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

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

June 24, 2010

Written Testimony of
United States Magistrate Judge
Stephen Wm. Smith

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

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

1. Role of Magistrate Judges in Electronic Surveillance[1]

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

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

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

---

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

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

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

Another data point is provided by a local survey of such orders issued by our court in Houston from 1995 through 2007. According to that survey, Houston's five magistrate judges issued a total of 4,234 electronic surveillance orders, or about 325 every year.[4] Considering that this volume was generated by less than 1% of the federal magistrate judges in the country, it is safe to conclude that the 2006 total in the FJC study was not a fluke. A reasonable estimate is that the total number of electronic surveillance orders issued at the federal level each year substantially exceeds 10,000.[5]

---

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

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

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

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

2. In Pursuit of Hidden Elephants[6]

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

Still unsatisfied, I plunged into the legislative history of ECPA, reading every committee report and law review article I could find. I contacted law professors who had written about ECPA, as well as a former Congressional staffer who had helped draft the law and subsequent amendments. I met with our local U.S. Marshals, who gave me a tour of their local electronic surveillance shop and a demonstration of the technology. I called various service providers to get their perspective. I then spent several months drafting a memo, setting out my tentative conclusions and supporting analysis. I sent the memo to our local U.S. Attorney, asking him exactly what was wrong with my analysis and why. He forwarded the memo to DOJ, which responded months later with a detailed rebuttal, advocating what has since come to be known as the hybrid theory. Unpersuaded, I issued my first opinion on cell site information in October 2005.[7]

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

---

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

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

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

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

---

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

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

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

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

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

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

Other magistrate judges soon began to weigh in with published decisions of their own. Many agreed with me, some did not. The first opinion with a contrary view was issued in December 2005 by Magistrate Judge Gabriel Gorenstein in the Southern District of New York.[15] He held that a limited form of prospective CSI[16] could be obtained under the SCA standard of specific and articulable facts, a lesser showing than probable cause. His opinion accepted the Government's hybrid theory and provided what remains its most cogent expression to date. In essence, that theory argued that a lesser standard for obtaining this information could be implied from a combination of provisions in three separate statutes.[17] Even as he was adopting the hybrid theory's conclusion, Judge Gorenstein declared the result "unsatisfying,"

---

13 18 U.S.C. § 2510(12)(C).

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

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

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

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

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

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

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

---

18 405 F. Supp. 2d at 442.

19 *Id.* at 449-50.

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

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

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

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

3. A Modest Prescription: Simplicity and Transparency

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

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

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

---

22 Id. at 601.

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

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

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

---

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

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

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

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

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

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

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

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

---

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

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

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

upshot of this system is that, once sealed, an electronic surveillance order is likely to remain sealed long after the underlying investigation is closed, if not forever. This has been confirmed by a study of electronic surveillance orders issued by the Houston Division from 1995 through 2007. Out of 3,886 orders initially sealed "until further order of the court," 3,877 or 99.8% were still under seal as of April 2008.[31]

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

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

---

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

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

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

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

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

> Due to a peculiar combination of circumstances, these sealed orders are entirely off the radar screen, not only for the public at large, but also for appellate courts. Consider a typical pen register order. The only affected party which might have an incentive to object – the targeted e-mail customer or cell phone user – is never given prior notice of the order; in fact, the electronic service provider is usually forbidden from disclosing its existence. The provider is compensated for most expenses in complying with the order; any uncompensated inconvenience hardly justifies an appeal. The government obviously has no reason to object when its application is granted; in the rare case of a denial, why risk an appeal that could make "bad law"? There are always other magistrate judges to try.
>
> Add a sealing order to this mix, and the outcome is a lacuna of law from which little light escapes. This is especially unfortunate because [ECPA] is fiendishly complex, made more so by the passage of the Patriot Act in 2001. Each year . . . busy magistrate judges issue hundreds of ex parte cell phone tracking orders with literally no appellate guidance concerning the proper showing for their issuance – probable cause versus something less. . . Thus, when it comes to marking the bounds of legitimate government intrusion into our electronic lives, each magistrate judge has effectively become a law unto himself. This cannot be a good thing.[35]

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

---

35 *Kudzu, supra* at 211-12.

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

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

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

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

---

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

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

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

39 *See* FED. R. CRIM. P. 41(f)(2)(C).

orders by DOJ.[40]

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

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

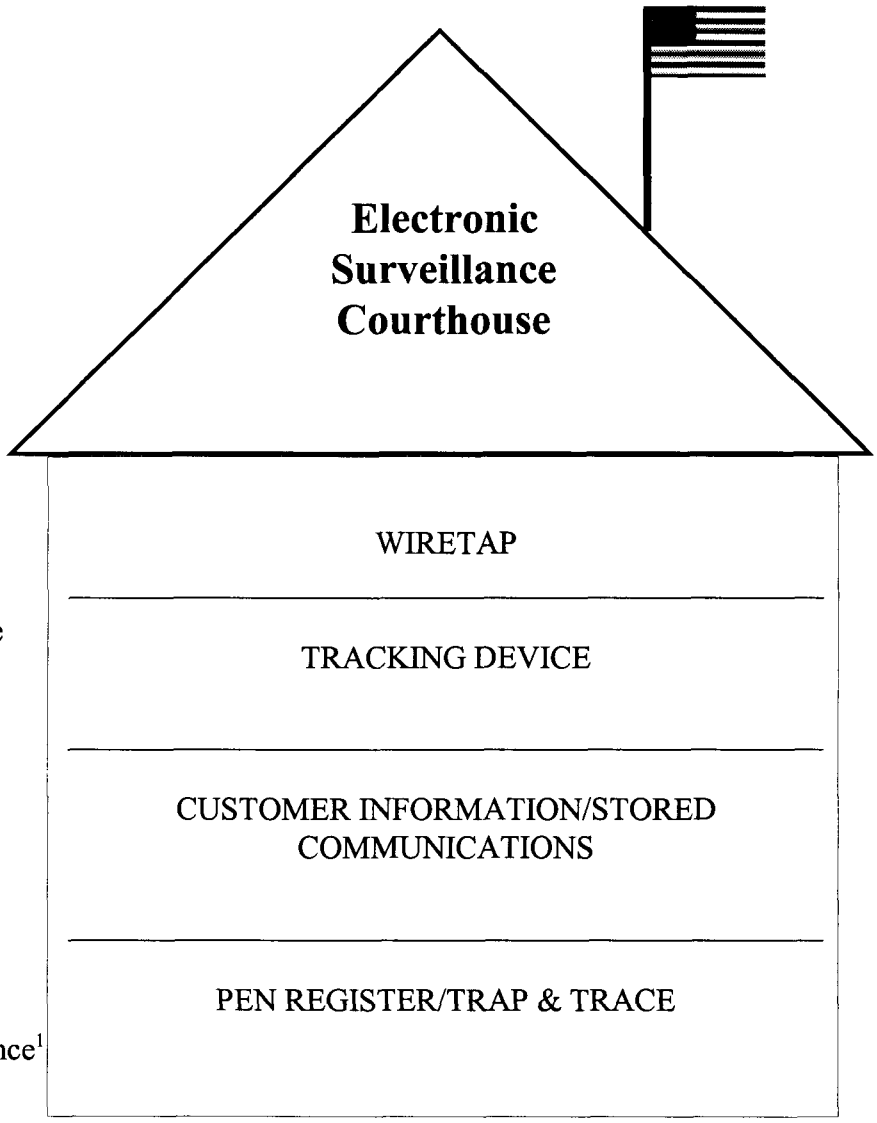
---

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

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

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

EXHIBIT A



Floor	Access Key:
4	Super-Warrant
3	Rule 41 Probable Cause
2	Specific and Articulable Facts
1	Certified Relevance[1]

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

EXHIBIT B

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

I. Prospective Cell Site Information (CSI)

A. Applications Denied Without Probable Cause

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

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

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

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

B. Applications Granted With Less Than Probable Cause

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

No reported opinions.

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

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

II. Historical Cell Site Information

A. Applications Denied Without Probable Cause

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

B. Applications Granted With Less Than Probable Cause*

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

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