2510 et seq.] shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire, oral, or electronic communication under this subsection shall be done in such way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of subsections (1) and (2) of section 2517 of this chapter [18 USCS § 2517] for investigations. The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, oral, or electronic communication or evidence derived therefrom under subsection (3) of section 2517 [18 USCS § 2517].

(b) Applications made and orders granted under this chapter [18 USCS §§ 2510 et seq.] shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years.

(c) Any violation of the provisions of this subsection may be punished as contempt of the issuing or

denying judge.

(d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7)(b) [18 USCS § 2518(7)(b)] which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of--

- (1) the fact of the entry of the order or the application;
- (2) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and
- (3) the fact that during the period wire, oral, or electronic communications were or were not intercepted.

The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed.

(9) The contents of any wire, oral, or electronic communication intercepted pursuant to this chapter [18 USCS §§ 2510 et seq.] or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court unless each party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved. This ten-day period may be waived by the judge if he finds that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

(10) (a) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter [18 USCS §§ 2510 et seq.], or evidence derived therefrom, on the grounds that--

- (i) the communication was unlawfully intercepted;
- (ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or
- (iii) the interception was not made in conformity with the order of authorization or approval.

Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter [18 USCS §§ 2510 et seq.]. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice.

(b) In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) of this subsection, or the denial of an application for an order of approval, if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within thirty days after the date the order was entered and shall be diligently prosecuted.

(c) The remedies and sanctions described in this chapter [18 USCS §§ 2510 et seq.] with respect to the interception of electronic communications are the only judicial remedies and sanctions for

nonconstitutional violations of this chapter [18 USCS §§ 2510 et seq.] involving such communications.

(11) The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if--

(a) in the case of an application with respect to the interception of an oral communication--

(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

(ii) the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and

(iii) the judge finds that such specification is not practical; and

(b) in the case of an application with respect to a wire or electronic communication--

(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

(ii) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing that there is probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility;

(iii) the judge finds that such showing has been adequately made; and

(iv) the order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted.

(12) An interception of a communication under an order with respect to which the requirements of subsections (1)(b)(ii) and (3)(d) of this section do not apply by reason of subsection (11)(a) shall not begin until the place where the communication is to be intercepted is ascertained by the person implementing the interception order. A provider of wire or electronic communications service that has received an order as provided for in subsection (11)(b) may move the court to modify or quash the order on the ground that its assistance with respect to the interception cannot be performed in a timely or reasonable fashion. The court, upon notice to the government, shall decide such a motion expeditiously.

18 USC § 2519. Reports concerning intercepted wire, oral, or electronic communications

(1) In January of each year, any judge who has issued an order (or an extension thereof) under section 2518 [18 USCS § 2518] that expired during the preceding year, or who has denied approval of an interception during that year, shall report to the Administrative Office of the United States Courts--

- (a) the fact that an order or extension was applied for;
- (b) the kind of order or extension applied for (including whether or not the order was an order with respect to which the requirements of sections 2518(1)(b)(ii) and 2518(3)(d) of this title [18 USCS §§ 2518(1)(b)(ii) and 2518(3)(d)] did not apply by reason of section 2518(11) of this title [18 USCS § 2518(11)]);
- (c) the fact that the order or extension was granted as applied for, was modified, or was denied;
- (d) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;
- (e) the offense specified in the order or application, or extension of an order;
- (f) the identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application; and
- (g) the nature of the facilities from which or the place where communications were to be intercepted.

(2) In March of each year the Attorney General, an Assistant Attorney General specially designated by the Attorney General, or the principal prosecuting attorney of a State, or the principal prosecuting attorney for any political subdivision of a State, shall report to the Administrative Office of the United States Courts--

- (a) the information required by paragraphs (a) through (g) of subsection (1) of this section with respect to each application for an order or extension made during the preceding calendar year;
- (b) a general description of the interceptions made under such order or extension, including (i) the approximate nature and frequency of incriminating communications intercepted, (ii) the approximate nature and frequency of other communications intercepted, (iii) the approximate number of persons whose communications were intercepted, (iv) the number of orders in which encryption was encountered and whether such encryption prevented law enforcement from obtaining the plain text of communications intercepted pursuant to such order, and (v) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions;
- (c) the number of arrests resulting from interceptions made under such order or extension, and the offenses for which arrests were made;
- (d) the number of trials resulting from such interceptions;
- (e) the number of motions to suppress made with respect to such interceptions, and the number granted or denied;
- (f) the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and a general assessment of the importance of the interceptions; and
- (g) the information required by paragraphs (b) through (f) of this subsection with respect to orders or extensions obtained in a preceding calendar year.

(3) In June of each year the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire, oral, or electronic communications pursuant to this chapter [18 USCS §§ 2510 et seq.] and the number of orders and extensions granted or denied pursuant to

this chapter [18 USCS §§ 2510 et seq.] during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the Administrative Office by subsections (1) and (2) of this section. The Director of the Administrative Office of the United States Courts is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by subsections (1) and (2) of this section.

All Writs Act

§ 1651. Writs

(a) The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.

(b) An alternative writ or rule nisi may be issued by a justice or judge of a court which has jurisdiction.

Rule 41 of the Federal Rules of Criminal Procedure

Search and Seizure

(a) Scope and Definitions.

(1) *Scope.* This rule does not modify any statute regulating search or seizure, or the issuance and execution of a search warrant in special circumstances.

(2) *Definitions.* The following definitions apply under this rule:

(A) "Property" includes documents, books, papers, any other tangible objects, and information.

(B) "Daytime" means the hours between 6:00 a.m. and 10:00 p.m. according to local time.

(C) "Federal law enforcement officer" means a government agent (other than an attorney for the government) who is engaged in enforcing the criminal laws and is within any category of officers authorized by the Attorney General to request a search warrant.

(D) "Domestic terrorism" and "international terrorism" have the meanings set out in 18 U.S.C. § 2331.

(E) "Tracking device" has the meaning set out in 18 U.S.C. § 3117(b).

(b) Authority to Issue a Warrant. At the request of a federal law enforcement officer or an attorney for the government:

(1) a magistrate judge with authority in the district--or if none is reasonably available, a judge of a state court of record in the district--has authority to issue a warrant to search for and seize a person or property located within the district;

(2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;

(3) a magistrate judge -- in an investigation of domestic terrorism or international terrorism -- with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;

(4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and

(5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:

(A) a United States territory, possession, or commonwealth;

(B) the premises -- no matter who owns them -- of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or

(C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

(c) Persons or Property Subject to Search or Seizure. A warrant may be issued for any of the following:

(1) evidence of a crime;

(2) contraband, fruits of crime, or other items illegally possessed;

(3) property designed for use, intended for use, or used in committing a crime; or

(4) a person to be arrested or a person who is unlawfully restrained.

(d) Obtaining a Warrant.

(1) *In General.* After receiving an affidavit or other information, a magistrate judge--or if authorized by Rule 41(b), a judge of a state court of record--must issue the warrant if there is probable cause to search for and seize a person or property or to install and use a tracking device.

(2) *Requesting a Warrant in the Presence of a Judge.*

(A) Warrant on an Affidavit. When a federal law enforcement officer or an attorney for the government presents an affidavit in support of a warrant, the judge may require the affiant to appear personally and may examine under oath the affiant and any witness the affiant produces.

(B) Warrant on Sworn Testimony. The judge may wholly or partially dispense with a written affidavit and base a warrant on sworn testimony if doing so is reasonable under the circumstances.

(C) Recording Testimony. Testimony taken in support of a warrant must be recorded by a court reporter or by a suitable recording device, and the judge must file the transcript or recording with the clerk, along with any affidavit.

(3) *Requesting a Warrant by Telephonic or Other Means.*

(A) *In General.* A magistrate judge may issue a warrant based on information communicated by telephone or other reliable electronic means.

(B) Recording Testimony. Upon learning that an applicant is requesting a warrant under Rule 41(d)(3)(A), a magistrate judge must:

- (i) place under oath the applicant and any person on whose testimony the application is based; and
- (ii) make a verbatim record of the conversation with a suitable recording device, if available, or by a court reporter, or in writing.

(C) Certifying Testimony. The magistrate judge must have any recording or court reporter's notes transcribed, certify the transcription's accuracy, and file a copy of the record and the transcription with the clerk. Any written verbatim record must be signed by the magistrate judge and filed with the clerk.

(D) Suppression Limited. Absent a finding of bad faith, evidence obtained from a warrant issued under Rule 41(d)(3)(A) is not subject to suppression on the ground that issuing the warrant in that manner was unreasonable under the circumstances.

(e) Issuing the Warrant.

(1) *In General.* The magistrate judge or a judge of a state court of record must issue the warrant to an officer authorized to execute it.

(2) *Contents of the Warrant.*

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

- (i) execute the warrant within a specified time no longer than 14 days;
- (ii) execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time; and
- (iii) return the warrant to the magistrate judge designated in the warrant.

(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

(C) Warrant for a Tracking Device. A tracking-device warrant must identify the person or property to

be tracked, designate the magistrate judge to whom it must be returned, and specify a reasonable length of time that the device may be used. The time must not exceed 45 days from the date the warrant was issued. The court may, for good cause, grant one or more extensions for a reasonable period not to exceed 45 days each. The warrant must command the officer to:

(i) complete any installation authorized by the warrant within a specified time no longer than 10 calendar days;

(ii) perform any installation authorized by the warrant during the daytime, unless the judge for good cause expressly authorizes installation at another time; and

(iii) return the warrant to the judge designated in the warrant.

(3) *Warrant by Telephonic or Other Means.* If a magistrate judge decides to proceed under Rule 41(d)(3)(A), the following additional procedures apply:

(A) *Preparing a Proposed Duplicate Original Warrant.* The applicant must prepare a "proposed duplicate original warrant" and must read or otherwise transmit the contents of that document verbatim to the magistrate judge.

(B) *Preparing an Original Warrant.* If the applicant reads the contents of the proposed duplicate original warrant, the magistrate judge must enter those contents into an original warrant. If the applicant transmits the contents by reliable electronic means, that transmission may serve as the original warrant.

(C) *Modification.* The magistrate judge may modify the original warrant. The judge must transmit any modified warrant to the applicant by reliable electronic means under Rule 41(e)(3)(D) or direct the applicant to modify the proposed duplicate original warrant accordingly.

(D) *Signing the Warrant.* Upon determining to issue the warrant, the magistrate judge must immediately sign the original warrant, enter on its face the exact date and time it is issued, and transmit it by reliable electronic means to the applicant or direct the applicant to sign the judge's name on the duplicate original warrant.

(f) *Executing and Returning the Warrant.*

(1) *Warrant to Search for and Seize a Person or Property.*

(A) *Noting the Time.* The officer executing the warrant must enter on it the exact date and time it was executed.

(B) *Inventory.* An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. The officer must do so in the presence of another officer and the person from whom, or from whose premises, the property was taken. If either one is not present, the officer must prepare and verify the inventory in the presence of at least one other credible person. In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.

(C) *Receipt.* The officer executing the warrant must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken or leave a copy of the warrant and receipt at the place where the officer took the property.

(D) *Return.* The officer executing the warrant must promptly return it--together with a copy of the inventory--to the magistrate judge designated on the warrant. The judge must, on request, give a copy of the inventory to the person from whom, or from whose premises, the property was taken and to the applicant for the warrant.

(2) *Warrant for a Tracking Device.*

(A) *Noting the Time.* The officer executing a tracking-device warrant must enter on it the exact date and time the device was installed and the period during which it was used.

(B) *Return.* Within 10 calendar days after the use of the tracking device has ended, the officer

executing the warrant must return it to the judge designated in the warrant.

(C) *Service.* Within 10 calendar days after the use of the tracking device has ended, the officer executing a tracking-device warrant must serve a copy of the warrant on the person who was tracked or whose property was tracked. Service may be accomplished by delivering a copy to the person who, or whose property, was tracked; or by leaving a copy at the person's residence or usual place of abode with an individual of suitable age and discretion who resides at that location and by mailing a copy to the person's last known address. Upon request of the government, the judge may delay notice as provided in Rule 41(f)(3).

(3) *Delayed Notice.* Upon the government's request, a magistrate judge--or if authorized by Rule 41(b), a judge of a state court of record--may delay any notice required by this rule if the delay is authorized by statute.

(4) *Return.* The officer executing the warrant must promptly return it--together with a copy of the inventory--to the magistrate judge designated on the warrant. The judge must, on request, give a copy of the inventory to the person from whom, or from whose premises, the property was taken and to the applicant for the warrant.

(g) *Motion to Return Property.* A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to protect access to the property and its use in later proceedings.

(h) *Motion to Suppress.* A defendant may move to suppress evidence in the court where the trial will occur, as Rule 12 provides.

(i) *Forwarding Papers to the Clerk.* The magistrate judge to whom the warrant is returned must attach to the warrant a copy of the return, of the inventory, and of all other related papers and must deliver them to the clerk in the district where the property was seized.

Sample Excerpt of
Discovery Request
(from E.D.N.Y)

1. Please provide all records or materials concerning cached emails. This includes, but is not limited to, wire or electronic communications that are in electronic storage in an electronic communications system. Please provide copies of any applications, orders, warrants, and “(d) subpoenas” that were prepared in connection with this case. 18 U.S.C. § 2703(d).
2. Please provide all records or materials concerning IP (Internet Protocol) addresses of websites the defendant visited and the to/from addresses of the defendant’s emails obtained through the use of a pen register. Please provide copies of any applications, orders, warrants, and subpoenas that were prepared in connection with this case. 18 U.S.C. §§ 3122, 3123.
3. In addition, please provide all records or materials concerning the full Uniform Resource Locators (URLs, or web addresses) visited by the defendant, and the total volume of information transmitted to or from the defendant’s account. Please provide copies of any applications, orders, warrants, and subpoenas that were prepared in connection with this case. 18 U.S.C. §§ 3122, 3123.
4. Please provide all records and materials concerning “post-cut-through dialed digits,” which includes any numbers dialed after a call is initially routed, obtained using a pen register or a trap and trace device. This includes information from a pen register, which records numbers dialed for outgoing calls made from the target phone, as well as information from a trap and trace device, which captures the numbers of calls made to the target phone. Please provide copies of any applications, orders, warrants, and subpoenas that were prepared in connection with this case. 18 U.S.C. §§ 3122, 3123. *See In the Matter of Applications of the United States of America for Orders (1) Authorizing the Use of Pen Registers and Trap and Trace Devices and (2) Authorizing Release of Subscriber Information*, 515 F. Supp. 2d 325 (E.D.N.Y. 2007).
5. Please provide all records and materials concerning real-time and historical cell phone location tracking. This “cell-site data” includes, but is not limited to, the location of the cell site/sector (physical address) at call origination (for outbound calling), at call termination (for incoming calls), and during the progress of the call, for the subject telephone. Please provide copies of any applications, orders, warrants, or subpoenas that were prepared in connection with this case. 18 U.S.C. §§ 2703(d), 3122, 3123. *See In the Matter of an Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005).

6. Please provide all other material that was obtained as a result of digital searches and seizures, whether with or without a warrant or subpoena.

O:\Client\Hay\00 FOLDERS 1-22\CLEs\CLE New\elec-surv.wpd

Testimony of
M.J. Stephen Smith
(6/24/10)

Before the
Committee on the Judiciary
Subcommittee on the Constitution, Civil Rights, and Civil Liberties
2237 Rayburn House Office Building
Washington, D.C. 20515

HEARING ON ELECTRONIC COMMUNICATIONS PRIVACY ACT REFORM
AND THE REVOLUTION IN LOCATION BASED
TECHNOLOGIES AND SERVICES

June 24, 2010

Written Testimony of
United States Magistrate Judge
Stephen Wm. Smith

Mr. Chairman, Ranking Member, and Members of the Subcommittee:

I am honored by your invitation to testify at today's hearing. I am a U.S. Magistrate Judge for the Southern District of Texas, sitting in Houston. While this testimony is my own, and not offered as the official position of any group or organization, it is a view from the trenches shared by many of my fellow magistrate judges across the country. Before reaching the substance of my testimony, it might be helpful to outline the role of magistrate judges in handling law enforcement requests under ECPA.

1. Role of Magistrate Judges in Electronic Surveillance¹

There are over 500 federal magistrate judges serving in district courts around the country. In addition to civil matters, our responsibilities on the criminal side generally include almost everything except conducting felony trials. We conduct initial appearances, appoint counsel for indigents, set bail conditions, hold detention hearings, issue criminal complaints and arrest warrants, take grand jury returns, handle extradition requests, misdemeanor trials, competency hearings, and suppression motions. One of our chief functions is to issue search warrants and other orders in aid of criminal investigations. These include electronic surveillance orders for pen registers, trap and trace devices, tracking devices, 2703(d) orders for telephone and e-mail account records and activity. That is where our experience with ECPA comes in.

Although different districts may handle it differently, in most districts there is at least one magistrate judge on criminal duty at all times, ready to take a call 24 hours a day, 7 days a week. In the Houston division we have 5 magistrate judges, and we rotate the criminal duty among ourselves every two weeks. While on duty we carry either a beeper or dedicated cell phone to allow instant access by law enforcement. It is not uncommon for a magistrate judge to be contacted at night or on a weekend to issue electronic surveillance orders in cases of emergency, such as a kidnaping or alien smuggling. With rare exceptions, ECPA orders pertain to ordinary crimes and criminals, not national security or terrorism cases.

The process is *ex parte*, meaning only one party – law enforcement – appears before the magistrate judge. Since this is at the criminal investigation stage, no

¹ For purposes of my testimony, "electronic surveillance" includes pen registers, trap and trace devices, tracking devices, cell site information ("CSI"), stored e-mail, telephone and e-mail activity logs, and customer account records from electronic service providers. Wiretap orders, which are issued only by district judges, are not included.

defendant has yet been charged so no defense counsel is there to challenge the government's request. Likewise, no representative of the electronic service provider or the target phone's subscriber is present. In fact, the orders routinely contain gag orders precluding the service provider from advising their customers that the government is accessing their cell phone or e-mail account records. The public rarely learns about these orders, even long after issuance, because they are routinely placed under indefinite (*i.e.*, permanent) seal.

Actual data on the number of electronic surveillance orders issued under ECPA is not readily available, as far as I know.² However, some idea can be gleaned from a recent survey by the Federal Judicial Center.³ This study, which looked at the prevalence of completely sealed cases in federal court, surveyed every federal case filed in all federal courts during 2006. It found that of the 97,155 criminal matters handled by magistrate judges that year, 15,177 were completely sealed from public. The vast majority of those were warrant-related applications.

Another data point is provided by a local survey of such orders issued by our court in Houston from 1995 through 2007. According to that survey, Houston's five magistrate judges issued a total of 4,234 electronic surveillance orders, or about 325 every year.⁴ Considering that this volume was generated by less than 1% of the federal magistrate judges in the country, it is safe to conclude that the 2006 total in the FJC study was not a fluke. A reasonable estimate is that the total number of electronic surveillance orders issued at the federal level each year substantially exceeds 10,000.⁵

² ECPA requires the Attorney General to report to Congress the number of pen registers applied for annually. *See* 18 U.S.C. § 3126. However, there is no separate reporting requirement for tracking devices under § 3117 or location information obtained under § 2703(d).

³ The study is available online at: [www.fjc.gov/public/pdf.nsf/lookup/sealcafc.pdf/\\$file/sealcafc.pdf](http://www.fjc.gov/public/pdf.nsf/lookup/sealcafc.pdf/$file/sealcafc.pdf).

⁴ *See In re Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F.Supp.2d 876, 895 (S.D. Tex. 2008).

⁵ This does not include the number of such orders issued by state courts.

2. In Pursuit of Hidden Elephants⁶

I took the bench in 2004, having no background in criminal law. In fact I had never heard of a trap and trace device until I was confronted with an application for one on my first day of criminal duty. The application also asked for something called “cell site information.” Reluctant to sign what I did not understand, I turned to the United States Code and encountered ECPA for the first time. The experience was frustrating: the terminology was unfamiliar, the organization not intuitive, and the syntax far from straightforward. The casenotes accompanying the statute shed no light; they cited only a handful of lower court decisions not particularly relevant to my questions. No appellate court had ever addressed the issue. I asked my colleagues on the bench, and found they were just as puzzled as I was. I tried to look at sample orders from other courts, but found that they were sealed. I met (several times) with the AUSAs, who basically argued that their request should be granted because other judges had done so.

Still unsatisfied, I plunged into the legislative history of ECPA, reading every committee report and law review article I could find. I contacted law professors who had written about ECPA, as well as a former Congressional staffer who had helped draft the law and subsequent amendments. I met with our local U.S. Marshals, who gave me a tour of their local electronic surveillance shop and a demonstration of the technology. I called various service providers to get their perspective. I then spent several months drafting a memo, setting out my tentative conclusions and supporting analysis. I sent the memo to our local U.S. Attorney, asking him exactly what was wrong with my analysis and why. He forwarded the memo to DOJ, which responded months later with a detailed rebuttal, advocating what has since come to be known as the hybrid theory. Unpersuaded, I issued my first opinion on cell site information in October 2005.⁷

Prospective CSI. From my research, I came to understand that ECPA authorized various criminal investigative tools under four different legal standards.

⁶ “[Congress] does not, one might say, hide elephants in mouseholes.” *Whitman v. American Trucking Ass’n*, 531 U.S. 457, 468 (2001) (Scalia, J.).

⁷ *In re Application*, 396 F.Supp.2d 747 (S.D. Tex. 2005). This was actually the second published decision on the topic. Magistrate Judge James Orenstein had issued a decision reaching the same conclusion two months earlier, although the government did not make the hybrid argument in support of that application. See *In re Application of the U.S.*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005).

Generally speaking, the more intrusive the investigative tool, the greater the legal process necessary to access it. Visualize it as a 4-story courthouse: pen registers and trap/trace devices are on the ground floor, having the least demanding standard (“certified relevance”); stored communications and account records are on the second floor, accessible with “specific and articulable facts”;⁸ tracking device warrants are on the third floor, covered by the familiar Rule 41 “probable cause” standard; wiretap orders are on the top floor, with their “super-warrant” requirements. A chart illustrating this “Electronic Surveillance Courthouse” is attached as Exhibit A.⁹

The essential difficulty, of course, is that ECPA does not explicitly refer to “cell site” or other location information from a cell phone. In the case before me, the Government sought compelled access to a full range of cell site information (CSI) on a prospective basis.¹⁰ My basic approach was to determine which floor of the courthouse was the best fit for this type of request. Because the Government’s stated purpose was to locate the target phone user in real time, the most obvious candidate seemed to be the third floor, for tracking devices. The statutory definition of a tracking device is very broad and unqualified, and could easily be read to encompass the unlimited CSI sought here.¹¹ Moreover, none of the other categories of electronic surveillance seemed to fit. The pen register standard was ruled out by a proviso in a 1994 statute known as CALEA.¹² The wiretap standard did not apply because CSI does not reveal the contents of a communication. The Stored Communications Act (SCA) standard did not seem to apply for two reasons: the definition of “electronic

⁸ This is an oversimplification, but sufficient for our purpose. *See* 18 U.S.C. § 2703.

⁹ Again, this chart oversimplifies in several respects. For example, it ignores the complicating distinction between communications held in a remote computing service and those held in electronic storage by an electronic communications service provider. It also excludes non-judicial processes such as administrative and grand jury subpoenas.

¹⁰ The application sought “the location of cell site/sector (physical address) at call origination (for outbound calling), call termination (for incoming calls) and, if reasonably available, during the progress of a call,” in addition to “the strength, angle, and timing of the caller’s signal measured at two or more cell sites, as well as other system information such as a listing of all cell towers in the market area, switching technology, protocols, and network architecture.” 390 F. Supp. 2d at 749.

¹¹ *See* 18 U.S.C. § 3117(b) (“the term ‘tracking device’ means an electronic or mechanical device which permits the tracking of the movement of a person or object.”).

¹² The Communications Assistance to Law Enforcement Act, 47 U.S.C. § 1002(a)(2).

communication” specifically excludes information from a tracking device;¹³ and the structure of the SCA was inherently retrospective, allowing access to documents and records already created, as opposed to prospective real time monitoring. I concluded that there was “no reason to treat cell phone tracking differently from other forms of tracking under 18 U.S.C. § 3117, which routinely require probable cause.”¹⁴

Other magistrate judges soon began to weigh in with published decisions of their own. Many agreed with me, some did not. The first opinion with a contrary view was issued in December 2005 by Magistrate Judge Gabriel Gorenstein in the Southern District of New York.¹⁵ He held that a limited form of prospective CSI¹⁶ could be obtained under the SCA standard of specific and articulable facts, a lesser showing than probable cause. His opinion accepted the Government’s hybrid theory and provided what remains its most cogent expression to date. In essence, that theory argued that a lesser standard for obtaining this information could be implied from a combination of provisions in three separate statutes.¹⁷ Even as he was adopting the hybrid theory’s conclusion, Judge Gorenstein declared the result “unsatisfying,”

¹³ 18 U.S.C. § 2510(12)(C).

¹⁴ 396 F. Supp.2d at 757. The opinion closed by expressing hope “that the government will seek appropriate review by higher courts so that authoritative guidance will be given the magistrate judges who are called upon to rule on these applications on a daily basis.” *Id.* at 765. Unfortunately, with a single exception in five years, that plea has fallen on deaf ears.

¹⁵ 405 F. Supp. 2d 435 (S.D.N.Y. 2005).

¹⁶ His order “contemplates the production only of: (1) information regarding cell site location that consists of the tower receiving transmissions from the target phone (and any information on what portion of that tower is receiving a transmission, if available); (2) tower information that is tied to a particular telephone call made or received by the user; and (3) information that is transmitted from the provider to the Government.” 405 F. Supp. 2d at 450.

¹⁷ I have compared this analysis (perhaps uncharitably) to a three-rail bank-shot: The first rail is the Pen Register Statute (as amended by the 2001 Patriot Act), asserted to be the exclusive means by which law enforcement might acquire non-content signaling information such as cell site data. The second rail is the 1994 CALEA statute, which provides that location information such as cell site data cannot be obtained “solely pursuant” to a pen/trap order. This was interpreted to mean that, while a pen/trap order is still a necessary condition for compulsory disclosure of cell site data, it is no longer sufficient, and must be combined with some additional authority. According to the Government, this authority is found in the third rail, otherwise known as the SCA, which allows Government access to cell phone customer records upon a showing of “specific and articulable facts.”

given the lack of clear guidance from Congress.¹⁸ Finally, he emphasized that his ruling was restricted to a limited form of CSI yielding only generalized location data.¹⁹

A spate of magistrate judge opinions followed in the next three years, and eventually even a few district judges weighed in. Surveying the published opinions, it is fair to conclude that the majority held that probable cause is the appropriate standard for government access to prospective cell site information. A minority of published decisions, following Judge Gorenstein, allow access under the lesser “specific and articulable facts” standard. Significantly, each of these opinions also restrict their holdings to limited CSI; not one reported decision has ever allowed access to unlimited (*i.e.*, multi-tower, triangulation or GPS) location data on anything other than a probable cause showing.²⁰ A chart of all published decisions to date concerning prospective cell site information is attached as Exhibit B.

Historical CSI. A later round of published decisions centered on the question of government access to historical cell site data. The first wave of CSI decisions, even those requiring probable cause for prospective location information, had assumed or suggested that historical location information was not materially different from other forms of account records or customer information in the hands of the phone company, and therefore obtainable under the lesser standard of SCA § 2703(d). Although not the first decision to challenge that consensus, the most prominent was issued in 2008 by Magistrate Judge Lisa Pupo Lenihan on behalf of all magistrate judges sitting in the Western District of Pennsylvania.²¹ Judge Lenihan reasoned that the text and legislative history of ECPA and its amendments warranted no “distinction between real-time (‘prospective’) and stored (‘historic’) cell-phone-derived

¹⁸ 405 F. Supp. 2d at 442.

¹⁹ *Id.* at 449-50.

²⁰ Most magistrate judges have not taken the time to issue published opinions on this question, so the possibility exists that published opinions are not a representative sample of magistrate judge opinion as a whole. Indeed, some standard government applications make the claim that “the silent majority of magistrate and district courts that routinely grant pen/trap/cell orders under the combined authority of Pen/Trap and SCA continue to do so without resort to publishing decisions affirming their current practice thus permitting the minority view to appear more pervasive than it is.”

²¹ 534 F. Supp. 2d 585 (W.D.Pa. 2008).

movement/location information.”²² Her decision is currently on appeal before the U.S. Court of Appeals for the Third Circuit. It is the first and to my knowledge the only time the Government has appealed any district court ruling on cell phone tracking. A listing of decisions addressing the standard for historical cell site information is included on Exhibit B.

Uncertainty over cell phone location information is hardly the only difficulty magistrate judges have encountered in dealing with ECPA. For example, there is the issue of post-cut-through dialed digits;²³ many others could be added. Those matters are beyond the scope of today’s hearing, so there is no need to address them here. But when the Subcommittee does decide to take up those matters we hope that you will again afford magistrate judges the opportunity to offer you the benefit of our experience.

3. A Modest Prescription: Simplicity and Transparency

ECPA was passed in 1986 as a laudable attempt to balance the privacy rights of citizens and the legitimate interests of law enforcement, given the communications technology of that day. In reforming and updating ECPA for the 21st century, the task of finding the appropriate balance belongs first of all to the political branches. Obviously, there are important First and Fourth Amendment concerns to be weighed. As a judicial officer, I do not presume to advocate for either side of that debate. That said, from a magistrate judge’s perspective, there are two systemic flaws in the existing statutory scheme that ought not be preserved in the next.

Undue complexity. The new statute should clearly specify the types of information available and the legal showing required for government access. To the extent distinctions must be made, legal standards should not be tied to a particular device or form of technology, which is probably on the road to obsolescence as you debate it. That type of standard inevitably presents judges with the most vexing of interpretive choices, forcibly fitting the round peg of tomorrow’s technology into the square hole of yesterday’s.

As a matter of logic, the legal standards for government access to location information should be geared to the level of intrusion into citizens’ privacy. But in

²² Id. at 601.

²³ See *In re Application of U.S.*, 622 F. Supp. 2d 411 (S.D. Tex. 2007) (Rosenthal, D.J.); *In re Application of U.S.*, 515 F. Supp. 2d 325 (E.D.N.Y. 2007) (Azrack); *In re Application*, 441 F. Supp. 2d 816 (S.D. Tex. 2006) (Smith).

my view the temptation to draw fine distinctions for different ways of monitoring cell phone location ought to be resisted. Even as to existing technology, those distinctions can be difficult to draw in the abstract. CSI comes in a wide variety of forms, offering differing tracking capabilities: Is there a meaningful distinction between CSI from a single urban tower and that from multiple rural towers? Between registration information or call-identifying information? What about “pings” or calls initiated by law enforcement? Should a different standard apply for location information pertaining to third parties calling or called by the target phone? How does one calibrate the relative degree of intrusion of such monitoring techniques, given that the precision of the location information obtained will vary from case to case, often depending on inferences drawn from other sources? For instance, when law enforcement already knows the business and residential addresses of the target (or the target’s family, friends, and associates), a single phone call signal captured from a single tower may be all that’s needed to reliably pinpoint a target’s exact location at a given time.

Similar difficulties will plague any attempt to distinguish between historical and prospective cell phone information. How is “historical” to be defined – one second after transmission?²⁴ One hour? One day? One month? The case law to date has understandably sidestepped this knotty issue.²⁵ To avoid confusion, any dividing line will have to be explicit, and necessarily arbitrary. The term “prospective” is also ambiguous; although often employed as a synonym for “real-time,” they are not really the same thing.²⁶ Real-time monitoring captures CSI the instant it is transmitted; it is the polar opposite of historical CSI. On the other hand, prospective CSI may be understood as referring to that generated anytime after the court issues its order. Thus, prospective CSI may well include not only real-time CSI, but also historical CSI generated while the order is in effect.²⁷ And what about historical CSI that is captured only at the instigation of law enforcement, and for which the provider has

²⁴ See Albert Gidari Jr., *Companies Caught in the Middle*, 41 U.S.F. L. Rev. 535, 544 (2007) (“In essence, [cell tower registration information] becomes historical, transactional information within a millisecond of when the provider receives it.”).

²⁵ In my orders I take the position that “historical” CSI means any data existing as of the date of the order. This avoids the need to pick an arbitrary age limit.

²⁶ See *In re Application of the U.S.*, 402 F. Supp. 2d 597, 599 & n.5 (D. Md. 2005) (Bredar).

²⁷ Pen/trap orders typically expire after 60 days, although they may be renewed an unlimited number of times. 18 U.S.C. § 3123(c)(2).

no legitimate business reason to generate or maintain on its own. Should the standard to *create* CSI be different than that to *retrieve* CSI maintained in the ordinary course of business?

The task of drafting a rational, readily comprehended, easily administered statutory scheme to govern law enforcement access to electronic communications is daunting. Complicating that effort – by multiple distinctions based on predicted intrusion levels for different forms of location data – seems not only ill-advised, but also counter-productive. It’s also likely to prove a waste of time in the wake of technology’s inexorable advance.

Undue Secrecy. As pointed out earlier, the vast majority of electronic surveillance orders are issued under seal. This of course is understandable – immediate disclosure of the target’s name and number might defeat the purpose of the surveillance. The problem is the duration and extent of that secrecy.

Under ECPA, secrecy is achieved in two-ways: (1) gag orders preventing service providers from informing customers about law enforcement monitoring of their cell phone and e-mail usage; and (2) sealing orders denying public access to judicial orders.²⁸ Typically, electronic surveillance orders contain both types of provisions, but rarely impose an expiration period; instead, those orders remain in place “until further order of the court.”²⁹ The catch is that there is no mechanism in place for the judge to revisit the sealing order. She does not retain jurisdiction over the case, which is not a “case” at all but an investigation that may or may not ripen into a real case. Other surveillance applications pertaining to that investigation will be given a separate case number and assigned to the judge on duty at the time.³⁰ The

²⁸ Pen register orders must be sealed, and must direct the provider not to disclose to anyone the existence of the order or the investigation, “until otherwise ordered by the court.” 18 U.S.C. § 3123(d)(1) & (2). By contrast, the SCA does not require § 2703(d) orders to be sealed, and allows for “preclusion of notice” to others only if there is reason to believe the investigation would be jeopardized or other adverse consequences would result. 18 U.S.C. § 2705(b)(1)-(5). As a practical matter, the government routinely combines pen/trap applications with requests for customer information under § 2703(d), and so gets the benefit of the more restrictive pen register provisions.

²⁹ *In Re Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 879-80 (S.D. Tex. 2008).

³⁰ In my court I have devised a protocol to deal with this problem: the order is initially sealed for 180 days, subject to extension upon a certification from the AUSA that the investigation is still active or that exceptional circumstances warrant the extension. *Id.* at 895.

upshot of this system is that, once sealed, an electronic surveillance order is likely to remain sealed long after the underlying investigation is closed, if not forever. This has been confirmed by a study of electronic surveillance orders issued by the Houston Division from 1995 through 2007. Out of 3,886 orders initially sealed “until further order of the court,” 3,877 or 99.8% were still under seal as of April 2008.³¹

The brunt of such secrecy is not necessarily borne by the surveillance targets who are ultimately charged with a crime. After all, they are entitled to discover the nature and source of the prosecution’s evidence, including electronic surveillance orders leading to arrest. Suppression motions are available in the event of a constitutional violation.³² But not everyone caught up in the web of electronic surveillance is ultimately charged with a crime. Any target is likely to call or be called by family, friends, associates, or even total strangers who have no connection to a criminal enterprise. Yet by the fortuity of a single call, these by-standers may be swept up in a criminal investigation, their cell phone use monitored and their location tracked in real time. Unlike criminal defendants, however, these presumably law-abiding citizens will never find out. The phone company cannot tell them, and courthouse records will disclose nothing. Ordinarily, a citizen whose house or office is searched is provided a warrant duly signed by a judicial officer, giving notice of the particulars of the search.³³ When a citizen wishes to challenge the legitimacy of a law enforcement search of his home pursuant to a warrant, the law affords due process for that purpose. But when searches are shrouded in permanent secrecy, as in most cases of electronic surveillance,³⁴ due process becomes a dead letter.

Such secrecy also has a pernicious impact on the judicial process of statutory interpretation. Any statute has its share of ambiguity and uncertainty, which is

³¹ See Stephen Wm. Smith, *Kudzu in the Courthouse: Judgments Made in the Shade*, 3 Fed. Cts. L. Rev. 177, 209-10 (2009) (hereafter “*Kudzu*”).

³² See *United States v. Forest*, 355 F.3d 942 (6th Cir. 2004).

³³ These procedures are specified in Rule 41, which incidentally was amended in December 2006 to cover tracking device warrants. The rule does allow for deferred notice in special circumstances.

³⁴ See *Kudzu*, *supra* at 208-211. There is also evidence of a trend toward permanent sealing of ordinary search warrants issued under Rule 41. *Id.* at 210. Until very recently, the sealing of a search warrant was regarded as an “extraordinary action” to be taken only in exceptional circumstances. See 3A Wright, King & Klein, Federal Practice and Procedure: Criminal 3D § 672, at 332-33 (2004).

resolved, case by case, through lower court rulings subject to review and correction by the courts of appeal and, ultimately, the Supreme Court. But this process of refinement and correction has not happened for ECPA. In a recent article I described this legal “black hole” for electronic surveillance orders:

Due to a peculiar combination of circumstances, these sealed orders are entirely off the radar screen, not only for the public at large, but also for appellate courts. Consider a typical pen register order. The only affected party which might have an incentive to object – the targeted e-mail customer or cell phone user – is never given prior notice of the order; in fact, the electronic service provider is usually forbidden from disclosing its existence. The provider is compensated for most expenses in complying with the order; any uncompensated inconvenience hardly justifies an appeal. The government obviously has no reason to object when its application is granted; in the rare case of a denial, why risk an appeal that could make “bad law”? There are always other magistrate judges to try.

Add a sealing order to this mix, and the outcome is a lacuna of law from which little light escapes. This is especially unfortunate because [ECPA] is fiendishly complex, made more so by the passage of the Patriot Act in 2001. Each year . . . busy magistrate judges issue hundreds of ex parte cell phone tracking orders with literally no appellate guidance concerning the proper showing for their issuance – probable cause versus something less. . . Thus, when it comes to marking the bounds of legitimate government intrusion into our electronic lives, each magistrate judge has effectively become a law unto himself. This cannot be a good thing.³⁵

The case now before the Third Circuit is the exception that proves the rule. The first appellate court decision on the proper standard for government access to cell site data will be handed down nearly a generation after ECPA was passed, and nearly a decade after its amendment by the Patriot Act. At that rate, cell site data will likely be a quaint technological memory before the next appellate court can consider it.³⁶

³⁵ *Kudzu, supra* at 211-12.

³⁶ One of the few appellate cases to deal with electronic surveillance in any respect illustrates the conundrum. *Warshak v. United States*, 532 F.3d 521 (6th Cir. 2008). The case arose after

Another consequence of this breakdown in the normal process of appellate review is “rent seeking”³⁷ on the part of prosecutors. Given the ambiguity and complexity of ECPA, reasonable judges will disagree on its application. Understandably then, prosecutors will tend to gravitate toward a judge who is known to view their requests less critically. The majority of electronic surveillance applications will thus be channeled to judges more inclined to grant them. The inevitable result of such electronic surveillance rent-seeking will be diminished privacy protection for the public as a whole. It may well be that a fully-informed public would not object to this trade-off in personal privacy for the sake of more efficient law enforcement. The problem is that, due to ECPA’s regime of secrecy, the public is not fully informed, and can be only dimly aware of the depth and breadth of electronic surveillance carried out under current law.

Possible Reforms. There are a number of ways to reduce secrecy and enhance transparency. Here are some that come to mind:

- elimination of automatic sealing for pen register orders;³⁸
- use of less restrictive techniques such as redaction of target names, phone numbers, and other identifying information;
- clear standards and duration limits for sealing and non-disclosure orders;
- clear standards and limits on the number of renewal orders;
- post-acquisition notice of tracking orders to cell phone users;³⁹
- more detailed, complete, and public reporting of electronic surveillance

a magistrate judge unsealed *ex parte* orders granting government access to plaintiff’s e-mails under the SCA. A panel of the Sixth Circuit initially held unconstitutional parts of the SCA which permitted access to e-mail without prior notice or a probable cause warrant. 490 F.3d 455, 461 (6th Cir. 2007). The panel’s decision was vacated and the case dismissed by the en banc court for lack of ripeness. Twenty-four years after ECPA, and one of its core provisions is not yet ripe for appellate review.

³⁷ I hesitate to use the term “judge shopping,” because I do not wish to imply that the AUSAs and law enforcement officers with whom I work are anything less than ethical and dedicated professionals. I would do the same in their shoes.

³⁸ Some judges question the need for any judicial role in the issuance of pen/trap orders. Under ECPA the judge’s role is a purely ministerial one of attesting to the prosecutor’s certification that the requested order is relevant to an ongoing criminal investigation.

³⁹ See FED. R. CRIM. P. 41(f)(2)(C).

orders by DOJ.⁴⁰

Other commentators have suggested extending the Wiretap Act's exclusionary rule to all types of electronic surveillance orders under ECPA, as well as enhancing civil remedies and penalties for ECPA violations.⁴¹ These ideas are also worth considering.

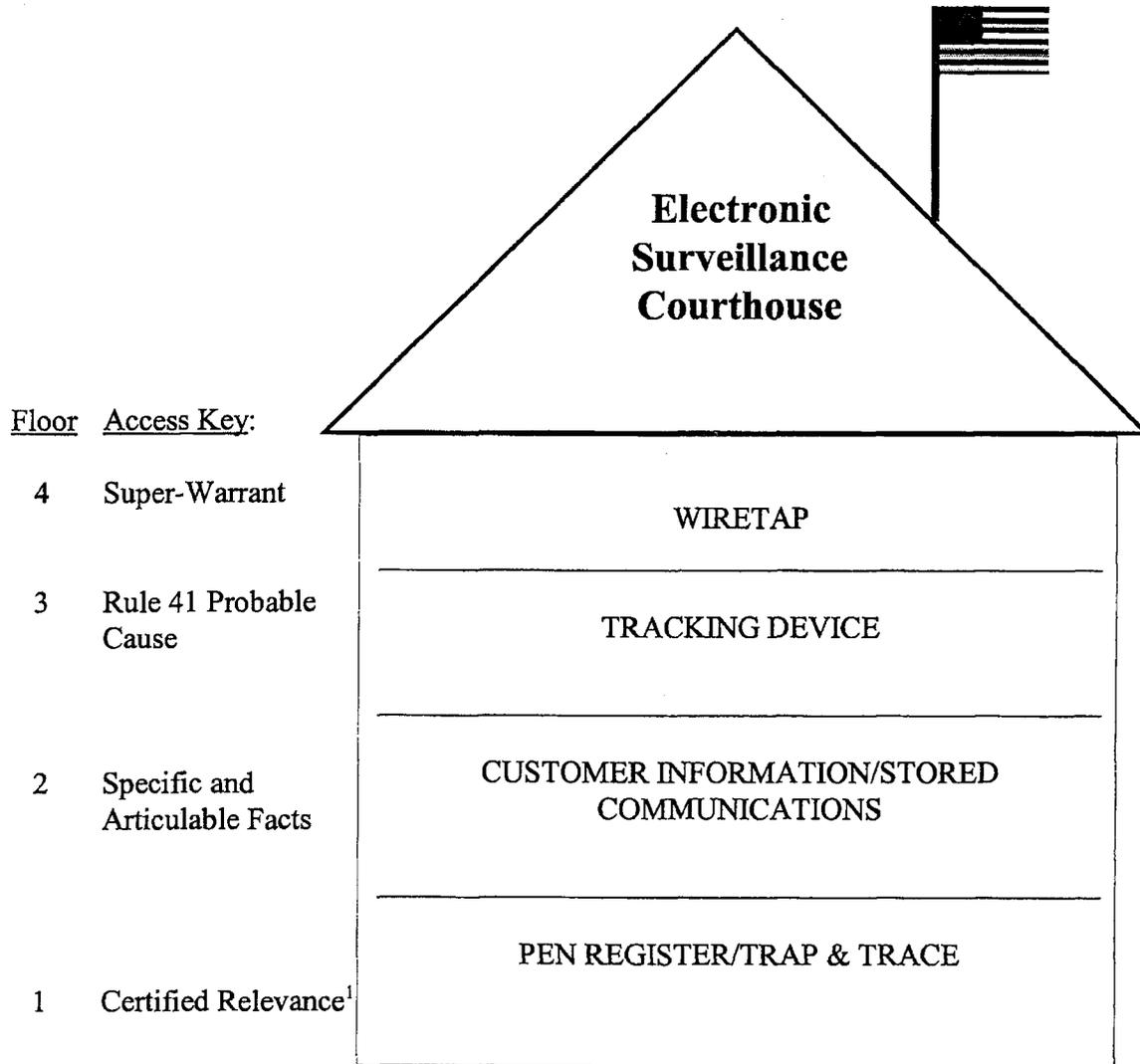
Whatever the details, the guiding principles for ECPA reform should be brighter lines and more light. Simplicity may not be entirely achievable in a statute dealing with complicated technology. Likewise, transparency is not practicable for every phase of a criminal investigation. But complexity and secrecy take hidden tolls in the form of diminished privacy protection, unchecked judicial power, and public confidence in the judicial system.⁴² The 21st century version of ECPA must recognize these dangers, and take necessary measures to avoid them.

⁴⁰ See K. Bankston, *Only the DOJ Knows: The Secret Law of Electronic Surveillance*, 41 U.S.F. L. Rev. 589, 633-34 (2007).

⁴¹ See O. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would change Computer Crime Law*, 54 Hastings L.J. 805 (2003); S. Freiwald, *Online surveillance: Remembering the Lessons of the Wiretap Act*, 56 Ala. L. Rev. 9 (2004).

⁴² See *Richmond Newspapers Inc. v. Virginia*, 448 U.S. 555, 571-72 (1980) (“[E]specially in the administration of criminal justice, the means used to achieve justice must have the support derived from public acceptance of both the process and its results. . . . People in an open society do not demand infallibility from their institutions, but it is difficult for them to accept what they are prohibited from observing.”).

EXHIBIT A



¹ Not Pictured: Administrative Subpoena
Grand Jury/Trial Subpoena
Consent
Written Request Relating to Telemarketing Fraud

EXHIBIT B
Summary of Reported Cell Site Decisions
(as of June 1, 2010)

I. Prospective Cell Site Information (CSI)

A. Applications Denied Without Probable Cause

1. Unlimited CSI (multi-tower, triangulation, GPS)

- *CSI Houston I*, 396 F. Supp. 2d 747 (S.D. Tex. Oct. 14, 2005) (Smith)
- *CSI Washington I*, 2005 WL 3658531 (D.D.C. Oct. 26, 2005) (Robinson)
- *CSI Baltimore I*, 402 F. Supp. 2d 597 (D. Md. Nov. 29, 2005) (Bredar)
- *CSI Washington II*, 407 F. Supp. 2d 132 (D.D.C. Dec. 16, 2005) (Facciola)
- *CSI Washington III*, 407 F. Supp. 2d 134 (D.D.C. Jan. 6, 2006) (Facciola)
- *CSI Fort Wayne*, 2006 WL 1876847 (N.D. Ind. July 5, 2006) (Lee, D.J.)
- *CSI Milwaukee II*, 2006 WL 2871743 (E.D. Wis. Oct. 6, 2006) (Adelman, D.J.)
- *CSI Corpus Christi*, 2007 WL 3342243 (S.D. Tex. Nov. 7, 2007) (Owsley)
- *CSI Pittsburgh*, 534 F. Supp. 2d 585 (W.D. Pa. Feb. 19, 2008) (Lenihan), *aff'd* 2008 WL 4191511 (W.D. Pa. Sep. 10, 2008) (McVerry, D.J.)

2. Limited CSI (single tower, call -related)

- *CSI New York I*, 396 F. Supp. 2d 294 (E.D.N.Y. Oct. 24, 2005) (granting reconsideration of but adhering to result reported at 384 F. Supp. 2d 562 (E.D.N.Y. Aug. 25, 2005) (Orenstein)
- *CSI Milwaukee I*, 412 F. Supp. 2d 947 (E.D. Wis. Jan. 17, 2006) (Callahan)
- *CSI New York III*, 415 F. Supp. 2d 211 (W.D.N.Y. Feb. 15, 2006) (Feldman)
- *CSI Baltimore II*, 416 F. Supp. 2d 390 (D. Md. Feb. 27, 2006) (Bredar)
- *CSI New York IV*, 2006 WL 468300 (S.D.N.Y. Feb. 28, 2006) (Peck)
- *CSI Houston III*, 441 F. Supp. 2d 816 (S.D. Tex. July 19, 2006) (Smith)
- *CSI Baltimore III*, 439 F. Supp. 2d 456 (D. Md. July 24, 2006) (Bredar)
- *CSI Puerto Rico*, 497 F. Supp. 2d 301 (D.P.R. July 18, 2007) (McGiverin, D.J.)
- *CSI New York VII*, 2009 WL 159187 (S.D.N.Y. Jan. 13, 2009) (McMahon, D.J.)

B. Applications Granted With Less Than Probable Cause

1. Unlimited CSI (multi-tower, triangulation, GPS)

No reported opinions.

2. Limited CSI (single tower, call-related)

- *CSI New York II*, 405 F. Supp. 2d 435 (S.D.N.Y. Dec. 20, 2005) (Gorenstein)
- *CSI Shreveport*, 411 F. Supp. 2d 678 (W.D. La. Jan. 26, 2006) (Hornsby)
- *CSI Charleston*, 415 F. Supp. 2d 663 (S.D.W. Va. Feb. 17, 2006) (Stanley) (granting the application to locate a non-subscriber, while rejecting the hybrid theory to locate subscribers)
- *CSI Houston II*, 433 F. Supp. 2d 804 (S.D. Tex. Apr. 11, 2006) (Rosenthal, D.J.)
- *CSI New York V*, 460 F. Supp. 2d 448 (S.D.N.Y. Oct. 23, 2006) (Kaplan, D.J.)
- *CSI Sacramento* 2007 WL 397129 (E.D. Ca. Feb. 1, 2007) (Hollows)
- *CSI Houston IV*, 622 F. Supp. 2d 411 (S.D. Tex. Oct. 17, 2007) (Rosenthal, D.J.)
- *CSI New York VI*, 632 F. Supp. 2d 202 (E.D.N.Y. Nov. 26, 2008) (Garaufis, D.J.)

II. Historical Cell Site Information

A. Applications Denied Without Probable Cause

- *CSI Fort Wayne*, 2006 WL 1876847 (N.D. Ind. July 5, 2006) (Lee, D.J.)
- *CSI Pittsburgh*, 534 F.Supp.2d 585 (W.D. Pa. Feb. 19, 2008) (Lenihan), aff'd 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008) (McVerry, D.J.). This case is currently on appeal to the Third Circuit.

B. Applications Granted With Less Than Probable Cause*

- *CSI Boston*, 509 F. Supp. 2d 76 (D. Mass Sept. 17, 2007) (Stearns, D.J.) (reversing 509 F. Supp. 2d 64 (D. Mass. July 27, 2007) (Alexander, M.J.))
- *United States v. Suarez-Blanca*, 2008 WL 4200156 (N.D. Ga. April 21, 2008) (Baverman)
- *United States v. Benford*, 2010 WL 12666507 (N.D. Ind. March 26, 2010) (Moody, D.J.)

*Note: Other decisions have granted such requests without extended discussion.