

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION**

IN THE MATTER OF THE APPLICATION OF THE §
UNITED STATES OF AMERICA FOR AN ORDER §
AUTHORIZING (1) INSTALLATION AND USE OF A §
PEN REGISTER AND TRAP AND TRACE DEVICE § MAGISTRATE NO. H-06-356M
OR PROCESS, (2) ACCESS TO CUSTOMER §
RECORDS, AND (3) CELL PHONE TRACKING §

OPINION

This opinion addresses two significant issues concerning law enforcement access to certain dialing and signaling information in the hands of telephone companies under the Electronic Communications Privacy Act (“ECPA”). The first is whether the Government may obtain “post-cut-through dialed digits” containing communication contents under the authority of the Pen/Trap Statute.¹ The second is whether limited cell site information may be obtained prospectively under the dual or hybrid authority of the Pen/Trap Statute and the Stored Communications Act (“SCA”).²

These questions arise from a recent governmental application for a court order authorizing installation and use of a pen register and trap/trace device, access to customer records, and cell phone tracking. The court initially granted this order in part, denying access to the dialed digits as well as the limited cell site authority. In response to the Government’s informal request, the court agreed to reconsider the dialed digits ruling and invited full briefing by the Government as well as interested parties. The Electronic Frontier Foundation and Center for Democracy and Technology have filed

¹ 18 U.S.C. §§ 3121-3127.

² 18 U.S.C. §§ 2701-2712. Although commonly referred to as separate statutes, both the SCA and the Pen/Trap Statute were enacted as components of the ECPA.

an amicus brief on that issue. Although additional briefing has not been solicited on the cell site issue, that ruling will be reconsidered in light of a recent decision by a district judge in this district.

I. Post-Cut-Through Dialed Digits

This issue is a matter of first impression in this circuit and elsewhere.³ Before addressing the merits it is helpful to survey the legal and technical background.

A. Background

“Post-cut-through dialed digits” are any numbers dialed from a telephone after the call is initially setup or “cut-through.” Sometimes these digits are other telephone numbers, as when a party places a credit card call by first dialing the long distance carrier access number and then the phone number of the intended party. Sometimes these digits transmit real information, such as bank account numbers, Social Security numbers, prescription numbers, and the like. In the latter case, the digits represent communications content; in the former, they are non-content call processing numbers. *U.S. Telecom*, 227 F.3d at 462.

Because of this dual capacity, post-cut-through dialed digits occupy a doubtful position under federal electronic surveillance laws, which are founded upon the fundamental (indeed, constitutional) distinction between communications content and non-content. It is well-established that the content of telephone communications is protected by the Fourth Amendment. *Katz v. United States*, 389 U.S. 347, 353-54 (1967). In order to gain authorization to intercept content, the Government must obtain a special wiretap warrant that satisfies not only the usual probable cause

³ Two published decisions have mentioned the post-cut-through dialed digits problem, but neither actually ruled on the issue. See *United States Telecom Assoc. v. Federal Communications Comm’n*, 227 F.3d 450, 462 (D.C. Cir. 2000); *In re Application of United States for an Order Authorizing Use of a Pen Register and Trap on (xxx) Internet Service Account/User Name, (xxxxxxx@xxx.com)*, 396 F. Supp. 2d 45, 48 and n.2 (D. Mass. 2005).

standard but also additional threshold requirements set out in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (commonly referred to as the “Wiretap Act”).⁴

By contrast, there is no Fourth Amendment protection for telephone numbers dialed to connect a call. *Smith v. Maryland*, 442 U.S. 735, 745-46 (1979). In 1986, Congress enacted the ECPA to regulate the process under which law enforcement could install pen registers, which capture phone numbers of outgoing calls, and trap and trace devices, which capture phone numbers of incoming calls. Although a court order was required, the threshold for obtaining the order was very low: a Government attorney need only certify that “the information likely to be obtained is relevant to an ongoing criminal investigation.” 18 U.S.C. § 3122(b)(2). Because pen register technology at that time was unable to obtain contents,⁵ the question of law enforcement access to dialed numbers straddling the line between content and non-content was simply not contemplated when the ECPA was enacted.

Telecommunications technology did not stand still, of course, and within a few years law enforcement became very concerned that criminal investigations were being hindered by the technical inability of telecommunications carriers to provide authorized electronic surveillance. In response to these concerns, Congress enacted the Communications Assistance for Law Enforcement

⁴ The standard for issuance of a Title III wiretap warrant is whether (1) “normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;” and (2) there is probable cause for believing “that an individual is committing, or is about to commit” one of a list of enumerated crimes, that the wiretap will intercept communications about the enumerated crime, and that the communication devices to be tapped are either being used in the commission of the crime or are commonly used by the suspect. 18 U.S.C. § 2518(3).

⁵ For a description of the existing pen register technology, see *Smith v. Maryland*, 442 U.S. at 736 n.1; *United States v. New York Tel. Co.*, 434 U.S. 159, 161-62, n.1 (1977); *United States v. Guglielmo*, 245 F. Supp. 534, 535 (N.D. Ill. 1965).

Act of 1994 (CALEA).⁶ Under this law, telecommunication companies were directed to build into their networks the technical capability to assist law enforcement with authorized interception of communications and “call-identifying information.” *See* 47 U.S.C. § 1002.⁷ Congress intended CALEA to preserve the status quo, and therefore the new statute did not modify the legal standards for electronic surveillance via wiretap or pen/trap devices.⁸

One of the new technological wrinkles discussed during congressional deliberations on CALEA was the capacity of pen registers to capture content information in the form of post-cut-through dialed digits. This is reflected in the following exchange between Senator Leahy and FBI Director Freeh:

Sen. Leahy: You say this would not expand law enforcement’s authority to collect data on people, and yet if you’re going to the new technologies, where you can dial up everything from a video movie to do your banking on it, you are going to have access to a lot more data, just because that’s what’s being used for doing it.

Mr. Freeh: I don’t want that access, and I’m willing to concede that. What I want with respect to pen registers is the dialing information, telephone numbers which are being called, which I have now under pen register authority. As to the banking accounts and what movie somebody is ordering in Blockbuster, I don’t want it, don’t need it, and I’m willing to have technological blocks with respect to that information,

⁶ Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in scattered sections of 18 U.S.C. and 47 U.S.C.).

⁷ “The purpose of [CALEA] is to preserve the Government’s ability, pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies such as digital or wireless transmission modes, or features and services such as call forwarding, speed dialing and conference calling, while protecting the privacy of communications and without impeding the introduction of new technologies, features and services.” H.R. Rep. 103-827(I), 103d Cong., 2d Sess. at 9 (October 4, 1994).

⁸ CALEA “provide[s] law enforcement no more and no less access to information than it had in the past.” *Id.* at 22.

which I can get with subpoenas or other process. I don't want that in terms of my access, and that's not the transactional data that I need.⁹

Accordingly, CALEA was amended to address the post-cut-through dialed digits issue, by inserting the following limitation into the Pen/Trap Statute's provision authorizing pen registers:

(c) Limitation.— A government agency authorized to install and use a pen register under this chapter 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 and signaling information utilized in call processing.

Pub. L. No. 103-414, § 207, 108 Stat. 4279, 4292 (1994) (codified at 18 U.S.C. § 3121(c)).

Subsequent to CALEA's passage, attention turned to the development of specific technological standards through which telecommunications carriers would comply with their obligation to assist law enforcement by providing "call-identifying information."¹⁰ Development of such standards was left to the telecommunications industry, in consultation with law enforcement agencies and consumers, under the auspices of the Federal Communications Commission. 47 U.S.C. § 1006. In 1999, the FCC issued a ruling on the proposed technical standards (referred to as the "J-Standard"), finding among other things that the J-Standard must include the capability for "post-cut-through dialed digit extraction."¹¹ This capability required carriers to use tone-detection equipment to generate a list of all digits dialed after a call has been connected, including numbers dialed after

⁹ *Wiretapping: Joint Hearing of the Technology and Law Subcomm. of the Senate Judiciary Comm. and the Civil and Constitutional Rights Subcomm. of the House Judiciary Comm.*, 103d Cong., 2d Sess. 50 (March 18, 1994) (witness testimony of Louis J. Freeh, Director, Federal Bureau of Investigation).

¹⁰ Call-identifying information is defined in the act as "dialing or signaling information that identifies the origin, direction, destination, or termination or each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier." 47 U.S.C. § 1001(2).

¹¹ *In the Matter of Communications Assistance for Law Enforcement Act*, 14 F.C.C.R 16794 (1999).

connecting to a long distance carrier (such as 1-800-CALL-ATT), or to an automated telephone service, such as bank account or credit card numbers.

Several entities challenged the FCC decision and the petitions for review were consolidated in *United States Telecom Assoc. v. Federal Communications Comm'n*, 227 F.3d 450 (D.C. Cir. 2000). Petitioners contended that the CALEA obligation to produce “call-identifying information” should be limited to telephone numbers only, and that the FCC exceeded its authority by including the broader dialed digit extraction capability in the J-Standard. Applying the usual *Chevron* deference standard of review,¹² the D.C. Circuit first determined that CALEA was ambiguous with respect to its definition of call-identifying information. The court rejected the contention that the definition should be read in parity with ECPA definitions of “pen register” and “trap and trace device,” which are limited to phone numbers: “CALEA neither cross-references nor incorporates ECPA’s definitions of pen registers and trap and trace devices. Moreover, the fact that CALEA’s definition of ‘call-identifying information’ differs from the ECPA’s description of the information obtainable by pen registers and trap and trace devices reinforces the statute’s inherent ambiguity.” *Id.* at 459.

Next, the court determined that the FCC’s ruling as to dialed digit extraction reflected a lack of reasoned decision-making. In particular, the FCC failed to explain how the dialed digit extraction capability would meet the statutory requirements of a “cost-effective” method that would “protect the privacy and security of communications not authorized to be intercepted.” *Id.* at 461-62 (citing 47 U.S.C. § 1006(b)(1) & (2)). The Government had argued that the FCC’s ruling adequately protected privacy because a law enforcement agency is entitled to receive all post-cut-through digits

¹² *Chevron U.S.A. Inc. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837 (1984).

with a pen register order, subject to CALEA's "reasonably available technology" caveat (18 U.S.C. § 3121(c)). The court effectively side-stepped this argument, observing that "[n]o court has yet considered that contention, however, and it may be that a Title III warrant is required to receive all post-cut-through digits." *Id.* at 462. Because the FCC had not given "any meaningful consideration" to protecting the privacy of dialed digit contents, its order regarding dialed digit extraction was vacated and remanded for further proceedings.¹³ *Id.* at 462-63.

Congress returned to the dialed digits issue in the fall of 2001 during its consideration of the USA PATRIOT Act. Among the law enforcement enhancements within the initial DOJ-proposed bill was a provision amending the Pen/Trap Statute to include all "dialing, routing, addressing, or signaling information," thereby extending its coverage to Internet communications. *See* Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 Nw. U.L. Rev. 607, 637 (Winter 2003). Privacy advocates objected to this broadened definition, concerned that it might allow the Government to obtain the contents of communications without a wiretap order. *Id.* at 640-41. Senator Leahy, who had been instrumental in passing the CALEA "reasonably available technology" limitation, declared on the Senate floor that § 3121(c) had so far not achieved its purpose of protecting dialed digit contents from collection by pen registers:

When I added the direction on use of reasonably available technology (codified as 18 U.S.C. 3121(c)) to the pen register statute as part of the Communications Assistance for Law Enforcement Act (CALEA) in 1994, I recognized that these devices

¹³ After remand, the FCC ruled in April 2002 that dialed digit extraction capability was required by CALEA. Order on Remand, 17 F.C.C.R. 6896, 2002 FCC LEXIS 1716, **1 (April 5, 2002). The FCC determined that it was appropriate to include the capability for dialed digit extraction in the J-Standard, but that it was up to the courts to determine what valid legal instrument was necessary for the Government to obtain the information. The FCC stated "[i]f a [law enforcement agency] thinks a pen register is the proper authority to obtain information under the dialed digit extraction capability, then it must convince the court of this fact." *Id.* at **108.

collected content and that such collection was unconstitutional on the mere relevance standard. Nevertheless, the FBI advised me in June 2000, that pen register devices for telephone services “continue to operate as they have for decades” and that “there has been no change . . . that would better restrict the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing.” Perhaps, if there were meaningful judicial review and accountability, the FBI would take the statutory direction more seriously and actually implement it.

147 Cong. Rec. S11000 (Oct. 25, 2001) (remarks of Sen. Leahy).

To alleviate this concern that had not been fully alleviated by CALEA, Congress amended the Pen/Trap Statute in three ways: (1) the phrase “shall not include the contents of any communication” was added to the pen register definition at § 3127(3); (2) the same phrase was added to the trap and trace device definition at § 3127(4); and (3) the phrase “so as not to include the contents of any wire or electronic communications” was added to the reasonably available technology limitation at § 3121(c). Senator Leahy explained the significance of the latter amendment on the Senate floor:

The USA Act also requires the government to use reasonably available technology that limits the interceptions under the pen/trap device laws “so as not to include the contents of any wire or electronic communications.” This limitation on the technology used by the government to execute pen/trap orders is important since as the FBI advised me in June 2000, pen register devices “do capture all electronic impulses transmitted by the facility on which they are attached, including such impulses transmitted after a phone call is connected to the called party.” The impulses made after the call is connected could reflect the electronic banking transactions a caller makes, or the electronic ordering from a catalogue that a customer makes over the telephone, or the electronic ordering of a prescription drug.

This transactional data intercepted after the call is connected is “content.”

Id.; see also Beryl A. Howell, *Seven Weeks: The Making of the USA PATRIOT Act*, 72 GEO. WASH. L. REV. 1145, 1198 (2004).

On May 24, 2002, Deputy Attorney General Larry D. Thompson issued a memorandum setting out DOJ policy on post-cut-through dialed digits in light of the PATRIOT Act amendments¹⁴. This policy consists of two “basic principles”: (1) law enforcement would use reasonably available technology to minimize over-collection of contents, while still allowing collection of all non-content digits; and (2) no affirmative investigative use would be made of any content digits incidentally collected.

¹⁴ The DOJ Memo reads in pertinent part:

1. Use of reasonably available technology to avoid overcollection. As mandated by section 3121(c), an agency seeking to deploy a pen register or trap and trace device must ensure that it uses “technology reasonably available to it” that restricts the information obtained “so as not to include the contents of any wire or electronic communications.” 18 U.S.C. § 3121(c) (West. Supp. 2002). *This provision imposes an affirmative obligation to operate a pen register or trap and trace device in a manner that, to the extent feasible with reasonably available technology, will minimize any possible overcollection while still allowing the device to collect all of the limited information authorized.*

Moreover, as a general matter, those responsible for the design, development, or acquisition of pen registers and trap and trace devices should ensure that the device developed or acquired for use by the Department reflect reasonably available technology that restricts the information obtained “so as not to include the contents of any wire or electronic communications.”

2. No affirmative investigative use of any overcollection that occurs despite use of reasonably available technology. To the extent that, despite the use of “technology reasonably available to it,” an agency’s deployment of a pen register does result in the incidental collection of some portion of “content,” it is the policy of this Department that such “content” may not be used for any affirmative investigative purpose, except in a rare case in order to prevent an immediate danger of death, serious physical injury, or harm to the national security. For example, if, despite the use of reasonably available technology, a telephone pen register incidentally recorded a bank account number and personal identification number (PIN) entered on an automated bank-by-phone system, those numbers should not be affirmatively used for any investigative purpose.

Larry, D. Thompson, “Avoiding Collection and Investigative Use of ‘Content’ in the Operation of Pen Registers and Trap and Trace Devices,” May 24, 2002, available at <http://www.judiciary.house.gov/judiciary/attachd.pdf>, (“DOJ Memo”) (emphasis added).

In response to the briefing order in this case, the Government has filed a submission that “technology currently is not reasonably available which would permit law enforcement to reliably discern and then separately collect only those post-cut-through digits that are call processing information from those that may constitute content.”¹⁵ For this reason, the Government apparently employs no filtering technology at this time, and seeks this court’s authorization to gather all dialed digits, content and non-content, in reliance on its pledge to make no affirmative investigative use of content digits.

B. Statutory Text

The starting point of statutory interpretation is always the wording of the statute. If its meaning is plain and unambiguous, the job is done and further inquiry moot. *See, e.g., Barnhart v. Sigmon Coal Co.*, 534 U.S. 438, 450 (2002). Here we begin with the relevant definitions. In pertinent part, “pen register” is defined as:

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 . . .*

18 U.S.C. § 3127(3) (emphasis added). Similarly, “trap and trace device” is defined in pertinent part as:

A device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, or 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 . . .*

¹⁵ Exhibit A to Government’s brief, filed under seal.

18 U.S.C. § 3127(4) (emphasis added). The emphasized passages plainly declare that, by definition, pen/trap devices *must not* obtain information that *includes* contents. This proscription against content is unqualified.

The term “contents” of communication is defined as “any information concerning the substance, purport, or meaning of that communication.” 18 U.S.C. §§ 2510(8), 3127(1). It is undisputed that post-cut-through dialed digits can and often do include call content. *See United States Telecom.*, 227 F.3d at 462. As the D.C. Circuit explained:

For example, subjects calling automated banking services enter account numbers. When calling voicemail systems, they enter passwords. When calling pagers, they dial digits that convey actual messages. And when calling pharmacies to renew prescriptions, they enter prescription numbers.

Id. Some post-cut-through digits are non-content telephone numbers, as when a party places a credit card call by first dialing a long distance carrier access number, and then, after the initial call is “cut through,” dialing the number of the intended party.¹⁶ *Id.* The Government’s application covers all post-cut-through dialed digits, both content and non-content.

The Government contends that the seemingly unconditional command of § 3127 is relieved by § 3121(c), which reads in its entirety:

(c) Limitation.— A government agency authorized to install and use a pen register or trap and trace device under this chapter 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

¹⁶ Even in this latter example, however, the calling party may be required to enter content information such as an account number before the carrier will proceed with the call. The Government argues that account number digits dialed in this manner actually become non-content call set-up information, thereby losing their “protected” content status. Resolution of this particular question is immaterial here, because the Government’s application seeks access to all digits dialed, before and after call set-up.

in the processing and transmitting of wire or electronic communications *so as not to include the contents of any wire or electronic communications*.

18 U.S.C. § 3121(c) (emphasis added). On its face, however, this section does not expressly authorize anything. Instead, it imposes an affirmative obligation (“shall use technology”) upon a law enforcement agency which has already been “authorized to install and use” a pen/trap device.

The Government responds that § 3121(c) implicitly authorizes acquisition of contents. According to the Government, there is no available technology which can reliably isolate all content from non-content dialed digits.¹⁷ Since this is so, the affirmative obligation is cancelled, because it presumes a state of technology that does not exist. And because that state of technology does not exist, the Government further infers that the section affirmatively authorizes acquisition of mixed content and non-content dialed digits. Otherwise the section serves no purpose and would be rendered superfluous, in violation of the well-known canon of construction. *TRW Inc. v. Andrews*, 534 U.S. 19, 31 (2000).

There are numerous difficulties with the Government’s construction. First, it rests almost entirely upon legislative silence. Section 3121(c) does not say what the outcome would be if technology could not separate all content from non-content dialed digits. The most natural reading of the provision is that Congress assumed that such technology would be available, and for that reason did not address or even contemplate the contrary scenario. If Congress did contemplate the

¹⁷ The Government has submitted an affidavit from a federal law enforcement agency supporting this proposition, but has requested that it remain sealed. For that reason the court is in no position to adjudicate this issue, and will assume only for purposes of this opinion that no such technology presently exists. That said, it does seem surprising that a satisfactory computer-based algorithm could not be devised to solve this problem, which at bottom is a matter of digital sorting—a task well-suited to computers. After all, the Government apparently has the capacity to recognize content digits after they are received. *See* DOJ Memo. It is not evident why such recognition is impossible prior to receipt.

possibility that technology would not be available, then it is certainly curious why it did not explicitly declare content digits as fair game, especially since the statute elsewhere excludes content in unqualified terms. Of course, this anomaly disappears if the passage is construed not to allow acquisition of contents in this situation, as *amici* contend.

The Government incorrectly argues that its interpretation is the only way to avoid rendering § 3121(c) superfluous. According to the DOJ Memo: “This provision imposes an affirmative obligation to operate a pen register or trap and trace device in a manner that, *to the extent feasible* with reasonably available technology, will *minimize* any possible overcollection while still allowing the device to collect *all* of the limited information authorized.” (Emphasis added). The italicized words and phrases do not appear in the statute, but constitute the DOJ’s gloss on the passage, which can be reduced to the following maxim: “minimize content, but allow all non-content.” This is admittedly one possible way to read § 3121(c), but there is another — that the Government must use technology reasonably at hand to gather as many non-content digits as possible, without also including contents. In other words, “maximize non-content, but disallow all content.” This “maximization” reading is not only inherently plausible, but also in harmony with the unqualified content proscription found in the concluding passage of § 3121(c) (“so as not to include the contents of any wire or electronic communications”). By contrast, the Government’s minimization reading contradicts, or at least creates serious tension with, the explicit content prohibitions inserted into the statute by the PATRIOT Act. The operative canon of statutory construction here is not the rule against superfluity, but rather the rule that statutory provisions be construed in harmony with one another. *See Food and Drug Admin. v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 133 (2000) (“A court must therefore interpret the statute as a symmetrical and coherent regulatory

scheme, and fit, if possible, all parts into an harmonious whole . . .” (internal quotations and citations omitted)). Thus, the Government is the party at odds with traditional canons of construction, not *amici*.

In practice, it appears the Government has not even adhered to its own view that the statute imposes an affirmative obligation to minimize content collection. According to its submissions, the Government has concluded that no technology currently available would permit law enforcement to isolate call processing digits from content digits with 100% accuracy. Apparently for that reason, the Government is not currently using any minimization technology at all. Instead, it asks this court to authorize the collection of all digits dialed, before and after call set-up, and to rely upon the Government’s promise not to make affirmative investigative use of contents. But the Government’s affirmative obligation under § 3121(c) is not a mere contingency, lying dormant until some future day when a foolproof filter is found. It is, as the DOJ memo appears to recognize, a continuing obligation to use whatever technology is available at any given time to avoid collection of contents. That technology need not be perfect, only reasonably available, and if so it must be used.

Although not discussed in these filings, there surely are some technological means to avoid collection of content. As one DOJ manual advises:

Caveat. Technology is available to limit the pen register device so that it only records a specified number of dialed digits, for example, the first 10 digits. While this may eliminate the inadvertent collection of the “content” of a communication (referred to as “overcollection”), it may also eliminate the collection of legitimate, lawful data pertinent to an investigation.

R. Stabe, *Electronic Surveillance – Non-Wiretap*, at § 3.4, in FEDERAL NARCOTICS PROSECUTIONS.¹⁸ Restricting the number of recorded digits might well deprive law enforcement of some legitimate telephone numbers under a pen register order, but that does not mean that the Government could not obtain them through other means.¹⁹ If the Government believes that pen register technology is too restrictive, then the correct response under the statute is to develop better technology, not ignore the statutory command. The Government’s position (“minimize content, but allow all non-content”) gives no incentive to anyone in government or industry to alter the technological status quo, which perhaps explains why there is no effective filtering technology 12 years after CALEA decreed its use.

Courts should not be in the business of crafting exceptions to unqualified proscriptions handed down by Congress. “Shall not include contents” is not a precatory suggestion, it is a plain commandment. While not etched upon a tablet of stone, this edict from Capitol Hill is no less binding upon those who must interpret and execute it.

C. Legislative History

Because the text of the statute is so plain, there is no need to resort to legislative history for clearer signs of congressional intent. Even so, the legislative history already recited in this opinion abundantly confirms the plain meaning of the statute.

Briefly summarized, that history reflects persistent Congressional efforts to assure that communications contents retain their protected legal status in the face of changing technology and law enforcement capabilities. The initial Pen/Trap Statute, part of the ECPA, was “primarily a privacy law.” Kerr, 97 Nw. L. Rev. at 638. It regulated the phone number collection that would

¹⁸ Formerly available at <http://10.173.2.12/usao/eousa/ole/usabook/drug/03drug.htm>.

¹⁹ See 18 U.S.C. §§ 2510-2518; 18 U.S.C. §§ 2701-2712.

otherwise have been unregulated after *Smith v. Maryland*. Because existing pen register technology in the 1980s did not allow over-collection of content, there was no need for Congress to address the contents problem in that portion of the ECPA.²⁰ When Congress became aware of the issue in 1994, it passed the CALEA amendment to the Pen/Trap Statute imposing an affirmative obligation to use technology to restrict the information collected to call-processing numbers. *See* 18 U.S.C. § 3121(c). Advised in 2001 that pen registers continued to collect content despite CALEA's technology limitation,²¹ Congress acted again by inserting into the Patriot Act not one but three separate directives placing contents out of bounds for pen/trap devices. 18 U.S.C. §§ 3121(c), 3127(3) & (4).

The Government has a different take on the 2001 amendments, urging that the amendments to the pen/trap definitions “were not intended in any way to trump the provision in 3121(c).”²² In support, the Government cites Senator Leahy's analysis of that portion of the PATRIOT Act (§ 216) that contained all three amendments:

[Section 216] also ensures that the pen register and trap and trace provisions apply to facilities other than telephone lines (e.g., the Internet). It specifically provides, however, that the grant of authority to capture “routing” and “addressing” information for internet users does not authorize the interception of the content of any such communications. It further requires government to use the latest available technology to insure that a pen register or trap and trace device does not intercept the content of any communications.

147 Cong. Rec. S11006-S11007 (Oct. 25, 2001). But nothing in this passage supports the Government's claim that it “presupposes that the Government may receive incidentally and

²⁰ *See generally* Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. Cal. L. Rev. 949, 982-989 (1996) (discussing the limited capacity of the early pen register considered in *Smith v. Maryland*, and the evolution of the modern version).

²¹ 147 Cong. Rec. S11000 (Oct. 25, 2001) (remarks of Sen. Leahy).

²² Government brief, at 7.

unavoidably collected content information” under a pen/trap order.²³ Nor is there any tension between the definition amendments and the technology section amendment. All three point in exactly the same direction — interception of any communications content is not authorized, and technology must be used to insure that communications content is not collected.

Also questionable is the Government’s apparent presumption that the pre-PATRIOT Act version of § 3121(c) was intended to authorize the collection of content so long as filtering technology was unavailable. One respected authority, in an article addressing what he considered unfounded criticism of the PATRIOT Act by privacy advocates, noted that despite “ambiguous language in the pen register statute dating from 1986 . . . no one had ever thought that the contents of communications that happen to include numbers were somehow exempted from the Wiretap Act.” *See* Kerr, 97 Nw. U.L. Rev. at 642; *see also id.* at 641 (characterizing such an interpretation as “fanciful” and “difficult to imagine.”). While there is no need for the court to definitively construe previous versions of the Pen/Trap Statute, it is appropriate to note that the fundamental premise of the Government’s argument from legislative history is highly dubious.

Post-cut-through dialed digit contents may be intercepted by law enforcement under the Wiretap Act, and collected from electronic storage under the SCA. They are not available to law enforcement under the Pen/Trap Statute. Section 3121(c) is a limitation, not a license. Because the Pen/Trap Statute triply forbids what the Government requests, the application to acquire post-cut-through dialed digits must be denied.

²³ Government brief, at 7.

II. Limited Cell Site Information

Invoking the same legal theory rejected by this court last fall,²⁴ the Government again seeks to obtain an order authorizing access to prospective cell site information as part of a criminal investigation. This time, the Government has narrowed the scope of its cell site request: “‘Cell site information’ as used in this application refers to the antenna tower and sector to which the cell phone sends its signal. This includes the physical location and/or address of the cellular tower and identification of the particular sector of the tower receiving the signal.” Government’s sealed application (Dkt. 1). Previously, the Government had sought unlimited cell site data, including all cell site activations when the phone was on, control channels, signal strength, and other network information which would permit “triangulation” of the user’s location.

The statutory argument for limited cell site authority is precisely the same “hybrid” or “dual authority” theory offered in support of the Government’s earlier application for unrestricted cell site information.²⁵ No published court opinion has yet agreed with the Government that unlimited cell site information is obtainable via the combined authority of the Pen/Trap Statute, CALEA, and the

²⁴ *In re Application for Pen Register and Trap/Trace Device with Cell Site Authority*, 396 F. Supp. 2d 747 (S.D. Tex. 2005). Because official captions of cell site cases are both unwieldy and undistinctive, a shorthand citation to court locale will be used, *e.g.*, *CSI Houston I*.

²⁵ *See* 396 F. Supp. 2d at 761. The terms “dual” and “hybrid” will be used interchangeably to refer to the Government’s theory and its proponents.

SCA.²⁶ Rather than confront these adverse rulings directly by appeal—a course explicitly urged by this and other courts—the Government has chosen to alter its application instead of its legal theory.²⁷

Although a majority of published opinions continue to reject the dual theory as a basis even for limited cell site information,²⁸ four courts have granted such limited applications on that ground.²⁹ The first to provide a qualified endorsement of the Government’s dual theory is Magistrate Judge Gorenstein’s opinion in *CSI New York I*. Subsequent decisions adopting the minority view have essentially followed Judge Gorenstein’s analysis in all major respects; indeed, his opinion

²⁶ *CSI Houston I*, 396 F. Supp. 2d 747 (S.D. Tex. 2005); *CSI DC I*, Nos. 04-403-04, 407-411, 2005 WL 3658531 (D.D.C. Oct. 26, 2005); *CSI Baltimore I*, 402 F. Supp. 2d 597 (D. Md. 2005); *CSI DC II*, 407 F. Supp. 2d 132 (D.D.C. 2005); *CSI DC III*, 407 F. Supp. 2d 134 (D.D.C. 2006)..

²⁷ One AUSA has candidly conceded that this strategy is guided not so much by legal principle as by a desire to placate recalcitrant magistrate judges. *CSI Rochester*, 415 F. Supp. 2d 211, 218 n.5 (W.D.N.Y. 2006) (“There’s a common sense decision that says if we want to do this higher step, if we want to go to triangulation, we’re gonna have a hell of a fight . . .”).

²⁸ *CSI Central Islip*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005); *CSI Milwaukee*, 412 F. Supp. 2d 947 (E.D. Wisc. 2006); *CSI Rochester*, 415 F. Supp. 2d 211 (W.D.N.Y. 2006); *CSI Baltimore II*, 416 F. Supp. 2d 590 (D. Md. 2006); *CSI New York II*, No. 06 Crim. Misc. 01, 2006 WL 468300 (S.D.N.Y. Feb. 28, 2006); *CSI-Fort Wayne*, Nos. 1:06-MC-6, 1:06-MC-7, 2006 WL 1876847 (N.D. Ind. July 5, 2006).

²⁹ See *CSI New York I*, 405 F. Supp. 2d 435 (S.D.N.Y. 2005); *CSI Sacramento*, No. S-06-SW-0041, slip op. (E.D. Ca. March 15, 2006); *CSI Shreveport*, 411 F. Supp. 2d 678 (W.D. La. 2006); *CSI Houston II*, Misc. No. H-06-0085, 2006 WL 1566166 (S.D. Tex. April 11, 2006).

remains the most cogent expression of the Government's dual theory to date.³⁰ For that reason it will be the focus here.

The Government asserts that legal authority for its application may be implied from three separate statutes, via a process I have previously likened to a three-rail bank shot. 396 F. Supp. 2d at 765. The first rail is the Pen/Trap Statute, 18 U.S.C. § 3121 *et seq.*, which is asserted to be the exclusive means by which law enforcement may acquire non-content signaling information such as cell site data. The second rail is CALEA § 1002(a), which provides that location information such as cell site data cannot be obtained "solely pursuant" to a pen/trap order. Hybrid proponents interpret this to mean that, although a pen/trap order is still a necessary condition for compelling disclosure of cell site data, it is no longer sufficient, and must be combined with some additional authority. This additional authority is said to reside in the third rail, otherwise known as the SCA, 18 U.S.C. § 2703, which allows the Government to obtain cell phone customer records upon a lesser showing than probable cause.³¹

³⁰ District Judge Lee Rosenthal has taken the minority view. *CSI Houston II*, Misc. No. H-06-0085, 2006 WL 1566166 (S.D. Tex. April 11, 2006). Her opinion, which adopts *in toto* the analysis of Magistrate Judge Gorenstein, is the main impetus for this detailed re-examination of the dual theory as applied to limited cell site information. While the focus here will necessarily be upon Judge Gorenstein's opinion rather than Judge Rosenthal's, two misstatements in the latter should be noted. First, Magistrate Judge Bredar's decision at 402 F. Supp. 2d 597 (D. Md. 2005) did not grant a cell site application on less than probable cause. *See* 2006 WL 1566166, at *3. Actually, this is one of two opinions by Judge Bredar *denying* cell site applications. Judge Bredar's second decision decisively rejects the dual theory as applied to limited cell site information. *CSI Baltimore II*, 416 F. Supp. 2d 390, 393-97 (D. Md. 2006). Second is the inaccurate assertion that courts rejecting the dual theory are relying on "congressional testimony from the former director of the Federal Bureau of Investigation about certain aspects of the PATRIOT Act..." 2006 WL 1566166, at *2-3. The testimony in question was given in relation to CALEA, *not* the PATRIOT Act, which was passed by a different Congress seven years later. This time gap poses a significant difficulty for the dual theory. *See* 396 F. Supp. 2d at 762-64.

³¹ "A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court (continued...)"

Judge Gorenstein’s opinion rests upon meticulous analysis of the text of these three statutes, with occasional resort to legislative history as needed. *CSI New York I*, 405 F. Supp. 2d at 439, 441. What follows is a rail-by-rail critique of that analysis, demonstrating that (A) the Pen/Trap Statute is not the exclusive mechanism to obtain signaling information such as cell site data; (B) the “solely pursuant” clause of CALEA § 1002(a) need not be construed to mean that a pen/trap order is a necessary condition for obtaining cell site data; and (C) even if a pen/trap order were a necessary condition, the SCA by its own terms cannot provide the needed additional authority. Part D concludes by pointing out additional flaws in the dual argument yet to be addressed satisfactorily (if at all) by its proponents.

A. The First Rail: The Pen/Trap Statute

The lynchpin of the dual theory is that the Pen/Trap Statute constitutes the *exclusive* mechanism by which the Government may install a pen register and, by extension, obtain the signaling information a pen register is designed to yield. *CSI New York I*, 405 F. Supp. 2d at 441. At several points *CSI New York I* invokes this exclusivity premise in support of a *reductio ad absurdum* argument: if signaling information such as cell site data could not be obtained via a pen/trap order (whether alone or in combination), then such data would not be available to the Government by *any* mechanism at all. *Id.* at 441-43.

Now it is hard to dispute the absurdity of concluding that cell site information is totally beyond the reach of law enforcement. But the source of this absurdity lies within the initial premise

³¹ (...continued)
of competent jurisdiction and shall issue only if the government 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. . . .” 18 U.S.C. § 2703(d).

itself. Bear in mind that the legal threshold for a pen/trap order is the minimum possible for any court order—a mere certificate of relevance by a Government attorney. According to hybrid proponents, this pen/trap standard is not only a threshold, but also a ceiling. “Fed. R. Crim. P. 41 or Title III cannot by themselves provide authority for the Government’s application because any warrant or order issued pursuant to those mechanisms must necessarily authorize the installation of a ‘pen register.’” *CSI New York I*, 405 F. Supp. 2d at 441. In other words, a judge who would be compelled to grant a pen register application solely upon the Government’s certification of relevance must deny that application if the Government goes further and establishes probable cause under Rule 41.

At least one court has described this result as absurd. *CSI Baltimore II*, 416 F. Supp. 2d 390, 397 n.11 (D. Md. 2006). It certainly runs counter to the commonly accepted understanding of the ECPA. “One feature of ECPA is that through use of greater legal process officials can gain access to any information that they could obtain with lesser process.” J. Carr & P. Bellia, *Law of Electronic Surveillance* § 4:77, at p. 4-193 (2006); *see also* Orin S. Kerr, *A User’s Guide to the Stored Communications Act, And a Legislator’s Guide to Amending It*, 72 *Geo. Wash. L. Rev.* 1208, 1222 (2004) (“The rules for compelled disclosure operate like an upside-down pyramid. Because the SCA’s rules allow greater process to include the lesser, different levels of process can compel different groups of information. The higher up the pyramid you go, the more information the government can obtain.”). This “nested hierarchy” structure is also reflected in the manual published by DOJ’s Computer Crime and Intellectual Property Section (CCIPS). CCIPS Manual (July 2002), at § III D (“Thus, a § 2703(d) court order can compel everything that a subpoena can compel (plus additional information), and a search warrant can compel the production of everything that a §

2703(d) order can compel (and then some)”). The common sense of this approach is obvious. Legal process is calibrated to the degree of intrusion. So “the greater the privacy interest at stake, the higher the threshold Congress uses.” Kerr, 97 Nw. U. L. Rev. at 620-21 (setting out “the continuum of court orders and legal processes” that Congress currently uses to govern law enforcement surveillance of communications networks). The higher the legal threshold, the more information becomes accessible.

Hybrid proponents do not explain what rational law enforcement purpose is served by construing the Pen/Trap Statute as both a floor and a ceiling, thereby excepting it from the usual ECPA “greater includes the lesser” scheme. Perhaps a rationale could be constructed if a pen/trap order possessed unique features or authorities not available under Rule 41. But the U.S. Supreme Court eliminated this possibility by its holding in *United States v. New York Tel. Co.*, 434 U.S. 159 (1977).

In *New York Telephone*, a telephone company challenged a district court order authorizing a pen register under Rule 41. The Court affirmed the Rule 41 pen register in a three-part decision. First, the Court rejected the contention that pen registers must satisfy the tight strictures of Title III of the Wiretap Act. “Congress did not view pen registers as posing a threat to privacy of the same dimension as the interception of oral communications and did not intend to impose Title III restrictions upon their use.” *New York Telephone*, 434 U.S. at 168. Second, the Court held that the pen register order was properly issued under Rule 41, which “is sufficiently flexible to include within its scope electronic intrusions authorized upon a finding of probable cause.” *Id.* at 169. Finally, and most importantly, the Court upheld the district court’s authority to order the additional features now commonly associated with pen/trap orders: (i) directing the phone company to provide all facilities

and technical assistance necessary to employ the pen registers unobtrusively, (ii) in return for reasonable compensation, (iii) for a limited period of time, and (iv) without disclosure to the investigative targets. *Id.* at 172-75. Rejecting the contrary view of the lower court, the Court held that the All Writs Act supplied any additional authority needed to carry out the surveillance authorized by the Rule 41 warrant. The technical assistance order was essential “to prevent nullification of the court’s warrant and the frustration of the Government’s right under the warrant to conduct a pen register surveillance.” *Id.* at 175 n.23.

Almost as noteworthy as the holdings themselves was the Court’s stated rationale. In support of its Rule 41 holding, the Court twice invoked a variant of the “greater includes the lesser” maxim: “[I]t would be anomalous to permit the recording of conversations by means of electronic surveillance while prohibiting the far lesser intrusion accomplished by pen registers.” *Id.* at 170; *see also id.* at n.18 (“What ‘strains credulity’ is the dissent’s conclusion . . . that Congress intended to permit the interception of telephone conversations while prohibiting the use of pen registers to obtain much more limited information.”). The Court used the same principle to justify its technical assistance holding, noting that Title III conferred similar authority upon federal courts to facilitate wiretaps: “In light of this direct command to federal courts to compel, upon request, any assistance necessary to accomplish an electronic interception, it would be remarkable if Congress thought it beyond the power of the federal courts to exercise, where required, a discretionary authority to order telephone companies to assist in the installation and operation of pen registers, which accomplish a far lesser invasion of privacy.” *Id.* at 177.

Although predating the ECPA, *New York Telephone* has never been overruled. Its practical import was admittedly diminished two years later, when *Smith v. Maryland* held that use of a pen

register was not a “search” under the Fourth Amendment because it did not acquire the contents of communications. 442 U.S. 735, 741 (1979). Thereafter, federal law enforcement agencies obtained pen registers via court order under then-existing Rule 57,³² which did not require independent judicial review of supporting facts. *See* H. Rep. No. 99-647, at 25 (June 19, 1986). While the ECPA ultimately approved this lowering of the minimum necessary showing required to obtain a pen register order, nothing in the ECPA or its history suggests any dissatisfaction with either the holdings or the rationale of *New York Telephone*. In particular, the new Pen/Trap Statute incorporated the same technical assistance features that the Supreme Court had already found within the district court’s power by virtue of Rule 41 and the All Writs Act. Thus, the only material difference³³ between Rule 41 and the Pen/Trap Statute is the legal threshold for access to pen register information.

And so the unanswered question remains – what conceivable law enforcement purpose could pen/trap “exclusivity” serve? Most would concede the irrationality of instructing a civil jury to find for the plaintiff upon proof by a preponderance of evidence, but against the plaintiff if he proves his case beyond a reasonable doubt. This instruction seems nonsensical, because the greater proof would surely include the lesser. But according to hybrid proponents, this greater-includes-the-lesser maxim does not apply to the Pen/Trap Statute; law enforcement cannot obtain pen register information if it offers too much proof.

³² This catch-all rule provided: “In all cases not provided for by rule, the district judges and magistrates may regulate their practice in any manner not inconsistent with these rules or those of the district in which they act.” FED. R. CRIM. P. 57 (1944) (amended Dec. 1, 1995).

³³ Rule 41 does contain other requirements, such as notice and a 10 day execution period, but the *New York Telephone* Court noted that the rule was “not so inflexible” as to require strict adherence to such procedural aspects in every situation. 434 U.S. at 169 n.16.

The only justification so far offered for this strange result is that it comports with a literal reading of the statute. The proposition is debatable,³⁴ but there is no need to resolve that question. Even granting that exclusivity might be a plausible reading of the literal text, it is not the only possible way to interpret these words. Statutes should be construed to avoid absurd results whenever possible. *United States v. Wilson*, 503 U.S. 329, 334 (1992); *Armstrong Paint & Varnish Works v. Nu-Enamel Corp.*, 305 U.S. 315, 333 (1938) (“To construe statutes so as to avoid results glaringly absurd, has long been a judicial function.”). Here, absurdity can be avoided by construing these words in harmony with the “greater includes the lesser” rule, a maxim not only endorsed by the Supreme Court but also recognized as the organizing principle of the ECPA. Under this reading, § 3121(a) establishes the minimum, but not the maximum, legal process under which a pen/trap may be installed or used. Such a construction does no violence to the evident statutory purpose of § 3121(a), which was to set a floor but not a ceiling for pen/trap use. Because this reading of the statute avoids the absurd result that the Government is entitled to *less* information when it presents *more* proof, ordinary rules of statutory construction must prefer this interpretation. *Wilson*, 503 U.S. at 334.

B. The Second Rail: CALEA § 1002(a)

Rejection of Pen/Trap Statute exclusivity also dramatically undermines another key element of the dual theory. CALEA § 1002(a) declares that information about the physical location of the subscriber may not be acquired “solely pursuant to” the Pen/Trap Statute. 47 U.S.C. § 1002(a).

³⁴ The limitation in § 3121(a) refers only to the devices themselves, not the information derived from them. And the device definitions in § 3127 do not seem to encompass all means of obtaining signaling information; “pen register” is a device or process which only “records or decodes” such information, and “trap and trace device” is one which only “captures” incoming electronic impulses.

Hybrid proponents contend that this can only mean that such information is available via the Pen/Trap Statute combined with some additional, unspecified authority; in other words, the Pen/Trap Statute is a necessary but not sufficient condition for obtaining cell site data. Otherwise, they say, “the Government may not acquire cell site information by *any* mechanism” at all, which would obviously be an absurd result. *CSI New York I*, 405 F. Supp. 2d at 441 (emphasis in original). But this argument to absurdity collapses once the prop of Pen/Trap Statute exclusivity is removed. As explained above, the Supreme Court itself has declared Rule 41 a sufficiently flexible vehicle for obtaining pen register information, and nothing in the ECPA altered that holding. So CALEA’s elimination of the pen/trap order as a legal basis to obtain cell site data does not place such information beyond the reach of law enforcement.

Beyond this unavailing *reductio ad absurdum*, hybrid proponents offer another argument emphasizing the word “solely” and its syntactical position within the CALEA proviso:

The use of the word “solely” is significant. “Solely” means “without another” or “to the exclusion of all else.” If we are told that an act is not done “solely” pursuant to some authority, it can only mean that the act is done pursuant to that authority “with [] another” authority.

CSI New York I, 405 F. Supp. 2d at 442 (emphasis added, internal citations omitted). Thus, the word “solely” in § 1002(a) must mean that a pen/trap order is a *necessary but insufficient* condition for obtaining cell site data. Any other construction, it is claimed, necessarily reads the word “solely” out of the statute, in violation of the canon that every word in a statute must count. *Id.*

This argument is unconvincing for several reasons. CALEA legislative history contains no clue that its drafters imbued the word “solely” with the significance now attributed by hybrid proponents. The legislation summary in the final House report omits the word entirely: “Call

identifying information obtained pursuant to pen register and trap and trace orders may not include information disclosing the physical location of the subscriber sending or receiving the message, except to the extent that location is indicated by the phone number.” H.R. Rep. No. 103-827(I), 1994 WL 557197, at p. 25 (Oct. 4, 1994). Nor is the word mentioned in the testimony of FBI Director Freeh, the chief law enforcement proponent of the legislation. *Wiretapping Access: Hearing Before the Subcomm. on Telecomm. and Fin. of the Comm. on Energy and Commerce*, 103d Cong. (September 13, 1994) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation), available at 1994 WL 497163.

Nor does CALEA logically compel the conclusion that a pen/trap order is always necessary, in combination with other unspecified authority, to secure cell site data. The “solely pursuant” phrase leaves open the possibility that a pen/trap order may be neither necessary nor sufficient to obtain such data. Consider the following true statement: “A person cannot practice law in California solely pursuant to a law degree.” A law degree is not *sufficient* because additional conditions must be met to obtain a law license, most notably passing the bar exam. But neither is a law degree a *necessary* condition for obtaining a California law license. California is among a handful of states that permits individuals to sit for the bar exam after a four year period of informal study (sometimes termed “reading law”). Just as a law degree may be one route, but not the only route, to obtain a California law license, so a pen/trap order may be one route, but not the only route, to obtain cell site information. Independent statutory authority (such as Rule 41) may also suffice, and this possibility cannot be ruled out based on a literal reading of the “solely pursuant” clause.

Moreover, the word “solely” can readily be given independent meaning, without also adopting the dual theory. This can most clearly be demonstrated by analogy. Consider the statement

“A barrel of oil cannot be purchased *solely* with a \$5 bill.” In this sentence the adverb “solely” conveys the idea that some amount of money will be required to make the purchase, but that five dollars is not enough. Absent the word “solely,” the statement might erroneously be interpreted to imply that no amount of U.S. currency could accomplish the sale. In the CALEA proviso, the word “solely” performs the same function: while some amount of legal process will be necessary to obtain location information, certification of relevance under the Pen/Trap Statute is not enough.

This analogy of legal process to legal tender is consistent with the hierarchical structure of electronic surveillance law, which sets a progressively higher threshold as the price for obtaining more intrusive information.³⁵ Granted, the weight here ascribed to the word “solely” is not very great— simply that the legal process associated with a pen/trap order may have some relevance in obtaining cell site data. But then a single adverb in a lengthy and complicated statutory sentence is not often asked to do much semantic heavy-lifting. In any event, the most natural reading of the CALEA proviso reinforces rather than undermines the “greater includes the lesser” structure of the ECPA.

C. The Third Rail: The Stored Communications Act

Many courts rejecting the dual theory do not object to the thesis that a pen/trap order combined with some additional statutory authority is sufficient to obtain cell site data. *See, e.g., CSI Rochester*, 415 F. Supp. 2d 211, 214-15 (W.D.N.Y. 2006). What they do object to is locating that

³⁵ See discussion *supra* at part II.A.

additional authority in the SCA. There are several good reasons for this objection, many of which have not yet been addressed by hybrid proponents.³⁶

Hybrid proponents concede that the SCA was not specifically enacted as the mechanism to collect cell site data. *CSI New York I*, 405 F. Supp. 2d at 447. They further concede that the SCA cannot be a “fully independent source of authority” to obtain cell site data, for essentially two reasons: first, a pen/trap order is itself a necessary, though not sufficient, condition for access to cell site data; second, (as both sides of the dispute agree) the SCA lacks the “structural” features typical of statutes authorizing ongoing surveillance, such as duration limits, periodic reporting, and the like.³⁷ Nevertheless, the SCA is said to be the “most obvious candidate” to be combined with the Pen/Trap Statute, because cell site data falls within the scope of customer “information” to which the SCA generally applies,³⁸ and because the missing structural features of the SCA are supplied by the Pen/Trap Statute.³⁹ According to hybrid proponents, nothing in the SCA prohibits such a combination of authority with the Pen/Trap Statute.

This is incorrect. The SCA does contain a formidable statutory hurdle which hybrid proponents have yet to mention, let alone clear. SCA § 2702(a)(3) expressly prohibits a phone company from disclosing subscriber information “to any governmental entity,” except under certain carefully delineated circumstances. That subsection reads:

³⁶ See *infra* at part II.D.

³⁷ *CSI New York I*, 405 F. Supp. 2d at 447-48. The structural argument against allowing access to cell site data under the SCA is detailed at *CSI Houston I*, 396 F. Supp.2d at 760.

³⁸ The textual argument against SCA coverage of such information is set out at *CSI Houston I*, 396 F. Supp. 2d at 758-59.

³⁹ *CSI New York I*, 405 F. Supp. 2d at 448.

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

* * *

(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.

Six exceptions to this prohibition are listed in § 2702(c), but not one of those exceptions mentions the Pen/Trap Statute.⁴⁰ The first exception (§ 2702(c)(1)) permits disclosure “as otherwise authorized in section 2703.” As all sides agree, a § 2703(d) order is not a stand-alone source of authority for obtaining cell site data; otherwise, there would be no need for a dual theory in the first place. Nor is there anything in § 2703 remotely suggesting a combination of authority with the Pen/Trap Statute. Ironically, § 2703 does mention several alternative legal avenues to obtain subscriber information, in addition to a § 2703(d) order: a Rule 41 search warrant, subscriber consent, a formal written request related to telemarketing fraud investigation, administrative subpoena, grand jury subpoena, and trial subpoena. Notably absent from this list is a pen/trap order, the one statutory mechanism that the dual theory considers indispensable for obtaining cell site data.

⁴⁰ (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;
- (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 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032); or
- (6) to any person other than a governmental entity.

18 U.S.C. § 2702(c).

No other exception listed in § 2702(c) comes even close to authorizing law enforcement access to cell site data in the course of routine criminal investigations. In fact, the sixth exception (authorizing disclosure “to any person other than a governmental entity”) underscores that the primary intent of the prohibition was to guard against unwarranted access to subscriber information *by the government*.

The necessary effect of this omission is to preclude the very authority law enforcement seeks. Section 2702(a)(3) prohibits a phone company from turning over subscriber information “to any governmental entity” except under specified circumstances. None of those circumstances include a pen/trap order. If hybrid proponents are correct that a pen/trap order is an indispensable condition for obtaining cell site data, then the SCA by its very terms *cannot* authorize such disclosure. The dual theory thus self-destructs, its initial premise at war with its intended conclusion.⁴¹

D. Still on the Table: Unanswered Questions

Several other problems confronting the dual theory have yet to be addressed by its proponents. For example: (1) pairing the Pen/Trap Statute and the SCA for this (or any) purpose is not mentioned in any statutory text or discussed in the legislative history; (2) the pairing seems unlikely given the temporal gaps among the relevant statutes: 15 years between the ECPA and the

⁴¹ If this analysis is correct, then phone companies disclosing customer information based on dual orders may be acting in violation of the SCA. A person or entity knowingly violating the SCA may be liable in a civil action for actual damages (a minimum of \$1000 per violation), punitive damages, reasonable attorney fees, and costs. 18 U.S.C. § 2707(c). Immunity is provided if the phone company acts in good faith reliance upon a court order. 18 U.S.C. § § 2703(e), 2707(e)(1). *See McCready v. eBay, Inc.*, No. 05-2450, 05-3043, 2006 WL 1881142 (7th Cir. July 10, 2006) (holding that the good faith defense protected eBay from liability for releasing information pursuant to a subpoena issued by a federal district court where there was no “indication of irregularity sufficient to put eBay on notice that the subpoena was “phony.”).

PATRIOT Act, 7 years between CALEA and the PATRIOT Act, and 4 years between the effective dates of CALEA's amendment of the SCA and the CALEA proviso; and (3) key portions of CALEA's legislative history, such as FBI Director Freeh's express denial that the SCA had any relevance to CALEA's law enforcement assistance provisions,⁴² and the statement of CALEA's House sponsor describing the final bill as "plac[ing] limits on the ability of law enforcement to use portable phones as *tracking devices*."⁴³

Perhaps more fundamentally, none of the decisions adopting the dual theory to date have directly addressed the tracking device definition of § 3117(b):

(b) Definition.--As used in this section, the term "tracking device" means an electronic or mechanical device which permits the tracking of the movement of a person or object.

18.U.S.C. § 3117(b).

⁴² See *Police Access to Advanced Communication Systems: Hearing Before the Subcomm. On Technology and the Law of the Comm. on the Judiciary of the United States Senate and the Subcomm. on Civil and Constitutional Rights of the Comm. on the Judiciary House of Representatives*, 103d Cong. (March 18, 1994) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation), available at 1994 WL 223962. Director Freeh in fact testified before two separate committees, early and late in the legislative process. *Id.* (March 18, 1994); *Wiretapping Access: Hearing Before the Subcomm. on Telecomm. and Fin. of the Comm. on Energy and Commerce U.S. House of Representatives*, 103d Cong. (September 13, 1994) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation), available at 1994 WL 497163. On both occasions Freeh submitted the same written statement emphasizing the separate spheres of the SCA and Pen/Trap Statute. *Wiretapping Access* (September 13, 1994), 1994 WL 497163, at 1. At the later appearance he summarized compromises and changes to the original bill; nowhere in that summary is there a hint that location information could be obtained via a combination of Pen/Trap and SCA authority. *Id.* at 5. ("[T]he assistance requirements in these bills exempt the provision of any location information associated with the use of cellular or mobile communications incidental to the execution of pen register court orders or pursuant to a subpoena.").

⁴³ 140 Cong. Rec. H10773-02, 1994 WL 545775 at p. 36 (statement of Rep. Edwards) (emphasis added).

CSI New York I declared that the tracking device statute was “of no relevance at all because it provides no guidance on the showing needed to install a tracking device.” 405 F. Supp. 2d at 449 n.8. At the time it was true that, although case law uniformly adhered to the probable cause standard, no statute or rule then defined the legal threshold for obtaining a tracking device warrant. Now, however, the legal landscape has changed. Effective December 1, 2006, Rule 41 of the Federal Rules of Criminal Procedure has been amended to expressly cover tracking devices as defined in § 3117(b). *See* proposed Rule 41(a)(2)(E). According to the new rule, a magistrate judge must issue a warrant to install or use a tracking device upon a showing of probable cause. *See* proposed Rule 41(d)(1).⁴⁴

Assorted other reasons have been given to justify by-passing the statutory definition. Some have noted that § 3117 contemplates the “installation” of a tracking device, suggesting that it may not apply in the context of current cell phone technology. *CSI New York I*, 405 F. Supp. 2d at 446 n.6. Yet the Pen/Trap Statute repeatedly uses the same supposedly anachronistic term. *See* 18 U.S.C. §§ 3121-25. Others have argued that no constitutionally protected privacy interests are at stake here, because (a) cell phone users are aware that cell phone signals reveal their location, and have therefore impliedly consented to the intrusion; and (b) a single cell tower will not pinpoint the user’s location within a building. *See, e.g., CSI Shreveport*, 411 F. Supp. 2d 678, 681-82 (W.D. La. 2006).

⁴⁴ As noted in the commentary to the rule, the Supreme Court has not yet squarely addressed whether a tracking device warrant may be based on a lesser showing than probable cause. *See United States v. Karo*, 468 U.S. 705, 718 n.5 (1984) (declining to reach the issue). The amended rule was not intended to resolve that question; “[i]nstead, it simply provides that if probable cause is shown, the magistrate judge must issue the warrant.” 2006 U.S. Order 21, Committee Note, at *11. The court has not found any case holding that a standard lower than probable cause is acceptable.

Whatever the merit of these arguments, they miss the mark here because the question before the court ultimately hinges upon *statutory* authority, not constitutional rights.

Implicit in some of the hybrid cases is the notion that the definition of tracking device in § 3117(b) encompasses only pinpoint or precise location tracking. *See id.*; *CSI New York I*, 405 F. Supp. 2d at 449. Nothing in the text or the legislative history of § 3117(b) offers any support for a restrictive interpretation of its plain and straightforward language. *See CSI Houston I*, 396 F. Supp. 2d at 753-54. Judicially rewriting this definition to include only “precise” tracking of movement would actively encroach upon legislative turf.

For all these reasons, the Government’s application for limited cell site tracking information based on the combined authority of the Pen/Trap Statute and the SCA must be denied.

III. Conclusion

Both issues of electronic surveillance law are decided here as matters of statutory interpretation only. The Government’s reach has exceeded its grasp, at least insofar as the ECPA and its various amendments are concerned.

Nevertheless, constitutional considerations do have an indirect bearing on the result here. The Government’s requests raise Fourth Amendment warning flags, which threaten heavy weather if either were to be allowed. There is a canon of construction known as “constitutional avoidance” which compels a court to construe a statute in a manner which avoids serious constitutional problems, unless such a construction is plainly contrary to the intent of Congress. *Edward J. DeBartolo Corp. v. Florida Gulf Coast Bldg & Constr. Trades Council*, 485 U.S. 568, 575 (1988). This canon is grounded on the presumption that when there are “competing plausible interpretations


of a statutory text,” Congress most likely “did not intend the alternative which raises serious constitutional doubts.” *Clark v. Martinez*, 543 U.S. 371, 381 (2005).

The constitutional difficulties of the dual theory for cell site surveillance are inherent. This statutory argument does not hinge upon the precision of the requested surveillance. If the dual theory were found to authorize the limited cell site data sought here, it must necessarily authorize far more detailed location information, such as triangulation and GPS data, which unquestionably implicate Fourth Amendment privacy rights. *See United States v. Karo*, 468 U.S. 705, 714 (1984). The constitutional problems created by this interpretation of the electronic surveillance statutes are the same, regardless of the breadth of the cell site data sought in a given case. The doctrine of constitutional avoidance was designed to avoid just such difficulties.

As *amici* correctly point out, the Government’s request for dialed digit contents likewise brings the canon of constitutional avoidance into play. The Government’s reading of 18 U.S.C. § 3121(c) would impinge upon Fourth Amendment protections because it permits the collection of communications content without a warrant based on probable cause, in apparent violation of *Katz v. United States*, 389 U.S. 347, 353-54 (1967). Given the presence of a competing interpretation which is not only plausible but more consistent with the statutory text and legislative history, this canon of construction weighs decisively against the Government’s position.

The court’s order of May 23, 2006 denying authority to collect post-cut-through dialed digits and limited cell site information is affirmed in all respects.

Signed at Houston, Texas on July 19, 2006.


Stephen Wm Smith
United States Magistrate Judge