Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Wes Clark
(*wc6@georgetown.edu*)
Osher Lifelong Learning Institute (OLLI)
George Mason University

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

- 3 class sessions:
  - Session #1: wiretaps & bugs
  - Session #2: pen registers and trap & trace devices; tracking devices
  - Session #3: pole cameras & tracking cell phones

2

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

3

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Acronyms

AAG	Assistant Attorney General
AG	Attorney General
aka	also known as
ATF	Bureau of Alcohol, Tobacco, Firearms & Explosives
C.F.R.	Code of Federal Regulations
CRM	DOJ's Criminal Resource Manual
CS	Confidential source aka informant aka "snitch"
CSLI	cell site location information
DAG	Deputy Attorney General
DAAG	Deputy Assistant Attorney General
DOJ	U.S. Department of Justice
DEA	Drug Enforcement Administration
ECPA	*Electronic Communications Privacy Act*, Pub. L. No. 99-508, 100 Stat. 1848, 1860 (2000).

4

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Acronyms (cont'd)

ELSUR	Electronic surveillance
ESN	Electronic serial number
ESU	Electronic Surveillance Unit of OEO
Et seq.	And the following
Ex parte	One party only – no adverse party
FBI	Federal Bureau of Investigation
FDA	Food and Drug Administration
FISUR	Physical surveillance
FISA	*Foreign Intelligence Surveillance Act*, Pub. L. No. 95-511, 92 Stat. 1783, *as amended, codified at* 50 U.S.C. (section) § 1801 *et seq.*
FISC	Foreign Intelligence Surveillance Court
FR/Fed. Reg.	Federal Register
FRCrP	Federal Rule of Criminal Procedure

5

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Acronyms (cont'd)

ICE/HSI	Immigration & Customs Enforcement/Homeland Security Investigations
IMEI	International Mobile Equipment Identification number,
IMSI	International Mobile Subscriber Identity
LCN	La Cosa Nostra
LEA	Law Enforcement Agency
LEO	Law enforcement officer
MEID	Mobile Equipment Identification (MEID) number
OC	Organized crime
OEO	DOJ's Office of Enforcement Operations, Criminal Div.
PC	Probable cause
Pub. L. No.	Public Law Number
REP	Reasonable expectation of privacy

6

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Acronyms (cont'd)

SCA	*Stored Communications Act, i.e.,* Title II of ECPA
Stat.	Statutes at Large
Sup. Ct.	Supreme Court Reporter (Supreme Court opinions)
SW	Search warrant
Title III/TIII	Title III, *Omnibus Crime Control and Safe Streets Act of 1968*, Pub. L. No. 90-351, 82 Stat. 197, *as amended, codified at* 18 U.S.C. § 2510 *et seq.*
UFMI	Urban Fleet Mobile Identification (UFMI) number
U.S.	U.S. Reports (Supreme Court opinions)
USAM	DOJ's U.S. Attorneys' Manual
U.S.C.	U.S. Code
U.S.C.C.A.N.	U.S. Code Congressional & Administrative News
USMS	U.S. Marshals Service

7

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Acronyms (cont'd)

USPIS	U.S. Postal Inspection Service
USSS	U.S. Secret Service
§	Section
§§	Sections

8

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

- Why *Federal* law?
  - Because every state's ELSUR statutory regime can be more but not less restrictive/protective - thus Federal law is the template or at least the starting point for all state ELSUR laws.
- What kind of Federal ELSUR communication intercept regimes are there?
  - "dark" side vs. "light" side –
    - FISA vs. Title III also known as (aka) TIII – *Foreign Intelligence Surveillance Act* vs. *Title III of the Omnibus Crime Control and Safe Streets Act of 1968*

9

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

- FISA targets foreign powers/agents of foreign powers & seeks to collect "foreign intelligence information"
  - What is "foreign intelligence information?"
    - Information that relates to the ability of the United States to protect against -
      - Actual/potential attacks/grave hostile acts of a foreign power/agent of a foreign power;
      - Sabotage, international terrorism, or the international proliferation of weapons of mass destruction; or

10

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

      - Clandestine intelligence activities by an intelligence service/network of a foreign power or by an agent of a foreign power or
    - Information with respect to a foreign power/foreign power that relates to, & if concerning a United States person, is necessary to –
      - The national defense or security of the United States, or
      - The conduct of the foreign affairs of the United States.
- Whereas Title III is concerned with the collection of evidence against criminals and not generally against "spies."

11

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

- Whereas FISA proceedings & pleadings before the Foreign Intelligence Surveillance Court (FISC) are generally *CLASSIFIED*, TIII pleadings are not although they are sealed by the U.S. District Court that issues the TIII intercept order.
  - Sealing is done in order that the targets of the criminal investigation are not tipped off – so they don't flee, destroy evidence, intimidate/kill witnesses, or otherwise frustrate the investigation. It is also done to protect those innocently intercepted.
  - TIII pleadings may be "disclosed only upon a showing of *good cause*" & are kept for 10 yrs.
  - TIII pleadings are presented to the judge *ex parte* by the Federal prosecutor.

12

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

- Where can I find *Federal* law?

13

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

- Where can I find *Federal* law?
  - Statutes at Large (Stat.)
    - Published sequentially from the beginning of each numbered Congress, *e.g.*, Public Law Number (Pub. L. No.) 95-111, 92 Statutes at Large (Stat.) 1783 (page no.) – the 111th law passed by the 95th Congress and found at p. 1783 in vol. 92 Stat.
    - https://www.loc.gov/law/help/statutes-at-large/ (*accessed* 2/20/17)
  - United States Code (U.S.C.)
    - Takes the differing topic areas found dispersed in each of the public laws and arranges them by 50 easier-to-find subject areas. Thus, the U.S. Code has 50 titles. For example, many Federal criminal laws are found in Title 18. Many drug laws, including those that are criminal in nature, are in Title 21. National defense-related laws are often in Titles 10 and 50.

14

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

- United States Code (U.S.C.) – cont'd
  - Found in all law libraries in the U.S. to include the Fairfax County Law Library, Fairfax County Courthouse, 4110 Chain Bridge Road, Suite 115, Fairfax, VA 22030; 703-246-2170.
  - U.S.C. – which is regularly updated – is often the preferable research tool because one doesn't have to track down any statutory changes in subsequent Pub. L. No./Statutes at Large.
  - http://uscode.house.gov (*accessed* 2/20/17)
- Legislative history – Senate & House Reports; Senate/House Conference Reports.
  - Many are published in U.S. Code Congressional & Administrative News (U.S.C.C.A.N.) – a Thomson Reuters product.

15

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

- Code of Federal Regulations (C.F.R.)
  - Binding rules promulgated by the Federal agency with subject matter jurisdiction – arranged by category titles mirroring those of the U.S.C. - that implement the nation's public laws. For example, Title 21 C.F.R. will contain many of the rules affecting drugs that are promulgated by the Drug Enforcement Administration (DEA) and the Food and Drug Administration (FDA).
  - Many rules require public notice and comment before issuance.

16

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

- Code of Federal Regulations (C.F.R.) – cont'd
  - https://www.gpo.gov/fdsys/browse/collectionCfr.action?collectionCode=CFR (*accessed* 4/17/17)
- Federal Rules of Criminal Procedure (FRCrP)
  - Binding rules governing criminal pre-trial and criminal trial matters. For example, FRCrP 6 governs Federal grand juries and FRCrP 41 treats Federal search warrants.
    - https://www.federalrulesofcriminalprocedure.org/ (*accessed* 4/17/17)

17

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

- Federal Register (Fed. Reg. or FR)
  - Published daily – often contains public notice of rules that are proposed to be forthcoming in the C.F.R. as well as agency final rules that will be incorporated into the next year's publication of the appropriate subject matter C.F.R. title.
  - The FR also announces requests for public comment on proposed rules.
  - https://www.federalregister.gov/ (*accessed* 4/17/17)
- U.S. Department of Justice (DOJ) policy
  - U.S. Attorney's Manual (USAM) - https://www.justice.gov/usam/united-states-attorneys-manual (*accessed* 4/17/17)
  - DOJ Criminal Resource Manual (CRM) - https://www.justice.gov/usam/criminal-resource-manual (*accessed* 4/17/17)

18

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

- More on finding Federal law –
  - Court decisions aka caselaw:
    - Supreme Court
      - United States Reports; Supreme Court Reporter (Thomson Reuters); United States Supreme Court Reports, Lawyers' Edition (LexisNexis)
    - U.S. Courts of Appeal
      - Federal Reporter, 3d & Federal Appendix (Thomson Reuters)
    - U.S. District Courts – U.S. District Court Judges & U.S. Magistrate Judges.
      - Federal Supplement, 2d (Thomson Reuters)
    - Westlaw & LexisNexis

19

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

- Where can I find FISA and TIII law?
  - FISA: Pub. L. No. 95-511, 92 Stat. 1783, *as amended, codified at* 50 U.S.C. (section) § 1801 *et seq.*
  - TIII: Pub. L. No. 90-351, 82 Stat. 197, *as amended, codified at* 18 U.S.C. § 2510 *et seq.*
- *We will be discussing non-CLASSIFIED* ELSUR

20

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

21

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III

- 18 U.S.C. § 2510 definitions:
  - Wire communication – "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 . . . ." (telephone calls)
  - Oral communication – "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation . . . aka "reasonable expectation of privacy" or REP (face-to-face conversations)

22

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III

- 18 U.S.C. § 2510 definitions (cont'd):
  - Electronic communication – "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire . . . that affects interstate or foreign commerce, but does not include – any wire or oral communication (*e.g.*, text messages, emails, & faxes)
  - Intercept – "the aural or other acquisition of the contents of any wire, electronic, or oral communications through the use of any electronic, mechanical, or other device."
  - Judge of competent jurisdiction – "judge of a United States *district court* or a United States court of appeals" – 94 district courts & 13 circuit courts of appeal.

23

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III

- 18 U.S.C. § 2510 definitions (cont'd):
  - Aural transfer – "a transfer containing the human voice . . . ."
- 18 U.S.C. § 2511 – interceptions that are crimes
  - "Except as otherwise specifically provided in [Title III] *any person* who intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . . shall be punished [generally a fine and up to 5 years imprisonment]."

24

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III

- 18 U.S.C. § 2511(2)(c) & (d) – **consensual** intercepts:
  - It isn't unlawful "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 his prior consent to such interception."
  - It isn't unlawful "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 one of the parties to the communication has given his prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act . . . ."
    - "Candid Camera" Loni Anderson example

25

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III

- 18 U.S.C. § 2516 – who may authorize a Federal prosecutor to seek a TIII order from a U.S. District Court Judge?
  - Attorney General (AG), Deputy Attorney General (DAG), Associate Attorney General, any Assistant Attorney General (AAG), any Acting AAG, and (except for **roving** intercepts) any *Deputy AAG* (or Acting DAAG) in the *Criminal Division* specially designated by the AG "may authorize" that a TIII application be made to a "Federal judge of competent jurisdiction" and such judge may grant a TIII order approving the interception of wire or oral communication by the FBI "or a Federal agency having responsibility for the offense as to which application is made."
  - Note absence of "interception of electronic communication."

26

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III

- 18 U.S.C. § 2516(3) – (a) who may authorize a Federal prosecutor to seek a TIII order from a U.S. District Court Judge for the interception of *electronic* communications, (b) for which Federal offenses may the intercept orders be granted, and (c) for which type of Federal offenses may the intercept orders be had?
  - "Any [Federal prosecutor] may authorize an application . . . for an order authorizing or approving the interception of *electronic* communications . . . when such interception may provide or has provided evidence of any Federal felony."
    - However, as a matter of policy DOJ requires that its approval be secured before application is made to conduct the non-consensual interception of electronic communications. USAM 9-7.100.

27

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III

- What documents does a Federal prosecutor submit to a U.S. District Court Judge for his/her consideration?
  - (a) an application for the TIII order, (b) a supporting affidavit signed under oath by a Federal law enforcement officer (LEO)/ deputized state/local LEO, (c) a proposed TIII order, (d) a copy of the DAAG's faxed authorization to seek the TIII order, &, as appropriate, (e) a copy of the most recent AG order designating the DAAG/Acting DAAG.
  - What Federal LEOs are authorized to submit a TIII supporting affidavit?
    - FBI, DEA, ICE/HSI, ATF, USSS, USMS, USPIS, Federally deputized state/local LEO.
      - 29 CRM – DOJ Criminal Division policy.

28

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III

- Can a TIII be used to gather evidence concerning <u>*any*</u> Federal offense?
  - No, and except for the interception of *electronic* communications, the crime must be specified/listed in 18 U.S.C. § 2516(1)
    - Initially the listed offenses were characteristic of organized crime (OC) aka Mafia aka La Cosa Nostra (LCN) but over time the list has been expanded to encompass most serious Federal crimes.
      - *E.g.,* 18 U.S.C. § 2516(1)(e) covers "any offense involving . . . 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."

29

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

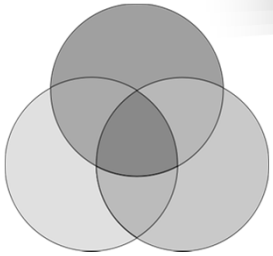
Title III

- What *kinds* of evidence and what *quantums* of evidence must the TIII application & affidavit contain?
  - <u>3 kinds</u> of <u>probable cause (PC)</u>:
    - (a) that the intercept targets are committing, have committed, or are about to commit a TIII predicate offense,
      - Recall: there is no laundry list of TIII predicate offenses with respect to ***electronic*** communications – all that's needed is <u>**any**</u> Federal <u>**felony**</u>.
    - (b) that they are communicating about it (PC "for belief that particular communications concerning [the] offense will be obtained"), &
    - (c) that they are communicating/will be communicating over or at the facilities where you want to conduct the intercept.

30

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III



31

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III

- But what is "probable cause?"
  - *Black's Law Dictionary:* "the facts must be such as would warrant a belief by a reasonable [person] – more than a bare suspicion but less than evidence that would justify a conviction"
    - *Greater than* the lesser standard of "reasonable suspicion" (which is the benchmark for a "stop & frisk") but *lesser than* the conviction test of "proof beyond a reasonable doubt."
    - PC must be based upon "reasonably trustworthy information."
      - As an example, if the LEO's PC is based upon informant/confidential source (CS) information, ask: 1) how reliable is the CS (his/her track record), and 2) what is the CS' basis of knowledge, *i.e.*, did the CS personally see/hear or was it rank rumor overheard in a bar?

32

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III

- What *kinds* of evidence and what *quantums* of evidence must the TIII application & affidavit contain? (cont'd)
  - Besides the 3 types of PC that must be demonstrated in a TIII application & affidavit, the pleadings must also show –
    - "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous."
      - Note: this is not a PC standard!
    - A TIII does not, however, have to be the investigative technique of absolute last resort.

33

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III

- What *kinds* of evidence and what *quantums* of evidence must the TIII application & affidavit contain? (cont'd)
  - Explanations of why other investigative methods are insufficient –
    - Physical surveillance (FISUR), although valuable at times, cannot reveal the full scope of the conspiracy nor the identities of all of the co-conspirators; further, it can be noticed and cause the wrongdoers to become more cautious in their illegal activities to include the use of counter-surveillance driving techniques. Additionally, the nature of the neighborhood (cul-de-sac, close-knit community, etc.) would make FISUR obvious.
    - Grand jury subpoenas by themselves will not uncover the full details of the targets' criminal activities because the principals will most likely invoke their 5th Amendment privilege not to testify. Service of the subpoenas will also tip off the targets of the investigation.

34

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III

- What *kinds* of evidence and what *quantums* of evidence must the TIII application & affidavit contain? (cont'd)
  - Explanations of why other investigative methods are insufficient (cont'd)–
    - CSs, although their information may help support the TIII application & affidavit, may not have direct contact with mid- or high-level targets; they may also decline to testify before grand juries or at trial for fear of personal or family safety. Further, CSs by themselves may not know the identities of all of the co-conspirators and their roles in the criminal syndicate.
    - Undercover agents (UCAs) may simply be unable to penetrate the upper levels of a conspiracy. For example, the law enforcement agency (LEA) may not have UCAs of the ethnicity to infiltrate a particular criminal organization, *e.g.*, a Chinese triad.

35

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III

- What *kinds* of evidence and what *quantums* of evidence must the TIII application & affidavit contain? (cont'd)
  - Explanations of why other investigative methods are insufficient (cont'd)–
    - Interviews of subjects/associates Although useful, such interview subjects may not know the full details of the conspiracy's inner workings, locations of cash, documents, computers, drugs, weapons, other contraband, money laundering methods, etc. Further, and without the threat of perjury, subjects/associates may well lie to the LEA such that it may divert investigative resources & unproductively pursue false leads. Additionally, conducting interviews at this stage of the investigation would tip off the targets.
    - Search warrants These are most useful at the *conclusion* or *take down* stage of an investigation, not in the midst of it which, unfortunately, would only serve to prematurely alert the "bad guys" causing them to become more secretive, flee, move/destroy evidence, etc.

36

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III

- What *kinds* of evidence and what *quantums* of evidence must the TIII application & affidavit contain? (cont'd)
  - Explanations of why other investigative methods are insufficient (cont'd)–
    - Tolls records, pen registers, trap & trace "devices"
      - Toll records document outgoing long-distance "toll" telephone calls. Today, however, with bundled TV, Internet, and telephone service commonly offered by service providers, there are no extra charges for calls that used to be considered to be "long distance" or so-called "toll" calls.
      - *Although we will cover pen registers as well as trap & trace "devices" in more detail later*, suffice it to say now that "pens" document outgoing telephone calls while trap & traces reveal incoming calls.
      - While pens, trap & traces, and tolls are useful, they don't reveal the identities of the conversants, their roles in the criminal organization, the conspiracy's details, nor can they distinguish between innocent and calls that are criminal in nature.

37

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III

- What *kinds* of evidence and what *quantums* of evidence must the TIII application & affidavit contain? (cont'd)
  - Explanations of why other investigative methods are insufficient (cont'd)–
    - Courts *frown* upon mere "boilerplate" recitations of why techniques other than a TIII are insufficient.
    - The examples must be tied into the particularities/characteristics of the investigation for which the TIII is being sought.

38

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III

- What if the target switches *personally identifiable* cell phones during the course of the authorized intercept period?
  - The application & order should specify that the intercept authorization also apply to changes in one of several possible identifying numbers such as –
    - Electronic serial number (ESN),
    - International Mobile Subscriber Identity (IMSI),
    - International Mobile Equipment Identification (IMEI) number,
    - Mobile Equipment Identification (MEID) number,
    - Urban Fleet Mobile Identification (UFMI) number, or
    - Any changed telephone number when the other identifying number remains the same.

39

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III

- What if the target is known to keep –
  - Changing the locations where s/he meets confederates and at the time you submit your TIII application, you cannot specifically identify the premises where the listening device ("bug") will be installed?
  - Or routinely uses a "burner" cell phone disposing of it every few days and you cannot specifically describe/identify the phone to be intercepted?
  - Seek a **"ROVING"** intercept TIII order, 18 U.S.C. § 2518(11)(a), (b).
    - *Note:* DOJ authorization from higher level officials required for a roving: AG, DAG, Associate AG, AAG, or Acting AAG.
    - *Bug:* application to state why specific identification of premises is not "practical;"
    - *Wiretap:* PC showing required that intercept target's "actions could have the effect of *thwarting* interception from a *specified* facility."

40

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III

- More on *roving* TIIIs –
  - *Bugs:* interception cannot begin until "the place where the communication is to be intercepted is ascertained by the person implementing the interception order."
  - *Wiretaps:* interception is limited "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."
  - 18 U.S.C. § 2518(11) & (12).

41

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III

- Does the District Court's TIII order do anything other than approve the intercept/overhear?
  - Yes, if a wire or electronic communication intercept, it directs the service provider to forthwith "furnish . . . all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively . . . . Any provider of wire or electronic communication service . . . shall be compensated . . . for reasonable expenses incurred in providing such facilities or assistance."
  - If a bug, the order will typically permit surreptitious break-ins to install, maintain, and remove the device(s). The application should specifically ask for this authority.
    - *Note:* either the target phones/bug locations have to be within the court's judicial district or the "wire room" has to be. However, if a bug is in a vehicle, the intercept has only to be within the U.S.

42

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III

- Does the District Court's TIII order do anything other than approve the intercept/overhear? – (cont'd)
  - "Gags" the service provider and, if a bug, the landlord/custodian: "No [service] provider or wire or electronic communication service . . . or landlord, custodian . . . shall disclose the existence of any interception or surveillance with respect to which the person has been furnished a court order . . . . 18 U.S.C. § 2511(2)(a)(ii).
  - *Importantly*, directs the LEA to "minimize" in *real time* the interception of non-pertinent communications, *i.e.*, conversations that are legally privileged *(e.g.*, attorney-client) or non-criminal in nature.
    - Exception to *real time* minimization: if communications are in *code* or in a *foreign language* for which an interpreter is not reasonably available, minimization can be conducted after-the-fact.

43

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III

- Does the District Court's TIII order do anything other than approve the intercept/overhear? – (cont'd)
  - Will direct periodic progress reports to the court, usually at 10-day intervals.
    - Since the Federal prosecutor writes the application & order, s/he can specify the interval between progress reports.
    - If you aren't getting "pertinent" conversations, provide a good explanation or the judge can shut down the intercept operation.

44

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III

- Does the District Court's TIII order do anything other than approve the intercept/overhear? – (cont'd)
  - It specifies the *intercept period* – normally the statutory maximum of 30 days!
    - No TIII order may authorize interception for "a period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days."
    - Assuming continuing PC, an unlimited number of 30-day extensions can be had.
    - Typically the 30 days begins to run the day after the judge signs the order but an even more prudent computation is to begin counting 24 hr. increments from the moment when the judge signs the order.
    - The LEA can't "sit" on an approved TIII order – the 30 days starts to run when intercept operations begin but no later than 10 days after the order is entered.

45

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III

- What happens after the TIII intercept concludes?
  - Not later than 90 days, the Federal prosecutor serves an *inventory* "on the persons named in the order or application, and such other parties to intercepted communications as the judge may determine."
  - The *inventory* is to specify –
    - "the fact of the entry of the [TIII intercept] order or the application;"
    - "the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and"
    - "the fact that during the period wire, oral, or electronic communications were or were not intercepted."
  - *Inventory* service can be postponed "on an *ex parte* showing of good cause."

46

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III

- What happens after the TIII intercept concludes? (cont'd)
  - The "tapes," *i.e.,* digital media, are sealed under the judge's direction & kept wherever the judge directs – usually with the intercepting LEA.
  - Kept for at least *10 years* and destroyed only upon an order of the issuing judge.
  - Typically the intercepting LEA will simultaneously record more than one original "tape" – one to be sealed by the court and another (a "duplicate original") with which the LEA works in furtherance of the investigation, trial preparation, to provide discovery, to prepare transcripts, etc.

47

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III

- Since the TIII pleadings and "tapes" are sealed, how can law enforcement make use of the intercepted communications without violating the court's sealing order?
  - LEOs *may disclose* TIII intercept contents/derivative evidence "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."
  - LEOs *may disclose* TIII intercept contents/derivative evidence "while giving testimony under oath or affirmation."
  - LEOs *may disclose* TIII intercept contents/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."

48

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III

- Since the TIII pleadings and "tapes" are sealed, how can law enforcement make use of the intercepted communications without violating the court's sealing order? (cont'd)
  - LEOs may *use* TIII intercept contents/derivative evidence "to the extent such use is appropriate to the proper performance of his official duties."
- What if the TIII memorializes *evidence of non-TIII predicate offenses*?
  - If such evidence is to be disclosed via testimony under oath or affirmation, it may be done so only if authorized/approved by a district court judge where s/he finds "on subsequent application" that the contents of the intercept were "otherwise" acquired in accordance with the requirements of TIII.
    - In other words, there cannot have been shenanigans to circumvent the TIII "laundry list" predicate offense requirement.

49

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III

- How do TIII application packets even get to the DAAG, Criminal Division?
  - They all are submitted to and screened by the Division's quality control "gatekeeper," the Electronic Surveillance Unit (ESU) of the Office of Enforcement Operations (OEO).
  - To my knowledge, no District Court Judge has ever denied a TIII application because the TIII packages are simply that good after having been scrubbed/vetted by the ESU.
    - If the application package is a poor one, the ESU will take the position that it cannot be passed along to the DAAG.
    - Should a deficient one nevertheless get past DOJ and the District Court Judge express skepticism, the Federal prosecutor will most likely simply withdraw the application rather than suffer a formal denial.

50

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III

- Does the OEO/ESU have requirements the field must satisfy in addition to those required by statute/TIII?
  - Yes, the TIII affidavit "must demonstrate criminal use of the target facility [*e.g.*, a phone] or premises within ***six months*** from the date of Department approval." 29 CRM.
  - Additionally, "the affidavit must also show recent use of the facility or premises within ***21 days*** from the date on which the Department authorizes the filing of the application." 29 CRM.
  - "The date range for all pen register/phone records data must be updated to within ***10 days*** of submission to OEO." 29 CRM.
  - For wire/electronic communication *extension* TIIIs, the affidavit "should include" direct quotes "including one from within ***seven days*** of Department approval" or an explanation why not. 29 CRM.

51

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Title III

- TIIIs by the numbers:
  - 1991: OEO reviewed 600 TIII requests.
  - 2005: OEO reviewed over 2,700 such requests.
  - 2015: 4,148 TIIIs authorized (Federal & state, roughly ⅔ of those were at the state level)
    - 94% were for *telephone* taps & most of those were for cell phones.

52

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Pen Register/Trap & Trace

53

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Pen Register/Trap & Trace

- 18 U.S.C. §§ 3121-3127 –
  - No interception of communication *contents!* That's what TIII is for. Intercepting outgoing and incoming *digits* not as intrusive as acquiring actual conversations.
- *Pen register*: "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." 18 U.S.C. § 3127(3). Real time data.
- *Trap & trace*: "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." 18 U.S.C. § 3127(4). Real time data.

54

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Pen Register/Trap & Trace

- Why no FRCrP 41 search warrant?
  - *Smith v. Maryland,* 442 U.S. 735 (1979): Question: does the installation and use of a pen register constitute a search within the meaning of the 4th Amendment?
  - Looking to earlier Supreme Court precedent, Justice Blackmun writing for the Court noted that the correct test was whether the person seeking the protection of the 4th Amendment "can claim a *justifiable, a reasonable, or a legitimate expectation of privacy* that [was] invaded by government action." The test has two parts:
    - Did the suspect "exhibit an actual (subjective) expectation of privacy" and,
    - If so, was that expectation "one that society is prepared to recognize as reasonable."

55

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Pen Register/Trap & Trace

- *Smith v. Maryland,* 442 U.S. 735 (1979) (cont'd) –
  - "Even if [Smith] did harbor some *subjective expectation* that the phone numbers he dialed would remain private, this *expectation is not one that society is prepared to recognize as reasonable*. This Court has consistently held that a person has no legitimate expectation of privacy in *information he voluntarily turns over to third parties*."
  - "When he used his phone, [Smith] voluntarily conveyed numerical information to the telephone company and 'exposed' that information . . . . In so doing, [Smith] *assumed the risk* that the company would reveal to police the numbers he dialed."
  - Consequently the *installation and use of the pen register was not a "search"* as contemplated by the 4th Amendment hence no warrant was required.

56

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Pen Register/Trap & Trace

- 18 U.S.C. §§ 3121-3127 (cont'd)
  - The statute requires only that the Federal prosecutor make a "**certification**" under oath or affirmation to a "court of competent jurisdiction" to *include* a U.S. Magistrate Judge (contrast this with a TIII) that "the ***information likely to be obtained is relevant*** to an ongoing investigation."
  - Upon such a "certification" the court "shall enter an *ex parte* order authorizing installation and use of the pen/trap & trace *anywhere within the United States* (contrast this with a TIII).
  - Order, which is sealed, is valid for **60 days** with 60 day extensions permitted.
  - Service provider is gagged – "shall not disclose the existence of the pen register or trap and trace device or existence of the investigation to the listed subscriber, or to any other person."

57

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Pen Register/Trap & Trace

- Related "tool" for obtaining a record of *past* telephone calls:
  - Grand jury (FRCrP 17), administrative *(e.g.,* 21 U.S.C. § 876), or trial subpoenas (FRCrP 17).
    - Often, administrative subpoenas are a preferred option because the records they obtain are not arguably governed by FRCrP 6 relating to grand jury secrecy.

58

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Devices aka Beepers

59

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Devices aka Beepers

- 18 U.S.C. § 3117 & FRCrP 41
  - § 3117: a "tracking device" is "an electronic or mechanical device which permits the tracking of the movement of a person or object."
  - § 3117 (cont'd): "If a court is empowered to issue a warrant . . . for the installation of a mobile tracking device, such order may authorize the *use* of that device within the jurisdiction of the court, and *outside that jurisdiction* if the device is installed in that jurisdiction."
  - FRCrP 41: U.S. Magistrate Judge empowered to issue a warrant to "*install* within the district a tracking device; the warrant may authorize use of the device to track the movement or a person or property within the district, *outside* the district, or both."

60

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Devices aka Beepers

- 18 U.S.C. § 3117 & FRCrP 41
  - FRCrP 41 (cont'd): A tracking device warrant must "specify a reasonable length of time that the device may be used. The time may *not exceed* ***45 days*** from the date the warrant was issued" with the option for one or more *45 day* extensions for *good cause* shown.
    - Any *installation* authorized by the warrant must be completed within a specified time not to exceed *10 days;*
    - And be completed in the *daytime* unless *good cause* is shown.
  - Within *10 days* after the tracking has ended, a copy of the warrant must be served "on the person who was tracked or whose property was tracked."
    - But won't this tip off the "bad guy?"
  - The court may *delay* that notice "if the delay is authorized by statute."

61

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Devices aka Beepers

- "Sneak & peek" search warrant (SW) statute:
  - 18 U.S.C. § 3103a: "With respect to the issuance of any warrant . . . or any other rule of law, to search for and seize any property or material . . . any notice required . . . to be given *may be delayed* if –
    - The court finds *reasonable cause* to believe that providing immediate notification . . . may have an adverse result;
    - The warrant provides for the giving of such notice within a *reasonable* period of its execution, which period may thereafter by extended by the court for *good cause* shown."
  - 18 U.S.C. § 2705(a)(2) defines "adverse result:" (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."

62

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Devices aka Beepers

- But do you even need a warrant to *install* and *use* a tracking device?
- Caselaw: *U.S. v. Knotts*, 460 U.S. 276 (1983)
  - "monitoring" aka *use* case
    - Device installed inside 5 gal. chemical drum;
    - Consent of chemical chloroform manufacturer;
    - Subsequent pick-up by purchaser/bad guy;
    - Drum transported by vehicles on public roads;

63

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Devices aka Beepers

- *U.S. v. Knotts*, 460 U.S. 276 (1983)(cont'd)
  - Drum stopped at bad guy's lake cabin;
  - SW successfully executed, drum retrieved (outside cabin), fully operable meth lab inside cabin.
    - No REP for drum movements outside the cabin in "open fields."
  - Defendant: Device installation OK, but monitoring violated sanctity of residence!!!

64

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Devices aka Beepers

- *U.S. v. Knotts*, 460 U.S. 276 (1983)(cont'd)
  - Supremes: "A person travelling in an automobile on public thoroughfares has no REP in his movements from one place to another."
  - Diminished expectation of privacy in an automobile "because its function is transportation and it seldom serves as one's residence or as a repository of personal effects. . . . It travels public thoroughfares where both its occupants and its contents are in plain view."

65

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Devices aka Beepers

- *U.S. v. Knotts*, 460 U.S. 276 (1983)(cont'd)
  - Supremes: No "expectation of privacy extended to the visual observation of [the] automobile arriving on his premises after leaving a public highway, nor to movements of objects such as the drum of chloroform outside the cabin in 'open fields.'"
  - "Visual surveillance from public places along [the driver's] route or adjoining [the owner's] premises would have sufficed to reveal all of these facts to the police."

66

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Devices aka Beepers

- *U.S. v. Knotts*, 460 U.S. 276 (1983)(cont'd)
  - Supremes: No invasion of legitimate expectation of cabin owner's privacy.
  - Device did not provide "information as to the movement of the drum within the cabin, or in any way that would not have been visible to the naked eye from outside the cabin."

67

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Devices aka Beepers

- *U.S. v. Karo*, 468 U.S. 705 (1984) – *installation* the key issue.
  - DEA puts device into a can of its ether; CS-supplier permits DEA to substitute its can for one of his.
    - Supremes: No search or seizure occurred with device installation and transfer of device-equipped ether can to Karo.
  - Device monitoring revealed ether can traveled on roads and came to rest inside house rented by bad guys.

68

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Devices aka Beepers

- *U.S. v. Karo*, 468 U.S. 705 (1984) (cont'd)
  - *Issue:* does monitoring device in a private residence, a location not open to visual surveillance, violate the 4th Amendment?
  - Supremes: Yes.
    - "[W]ithout a warrant, the Government surreptitiously employ[ed] an electronic device to obtain information that it could not have obtained by observation from outside the curtilage of the house."

69

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Devices aka Beepers

- *Issue:* What the heck is a *curtilage?*
  - "[T]he area to which extends the intimate activity associated with the 'sanctity of a man's home and the privacies of life.'"
  - An area considered to part of the "home" for Fourth Amendment purposes.

70

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Devices aka Beepers

- But Justice Scalia upended tracking device law throwing a *curve* in *U.S. v. Jones*, 132 S.Ct. 945 (2012).

  - A GPS tracker was surreptitiously placed onto a Jeep (registered to Jones' wife) while the vehicle was in a public parking lot; the device was then monitored as the Jeep drove on public streets.

71

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Devices aka Beepers

- *U.S. v. Jones,* 132 S.Ct. 945 (2012) (cont'd)
  - Although the LEOs got a SW from the U.S. District Ct. in DC, it was to be executed within 10 days. LEOs didn't install it until the 11th day and in Maryland – so it was, effectively, a warrantless *installation* and *use.*
  - Based in part on the GPS data, Jones was indicted for several drug distribution offenses and moved to suppress the GPS evidence.
  - The U.S. District Court granted the motion in part, suppressing the GPS data obtained while the vehicle was parked in the garage adjoining Jones' residence but not GPS information obtained while the vehicle was on the roads.
  - Relying on *Knotts,* the court ruled that "a person traveling in an automobile on public thoroughfares has no REP in his movements from one place to another."

72

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Devices aka Beepers

- *U.S. v. Jones*, 132 S.Ct. 945 (2012) (cont'd)
  - The U.S. Court of Appeals for the DC Circuit reversed holding that the entirety (*installation* and *use*) of the GPS surveillance violated the 4th Amendment.
  - The Supreme Court agreed, holding that both the *installation* and *use* constituted a search.
  - What happened to the argument that there is no REP with respect to a vehicle's movement on public roads?
  - Justice Scalia, writing for the Court, stressed that although the 4th Amendment was concerned with the REP, it was also grounded on the property-based concept of ***trespass***.

73

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Devices aka Beepers

- *U.S. v. Jones*, 132 S.Ct. 945 (2012) (cont'd)
  - Justice Scalia distinguished *Karo* noting that the facts in that case showed that the tracking device was installed *before* the container came into Karo's possession. Karo assumed the risk!
  - "By attaching the device to the Jeep, officers encroached on a protected area."
  - The judgment of the U.S. Court of Appeals for the DC Circuit is *affirmed*.

74

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Pole Cameras

75

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Pole Cameras

- Strictly 4th Amendment/search & seizure law!
- What is a **pole camera**?
  - A LEA puts a *video-only* camera on a utility pole.
  - What if the suspect has a *fence* around his/her property? Does s/he have a REP?
  - But isn't the LEA seeing only what a utility worker on the pole would see?
  - And the Supreme Court has previously ruled that police may make observations & take photos from publicly navigable airspace.

76

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Pole Cameras

- *United States v. Houston,* 813 F.3d 282 (6th Cir. 2016)
  - Convicted felon Rocky Houston lived on a farm posted with signs critical of government and depicting the dead bodies of a LEO and his companion. Rocky and his brother lived on the Houston family farm consisting of 3 adjacent properties. Rocky lived in a red brick building and his brother lived in a trailer.
  - Although the property wasn't fenced, blue tarps blocked views of the trailer's doors and foliage initially blocked views of Rocky's house.
  - The local sheriff told the ATF that Rocky was in *open possession of firearms* at his residence.

77

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Pole Cameras

- *United States v. Houston,* 813 F.3d 282 (6th Cir. 2016)(cont'd)
  - ATF tried to do drive-by surveillance but as one agent said, their vehicles stood out "like a sore thumb" in the rural area.
  - Solution? **Pole camera!** *Without a warrant*, the utility company installed it on a public pole about 200 yds. from the trailer. It could move left, right, and zoom. An agent testified that the camera saw the same thing to what agents would have observed "if they had driven down the public roads surrounding the farm." The camera was in operation for 10 weeks.
  - When search warrants were served, 25 weapons were recovered!

78

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Pole Cameras

- *United States v. Houston,* 813 F.3d 282 (6th Cir. 2016)(cont'd)

  - At trial, Rocky moved to suppress the video evidence. Too bad, so sad – he was convicted and sentenced to 108 months.

79

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Pole Cameras

- The 6th Circuit affirmed:
  - "There was no Fourth Amendment violation, because [Rocky] had *no REP in video footage recorded by a camera that was located on top of a public utility pole* and that captured the same views enjoyed by passersby on public roads."
  - "Additionally, the *length of the surveillance* did not render the use of the pole camera unconstitutional, because the Fourth Amendment does not punish law enforcement for using technology to more efficiently conduct their investigations."
  - Noting the **blue tarps** and quoting from one of the Supreme Court's aerial observation cases, the 6th Circuit observed that "the mere fact that an individual has taken measures to restrict some views of his activities does not preclude an officers' observations from a public vantage point where he has a right to be."
  - Contrast *United States v. Cuevas-Sanchez*, 821 F.2d 248 (5th Cir. 1987).

80

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Pole Cameras

- Although video-only surveillance is not covered by Title III, some of its requirements have been borrowed/mandated by six circuits where such ELSUR involves a REP: The 2nd, 5th, 7th, 8th, 9th, and 10th Circuits.
- Accordingly DOJ advises (32 CRM and USAM 9-7.200) that a SW be sought relying on both FRCrP 41 and the *All Writs Act* (28 U.S.C. § 1651) when such REP-implicated video-only surveillance is contemplated.
- DOJ Criminal Division approval also required in REP situations:
  - AAG, DAAG, OEO Director, OEO Associate Director

81

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Cell Phones

82

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Cell Phones

- Do you think Federal criminal investigators need a search warrant to track your phone's movements?
- Do you have an REP with respect to your cell phone's locations?
- Is the cell phone on your person or was it in the past? Are you and your phone in a residence, in a vehicle being operated on a public road, or are you carrying your phone while walking down Pennsylvania Avenue in DC? Did you leave your cell phone in a suitcase/briefcase that is now traveling without you?
- Is the LEA seeking the phone's *past* locations or its *prospective* location in *real time?*
- Is the LEA seeking CSLI or GPS location information?

83

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Cell Phones

- Courts have been referring to cell phone location data as determined by triangulation achieved by using signal strength and direction from cell towers as "cell site location information" or CSLI. This is different from GPS data.
  - "CSLI is a record of non-content-based information from the service provider derived from 'pings' sent to cell sites by a target phone. CSLI allows the target phone's location to be approximated by providing a record of where the phone has been used." *U.S. v. Lambis,* 197 F. Supp.2d 606 (S.D.N.Y. 2016).

There is no statute which, by its language, *specifically* deals with the tracking of cell phones by LEAs.

84

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Cell Phones

- Thus, the law in this area is developing through court decisions.
- Although no statute specifically addresses the tracking of cell phones, remember 18 U.S.C. § 3117: a "tracking device" is "an electronic or mechanical device which permits the tracking of the movement of a person or object."
- Unless the LEA uses a cell site simulator, *e.g.,* a Stingray, cell phone location information has to be obtained from a service provider (AT&T, Verizon, T-Mobile, Sprint, etc.) and this normally requires a court order. But what would be the statutory or Constitutional basis for such an order?
- In the mid- to late- 2000s DOJ used a combination of two statutes (a so-called "hybrid" theory) to obtain *real time/prospective* cell phone location information:

85

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Cell Phones

- Part of the *Electronic Communications Privacy Act* (ECPA), primarily 18 U.S.C. § 2703(d), together with the pen register/trap & trace (pen/trap) statute, 18 U.S.C. §§ 3121-3127.
- § 2703(d): "A court order for disclosure of [a record or other information pertaining to a subscriber or customer . . . not including the contents of communications] . . . shall issue *only if* the governmental entity offers *specific and articulable facts* showing that there are *reasonable grounds* to believe that . . . the information sought [is] *relevant and material* to an ongoing criminal investigation."

- The clear majority of the *lower* Federal courts that then considered DOJ's "hybrid" theory in the early to mid 2000s found it lacking and concluded that PC grounded upon FRCrP 41 was required to compel cell phone service providers to divulge *real-time/prospective* cell phone location information.
- For *past* or *historic* CSLI, some courts have said a § 2703(d) order will suffice:

86

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Cell Phones

- *U.S. v. Stimler,* No. 15-4053, slip op. at 12 (3d Cir. Jul. 7, 2017). Historic CSLI case. Leaning on one of its earlier decisions treating CSLI, the Third Circuit concluded that "the SCA's disclosure regime [*i.e.,* including § 2703(d)] did not violate the Fourth Amendment because individuals lack a reasonable expectation of privacy in CSLI."
- *U.S. v. Carpenter,* 819 F.3d 880 (6th. Cir. 2016), *cert. granted* Jun. 5, 2017. Historic CSLI case. "[T]he federal courts had long recognized a core distinction: although the content of personal communications is private, the information necessary to get those communications between point A to point B is not." Slip op. at 6.
  - "[W]e hold that the government's collection of business records containing cell-site data [CSLI] [pursuant to § 2703(d)] was not a search under the Fourth Amendment." Slip op. at 11.

87

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Cell Phones

- But is a search warrant required to track a cell phone's more precise/ accurate GPS coordinates? Even if it's real-time/prospective GPS cell phone data?
- *U.S. v. Riley,* No. 16-6149 (6th Cir. Jun. 5, 2017): **No!** Because "the defendant's movements could have been observed by any member of the public, . . . [there] could not possibly be a Fourth Amendment violation for law enforcement officer to monitor those movements by using cell-phone location data just because such electronic monitoring was more efficient than relying on visual surveillance alone." Slip op. at 7.
  - "[H]ere the tracking only revealed that Riley had traveled *to* the Airport Inn, not which *room* (if any) the phone was in at the time of the tracking." Slip op. at 8 (original emphasis).

88

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Cell Phones

- What if an LEA uses its own device to track cell phones by mimicking a cell tower, *i.e.,* a cell site simulator, *e.g.,* a StingRay? Would a warrant be required in this instance?

89

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations+

Tracking Cell Phones

- *U.S. v. Lambis,* No. 15cr734, 2016 WL 3870940 (S.D.N.Y. Jul. 12, 2016). "A cell-site simulator . . . is a device that locates cell phones by mimicking the service provider's cell tower (or 'cell site') and forcing cell phones to transmit 'pings' to the simulator."
  - "The device then calculates the strength of the 'pings' until the target phone is pinpointed." At *1.
- But to understand *Lambis* we first have to look at a Supreme Court case dealing with another type of technology, the thermal imager: *Kyllo v. U.S.,* 533 U.S. 27 (2001).

90

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Cell Phones

- *Kyllo* - Justice Scalia, writing for the court, framed the question before it: "whether the use of a thermal-imaging device aimed at a private home from a public street to detect relative amounts of heat within the home constitutes a 'search' within the meaning of the Fourth Amendment." At 2.
- "[O]btaining by sense-enhancing technology any information regarding the *interior* of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area' [*e.g.,* the sanctity of the home] constitutes a search – at least where (as here) the technology in question is *not in general public use*." At 5. (emphases added)
  - The thermal imaging device "might disclose . . . at what hour each night the lady of the house takes her daily sauna and bath – a detail many would consider 'intimate.'" At 6.

91

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Cell Phones

- "Where, as here, the Government uses a device that is *not in general public use, to* explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." At 7 (emphasis added).
- Justice Stevens in dissent: "There is . . . a distinction of constitutional magnitude between 'through-the-wall surveillance' [and] . . . indirect deductions from 'off-the-wall' surveillance, that is, observations of the exterior of the home." At 8.
  - "[A]ny member of the public might notice that one part of a house is warmer than another part or a nearby building if, for example, rainwater evaporates or snow melts at different rates across its surfaces." At 9.
  - "Heat waves, like aromas that are generated in a kitchen, or in a laboratory or opium den, enter the public domain if and when they leave a building." At 9.

92

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Cell Phones

- Returning now to *Lambis:*
  - Relying upon and quoting from *Kyllo* the U.S. District Court for the Southern District of New York said, "The DEA's use of the cell-site simulator revealed 'details of the home that would previously been unknowable without physical intrusion.'" At *2
  - "Moreover, the cell-site simulator is not a device in 'general public use.'" At *2.
  - "Absent a search warrant, the Government may not turn a citizen's cell phone into a tracking device." At 5.
- DOJ policy announced Sept. 3, 2015:
  - "[A]s a matter of policy, [DOJ] law enforcement agencies must now obtain a search warrant supported by probable cause and issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure" except in the following two circumstances:

93

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Cell Phones

- 1) *Exigent circumstances* such as the need to:
  - protect human life or avert serious injury;
  - prevent the imminent destruction of evidence;
  - engage in the hot pursuit of a felon; or
  - to prevent the escape by a suspect or convicted fugitive from justice.
- But even in *exigent circumstances* the use of a cell site simulator must comply with the pen/trap statute *and . . .*
  - The DOJ LEA must contact the duty AUSA who, in turn, will call an OEO ESU supervisory attorney who will . . .
  - Provide a "short briefing" to a Criminal Division DAAG who will either approve or disapprove of the use of the cell site simulator in exigent circumstances.
  - Assuming approval, the AUSA must apply for a pen/trap order within 48 hrs. as required by 18 U.S.C. § 3125.

94

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Cell Phones

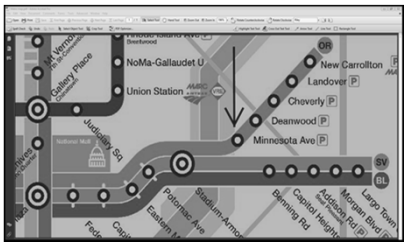
- 2) Undefined "exceptional circumstances where the law does not require a warrant" in which case approval to seek a pen/trap order must first be approved by/at/from:
  - The executive-level at the LEA's headquarters;
  - The U.S. Attorney; and,
  - A Criminal Division DAAG.
- And under this Sept. 3, 2015 DOJ cell site simulator policy –
  - "when the equipment is used to locate a known cellular device, all data must be deleted as soon as the device is located, and no less than once daily."
  - "when the equipment is used to locate an unknown cellular device, all data must be deleted as soon as the target cellular device is identified, and in any event no less than once every 30 days."
  - "prior to deploying [cell site simulator] equipment for another mission, the operator must verify that the equipment has been cleared of any previous operational data."

95

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Cell Phones

- Recent local case: *Jones v. U.S.,* No. 15-CF-322 (D.C.C.A. Sept. 21, 2017).



96

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

Tracking Cell Phones

- *Jones* (cont'd):
  - DCCA: "[We] conclude that the use of a cell-site simulator to locate Mr. Jones's phone *invaded a reasonable expectation of privacy* and was thus a search [for which no warrant complying with the Fourth Amendment had been obtained]."
  - "We thus conclude that under ordinary circumstances, the use of a cell-site simulator to locate a person through his or her cellphone invades the person's actual, legitimate, and reasonable expectation of privacy in his or her location information and is a search."

97

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

98

Federal Law of Electronic Surveillance (ELSUR) for *Criminal* Investigations

The End

99