Only the DOJ Knows: The Secret Law of Electronic Surveillance

By KEVIN S. BANKSTON*

THIS ARTICLE EXAMINES A TROUBLING PATTERN in the application of federal law enforcement surveillance statutes—namely, those portions of the Electronic Communications Privacy Act of 1986[1] (the "ECPA") sometimes known as the Pen Register Statute[2] ("PRS") and the Stored Communications Act[3] ("SCA")—whereby federal prosecutors secretly and routinely obtain court authorization for surveillance that Congress did not intend and which may violate the Fourth Amendment.

Case studies demonstrate how the United States Department of Justice ("DOJ") regularly applies for and receives secret surveillance authority from magistrate judges across the country, based on often-implicit legal arguments that are dubious at best and deceptive at worst. These case studies of legally questionable yet routine surveillance demonstrate how the government is steadily increasing its surveillance authority beyond the bounds of the law, shielded by the secrecy of the *ex parte* surveillance application process. The government has achieved this erroneous authority through reliance on often-unspoken and legally unsound arguments that are deployed for years at a stretch without being subjected to meaningful judicial scrutiny. Indeed, the case studies reveal that the DOJ has often actively avoided judicial scrutiny of the legal rationales behind its surveillance applications. This raises several questions: How many thousands of illegal and unconstitutional surveillances have been authorized in this

* Staff Attorney, Electronic Frontier Foundation (EFF). Thanks to Susan Freiwald and Lee Tien for their suggestions and support.

1. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C.A. §§ 2510–22, 2701–12, 3117, 3121–27 (West 2000 & Supp. 2006)).

2. Electronic Communications Privacy Act of 1986, Title III, § 301 (codified as amended at 18 U.S.C.A. §§ 3121–27 (West 2000 & Supp. 2006)). This portion of the ECPA is also sometimes known as the "Pen/Trap Statute."

3. Electronic Communications Privacy Act of 1986, Title II, § 201 (codified as amended at 18 U.S.C.A. §§ 2701–12 (West 2000 & Supp. 2006)).

manner? What other types of unlawful surveillance are federal prosecutors asking for and obtaining the permission to conduct? And, as one newly vigilant and obviously frustrated magistrate has asked, "*How long has this been going on?*"[4]

Only the DOJ knows.

This Article provides three case studies, describing three different types of surveillance that the DOJ has wrongfully and routinely obtained the authority to conduct under the PRS and the SCA. Part I, after a brief primer on the law of telephone surveillance, examines the first case study: warrantless wiretapping of digits dialed after a phone call has been completed. Part II, after providing an additional primer on the SCA's regulation of government access to stored communications and communications records, discusses the recent example of warrantless cell phone location tracking. Finally, Part III considers the historic example of warrantless surveillance of internet traffic data, prior to the PATRIOT Act's[5] authorization of such surveillance.

The Article concludes by briefly considering the causes of this routine and secret expansion of law enforcement surveillance authority. It proposes prescriptions to break the pattern of expansion, calling on Congress to amend the ECPA and calling on magistrates to follow the example of several judges noted in the case studies. These magistrates, when considering novel and troublesome surveillance applications, made the commendable decision to solicit the assistance of adversarial amici such as criminal defense attorneys and civil liberties organizations. More importantly, these magistrates chose to issue published written opinions that informed the public and provided guidance to their colleagues on the bench. Unfortunately, and as the case studies will show, this is a step that the vast majority of magistrates fail to take when considering applications from the government for permission to conduct surveillance. If more magistrates routinely published such decisions, the DOJ's practical monopoly on information about how it uses (or abuses) its surveillance powers would be put to an end, and the *ex parte* expansion of government surveillance authority would be conclusively exposed.

4. *In re* Application of the United States for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info., 396 F. Supp. 2d 294, 320 (E.D.N.Y. 2005) [hereinafter *Orenstein Opinion II*].

5. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("PATRIOT Act") of 2001, Pub. L. No. 107-56, 115 Stat. 272.

Before moving to the case studies, however, a disclaimer is in order. The author is currently a staff attorney who litigates government surveillance issues on behalf of the Electronic Frontier Foundation[6] ("EFF"), a non-profit civil liberties organization. As specified where appropriate, EFF has opposed the government in many of the cases discussed herein. Therefore, note that although the opinions herein are the author's own and do not necessarily reflect EFF's official positions, this Article is—admittedly and proudly, for better or for worse—a front-line dispatch from a privacy partisan.

I. Case Study: Warrantless Wiretapping of Post-Cut-Through Dialed Digits

Perhaps you have used your bank's automated telephone service, dialing a pass code to access your account and conduct your business using the buttons on your phone. Perhaps you have ordered a prescription from the drugstore in a similar manner, or dialed through the automated technical support tree offered by your computer vendor, or dialed to purchase from a catalog or book a plane flight, or pressed "1" to pick your favorite "American Idol." In the world of electronic surveillance, those digits you dial after you have dialed a phone number and the phone company has connected your call are known as "Post-Cut-Through Dialed Digits" ("PCTDDs").[7]

These PCTDDs are the subject of the first case study, which demonstrates that the government has for many years wiretapped PCTDDs without probable cause as a routine matter. The government has regularly engaged in such wiretapping despite repeated instructions from Congress not to do so and despite the dictates of the Fourth Amendment. Before delving into this case study, though, a brief introduction to the law of telephone surveillance is necessary.

A. Primer: The Wiretap Act, the Pen Register Statute, and the Fourth Amendment

Although intimidating in its details, the law surrounding telephone surveillance by law enforcement is relatively straightforward. Both statutory law and the Supreme Court's Fourth Amendment precedents clearly distinguish between the contents of telephone

6. Electronic Frontier Foundation, http://www.eff.org (last visited May 15, 2007).

7. *See, e.g.*, U.S. Telecom Ass'n v. FCC, 227 F.3d 450, 462 (D.C. Cir. 2000) (defining PCTDDs and giving examples).

calls, which are subject to strong legal protections, and the numbers that callers dial in order to place them, which are not.

Title III of the Omnibus Crime Control and Safe Streets Act of 1968[8] (the "Wiretap Act" or "Title III") requires the government to obtain a specialized court order (known as a "Wiretap Order") before its agents may use a wiretapping device to acquire someone's phone calls—or, as defined in the Act, before "intercept[ing]" the "content" of someone's "wire communications" with an "electronic, mechanical or other device."[9] Congress passed the Wiretap Act in response to two Supreme Court cases that had recently been decided, *Berger v. New York*[10] and *Katz v. United States.*[11] Those cases held that the Fourth Amendment protects private conversations from search and seizure via electronic eavesdropping.[12] Through the Wiretap Act, Congress intended to address the Supreme Court's Fourth Amendment concerns by providing a strict warrant procedure for such eavesdropping[13] with procedural safeguards so demanding that one noted commentator routinely refers to Wiretap Orders as "super-warrants."[14]

In 1979, the Supreme Court addressed another form of telephonic surveillance: the use of "pen registers," devices that attach to a phone line and record outgoing phone numbers dialed on that line.[15] In *Smith v. Maryland,*[16] the Court sharply distinguished between the contents of phone conversations and the phone numbers acquired by

8. Pub. L. No. 90-351, § 802, 82 Stat. 212 (codified as amended at 18 U.S.C.A. §§ 2510–22 (West 2000 & Supp. 2006)).

9. 18 U.S.C.A. § 2510 (West 2000 & Supp. 2006) (definitions); 18 U.S.C.A. § 2511 (West 2000 & Supp. 2006) (generally prohibiting interception); 18 U.S.C.A. § 2518 (West 2000 & Supp. 2006) (describing application and court order for interception).

10. 388 U.S. 41 (1967).

11. 389 U.S. 347 (1967).

12. *See Berger*, 388 U.S. at 57–60 (holding the State's electronic eavesdropping statute to be facially unconstitutional for lack of adequate Fourth Amendment safeguards); *Katz*, 389 U.S. at 353 (finding a Fourth Amendment expectation of privacy in the content of telephone calls made from a closed phone booth, which was violated when the government installed a listening device on the exterior of the booth).

13. *See* United States v. Tortorello, 480 F.2d 764, 773–75 (2d Cir. 1973) (noting that Congress designed the Wiretap Act to address the Fourth Amendment concerns identified by the Supreme Court in *Berger* and *Katz*, and finding that the Act's exacting requirements "d[o] not suffer from the infirmities that the Court found fatal" to the eavesdropping statute at issue in *Berger*).

14. *See, e.g.*, Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother that Isn't*, 97 NW. U. L. REV. 607, 630 (2003).

15. "[A] pen register . . . record[s] the numbers dialed from [a] telephone . . . ." Smith v. Maryland, 442 U.S. 735, 737 (1979).

16. *Id.*

pen register surveillance.[17] Although the Fourth Amendment protects the contents of a phone call under *Katz*, the Court in *Smith* held that dialed phone numbers, which do not reveal a phone conversation's contents, are not so protected.[18]

In 1986, Congress addressed the issue of pen register surveillance as part of the ECPA. Consistent with dialed digits' degraded Fourth Amendment status under *Smith*, Congress chose not to require a "super-warrant" for pen register surveillance. Rather, the ECPA's PRS authorized the issuance of court orders for the installation or use of pen registers to collect outgoing phone numbers—as well as "trap and trace" devices to collect incoming phone numbers—without a showing of probable cause.[19] These "Pen-Trap Orders" were much easier for the government to obtain than Wiretap Orders and lacked many of the procedural safeguards and accountability measures built into the Wiretap Act.[20] Most notably, rather than requiring a probable cause showing, the PRS allowed the government to obtain Pen-Trap Orders based only on a certification that the information sought is relevant to an ongoing criminal investigation.[21] However, and consistent with the Supreme Court's holding in *Katz*, Pen-Trap Orders could authorize only the collection of dialed numbers;[22] the Wiretap Act continued to protect call content against warrantless interception.[23]

This simple, constitutionally-derived statutory distinction between call contents and dialed numbers was soon to be disrupted, however,

17. "[A] pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications." *Id.* at 741. As the Court continued:

> Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed—a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.

Id. (quoting United States v. New York Tel. Co., 434 U.S. 159, 167 (1977)).

18. *Id.*

19. *See generally* 18 U.S.C.A. §§ 3121–27 (West 2000 & Supp. 2006).

20. *Id.* This lack of procedural safeguards in the PRS as compared to the Wiretap Act is detailed and criticized in Part IV.

21. *See* 18 U.S.C. § 3122(b)(2) (1986) (requiring that the government's application contain a certification of relevance); 18 U.S.C. § 3123(a)(1) (1986) (stating that the court "shall" issue a Pen-Trap Order upon such application).

22. 18 U.S.C. § 3127(3) (1986) (defining pen registers as devices that collect phone numbers).

23. 18 U.S.C. § 2510 (1986) (defining "intercept" as the acquisition of the contents of a communication).

when phone technology advanced to the point where people could use PCTDDs to communicate messages.

B. 1994: Congress Considers the Curious Case of Dialed Digits that Contain Content

In 1986, when Congress passed the PRS as part of the ECPA, rotary phones were still in widespread use. Therefore, Congress did not have reason to consider the possibility that after calls were connected, dialed digits could be used to communicate. Instead, Congress assumed that dialed digits could not include the content of communications,[24] and as a result the pen register definition did not (and at that time, did not need to) explicitly exclude devices that acquired content.[25]

By 1994, however, when Congress was considering passage of the Communications Assistance for Law Enforcement Act[26] ("CALEA"), it had become clear that callers were using dialed digits to communicate a wide variety of content. The following exchange between Senator Leahy and FBI Director Freeh reflected this new awareness:

> SEN. LEAHY: You say [CALEA] 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 cncede [sic] 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

24. A pen register "does not [record] the contents of a communication, rather it records the numbers dialed." H.R. REP. No. 99-647, at 78 (1986); *see also* People v. Bialostok, 610 N.E.2d 374, 378 (N.Y. 1993) ("The traditional pen register [considered in *Smith v. Maryland*] was, to a large extent, self-regulating. Neither through police misconduct nor through inadvertence could it reveal to anyone any information in which the telephone user had a legitimate expectation of privacy.").

25. The original PRS defined a pen register as "a device which records or decodes electronic or other impulses which identify numbers dialed or otherwise transmitted on the telephone line to which such device is attached." 18 U.S.C. § 3127(3) (1986); *see also* 18 U.S.C. § 3127(4) (providing the definition of a "trap and trace device").

26. Communications Assistance for Law Enforcement Act ("CALEA") of 1994, Pub. L. No. 103-414, 108 Stat. 4279 (codified at 47 U.S.C. § 1001-10 (2000) and in scattered sections of 18 U.S.C.). *See generally* Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949 (1996) [hereinafter Freiwald, *Uncertain Privacy*] (recounting the history of the passage of CALEA).

> it, don't need it, and *I'm willing to have technological blocks with respect to that information* . . . .[27]

As a result of this new concern over the government using pen registers to collect dialed digits that were not used to route calls, and in response to Director Freeh's willingness to accept "technological blocks" with respect to such information, Senator Leahy inserted into CALEA a provision to "further protect [ ] privacy . . . by restricting the ability of law enforcement to use pen register devices for tracking purposes or for obtaining transactional information."[28] When first enacted in 1994, this new privacy-protective provision—codified at 18 U.S.C. § 3121(c)—stated:

> *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.[29]

As for those dialed digits not used for call processing—i.e., those PCTDDs containing content—no published decisions in the following years directly decided the issue, but commentators assumed that the acquisition of such dialed digits would require a Wiretap Order.[30] As the D.C. Circuit explained in 2000, "[s]ome [PCTDDs] are telephone numbers, such as when a subject places a calling card, credit card, or collect call by first dialing a long-distance carrier access number and then, after the initial call is 'cut through,' dialing the telephone number of the destination party."[31] However, as the court further explained, PCTDDs also have other uses where they "can also represent

27. *Wiretapping: J. Hearing of the Tech. and Law Subcomm. of the S. Judiciary Comm. and the Civil and Constitutional Rights Subcomm. of the H. Judiciary Comm.*, 103d Cong. 50 (1994) (emphasis added), *available at* http://www.eff.org/Privacy/Surveillance/CALEA/freeh_031894_hearing.testimony.

28. H.R. REP. No. 103-827, at 10 (1994) (emphasis added); *see also id.* at 32 (provision "requires government agencies . . . to use, when reasonably available, technology that restricts the information captured by [a pen register] to the dialing or signaling information necessary to direct or process a call, excluding any further communication conducted through the use of dialed digits that would otherwise be captured.").

29. CALEA § 207, 108 Stat. 4279, 4292 (emphasis added).

30. *See, e.g.*, Kerr, *supra* note 14, at 642 ("[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.").

31. United States Telecom Ass'n v. FCC, 227 F.3d 450, 462 (D.C. Cir. 2000). *See also id.* at 456 (PCTDDs "include . . . the telephone numbers dialed after connecting to a dial-up long-distance carrier (*e.g.*, 1-800-CALL-ATT)."). EFF was one of the petitioners in this case challenging the FCC's implementation of CALEA on privacy grounds.

call content."[32] Therefore "it may be that a Title III [Wiretap Act] warrant is required to receive all post-cut-through digits."[33]

The DOJ did not consider this "may be" as a serious possibility, however. As would soon be revealed, the government's routine practice even after passage of CALEA was to collect all PCTDDs—including those representing call content—based solely on Pen-Trap Orders.

C. 2001: Congress (Again) Considers the Curious Case of Dialed Digits that Contain Content

Congress revisited the issue of PCTDDs when considering passage of the PATRIOT Act in the fall of 2001, and one could almost hear the annoyance in Senator Leahy's voice as he revealed from the floor a surprising admission by the government:

> 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 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 [i.e., the direction on use of reasonably available technology] more seriously and *actually implement it.*[34]

Plainly, Senator Leahy intended § 3121(c) to require the use of *some kind* of filtering where content was concerned, so that it could not be collected upon a mere relevance standard in violation of the Constitution. Therefore, the PATRIOT Act of 2001 addressed the concern that CALEA's addition of § 3121(c) apparently failed to resolve. The PATRIOT Act accomplished this by amending the definitions of "pen register" and "trap and trace device" to explicitly prohibit the collec-

32. *Id.* at 462 ("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.").

33. *Id.*

34. 147 CONG. REC. S11000 (daily ed. Oct. 25, 2001) (remarks of Sen. Leahy) (emphasis added).

tion of any communications content,[35] and by adding the phrase "so as not to include the contents of any wire or electronic communications" to the end of § 3121(c) in order to further strengthen its filtering requirement.[36]

Certainly, after those amendments no one could doubt that the government could not use pen registers to collect dialed digit content.[37] Right?

Wrong.

D. Showdown in Texas, 2006: The First Published Dialed Digit Surveillance Decision

In July of 2006, federal Magistrate Judge Stephen William Smith of the Southern District of Texas took the rare step of publishing his denial of an *ex parte* application by the government for surveillance authorization,[38] after taking the nearly unprecedented step of soliciting amici on the issue.[39] That decision is the first and only published opinion evaluating the legality of an application for PCTDD surveillance under the PRS. The opinion revealed that the government is *still* using pen registers to acquire all PCTDDs, even those that represent the contents of communications:

35. *See* 18 U.S.C.A. §§ 3127(3)–(4) (West Supp. 2006) (requiring that information recorded, decoded, or captured by pen registers or trap and trace devices, respectively, "shall not include the contents of any communication").

36. *See* 18 U.S.C.A. § 3121(c) (West Supp. 2006) (requiring use of "technology reasonable available" to restrict recordings "to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications").

37. *See, e.g.*, *In re* Application of the United States of America for an Order Authorizing the Use of a Pen Register and Trap on [xxx] Internet Service Account/User Name [xxxxxxxx@xxx.com], 396 F. Supp. 2d 45, 48 (D. Mass. 2005) (expressing skepticism, in dicta, that "anyone [would] doubt" that the amended 18 U.S.C. § 3127(3) prohibits a pen register from collecting PCTDD content).

38. *See In re* the Application of the United States of America for an Order Authorizing (1) Installation & Use of a Pen Register & Trap & Trace Device or Process, (2) Access to Customer Records, & (3) Cell Phone Tracking, 441 F. Supp. 2d 816 (S.D. Tex. 2006) [hereinafter *Smith Opinion II*].

39. EFF, joined by the Center for Democracy and Technology responded to the court's invitation and filed an amicus brief opposing the government's application. *See* Brief Amicus Curiae of EFF & Center for Democracy and Technology in Regard to Court's May 24, 2006 Order on Post-Cut-Through Dialed Digits, *In re* Application of the United States for an Order Authorizing (1) Installation & Use of a Pen Register & Trap & Trace Device or Process, (2) Access to Customer Records, & (3) Cell Phone Tracking, No. H-06-356M (S.D. Tex. Jun. 30, 2006), *available at* http://www.eff.org/legal/cases/Pen_Trap/EFF-and-CDT-Amicus.pdf.

> 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.[40]

Judge Smith, agreeing with amici's arguments,[41] declined to grant the government's request for authorization in an opinion worth quoting at length:

> 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.[42]

As Judge Smith continued, his tone echoed Senator Leahy's frustration from the Senate floor:

> 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.*[43]

40. *Smith Opinion II,* 441 F. Supp. 2d at 825 (emphasis added).

41. *Id.* at 824, 825, 837 (referring to EFF and Center for Democracy and Technology's argument from their amicus brief filed in this case).

42. *Id.* at 824–25.

43. *Id.* at 825–26 (emphasis added).

Judge Smith concluded by holding that "Section 3121(c) is a limitation, not a license."[44] "Because the Pen/Trap Statute triply forbids what the Government requests," Judge Smith held that the government may only acquire PCTDD content after obtaining a Wiretap Order based on probable cause. Accordingly, he denied the Government's application for a Pen-Trap Order.[45]

One might expect that the government, in light of Judge Smith's stinging public condemnation of its routine surveillance practice, would either appeal the decision or abandon the practice. The government has done neither. Instead, as described below, the DOJ brazenly continues to apply to other magistrates for Pen-Trap Orders authorizing the collection of all PCTDDs, based on ever more dubious arguments.

E. Brooklyn, 2007: Shifting Arguments in the Latest PCTDD Case

Since Judge Smith's decision, a more recent case in Brooklyn—which unfortunately has not yet resulted in any published decision—has shed new light on the DOJ's troubling tactics in the pursuit of Pen-Trap Orders authorizing the collection of PCTDD content.[46] There, Magistrate Judge Joan M. Azrack of the Eastern District of New York recently denied the government's *ex parte* applications for Pen-Trap Orders authorizing the collection of all PCTDDs, pending further briefing by the government.[47] The resulting government brief to Judge Azrack,[48] a copy of which has been provided to EFF,[49] contains

44. *Id.* at 827.

45. *Id.*

46. An attorney with the Federal Defenders of New York informed the author of this case. *See* E-mail from Yuanchung Lee, Assistant Federal Defender, Appeal Bureau, Federal Defenders of New York, to Kevin Bankston, Staff Attorney, EFF (Jan. 19, 2007, at 12:36:26 PST) (on file with author) (alerting author to case, *In re Applications of the United States of America for Orders (1) Authorizing the Use of a [sic] Pen Registers & Trap & Trace Devices & (2) Authorizing Release of Subscriber Information*, 06 Misc. 547 JMA, 06 Misc. 561 JMA (E.D.N.Y.), and providing a copy of the Government's brief). *See* Government's Memorandum of Law in Support of its Requests for Authorization to Acquire Post-Cut-Through Dialed Digits Via Pen Registers, *In re* Applications of the United States of America for Orders (1) Authorizing the Use of a [sic] Pen Registers & Trap & Trace Devices & (2) Authorizing Release of Subscriber Info., 06 Misc. 547 JMA, 06 Misc. 561 JMA (E.D.N.Y. Jan. 19, 2007) [hereinafter Brief of DOJ Regarding PCTDD in EDNY] (on file with author).

47. *See* E-mail from Yuanchung Lee, Assistant Federal Defender, Appeal Bureau, Federal Defenders of New York, to Kevin Bankston, Staff Attorney, EFF (Jan. 24, 2007, at 13:07:52 PST) (on file with author) (noting that briefing resulted from Judge Azrack's previous denial of applications).

48. *See* Brief of DOJ Regarding PCTDD in EDNY, *supra* note 46.

49. The government's brief was provided to EFF by the Federal Defenders of New York, who were invited by Judge Azrack to serve as an amicus in the case. *See* E-mail from

a troubling new argument that the government did not make in front of Judge Smith.

In the previous case before Judge Smith, government lawyers had reassured the court that they would voluntarily forego any investigative use of ill-gotten PCTDD content, consistent with the DOJ's own internal policy.[50] However, the government's need to rely on this voluntary pledge against the use of contents collected via pen-trap surveillance only served to highlight the fact that the PRS, unlike the Wiretap Act, does not contain a statutory requirement that government agents minimize the collection of information that they lack authority to collect.[51] More importantly, the government's reliance on its internal policy against the use of over-collected content underscored the absence of any statutory exclusionary rule in the PRS analogous to that in the Wiretap Act,[52] which prohibits the government from using unlawfully intercepted communications as evidence. Congress's failure to require minimization and prohibit the use of content acquired by pen-trap surveillance only strengthened the argument that Congress never intended for pen-trap devices to collect any content at all.[53]

Yuanchung Lee, *supra* note 47, and Memorandum of Law by Amicus Curiae Federal Defenders of New York, as Amicus Curiae Opposing the Government, *In re* Government Applications Seeking Authorization to Intercept All PCTDD Via a Pen Register Order, 06 Misc. 547 JMA, 06 Misc. 561 JMA (E.D.N.Y. Feb. 9, 2007) (on file with author).

50. *See Smith Opinion II*, 441 F. Supp. 2d 816, 822 n.14 (S.D. Tex. 2006) (quoting Memorandum from Deputy Att'y Gen., Larry D. Thompson, to Various Government Officials, Assistant Attorneys General, and All United States Attorneys, 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).

51. *See* 18 U.S.C. § 2518(5) (1986) (providing that wiretaps "shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter [the Wiretap Act]"). Where minimization cannot reasonably be accomplished at the time of interception, "minimization may be accomplished as soon as practicable after such interception." *Id.*

52. *See* 18 U.S.C.A. § 2515 (West Supp. 2006) (prohibiting the use of unlawfully intercepted wire or oral communications as evidence).

53. *See* Brief Amicus Curiae of EFF & Center for Democracy & Technology in Regard to Court's May 24, 2006 Order on Post-Cut-Through Dialed Digits, at 10 n.7, *In re* the United States for an Order Authorizing (1) Installation & Use of a Pen Register & Trap & Trace Device or Process, (2) Access to Customer Records, & (3) Cell Phone Tracking, No. H-06-356M (S.D. Tex. June 30, 2006), *available at* http://www.eff.org/legal/cases/Pen_Trap/EFF-and-CDT-Amicus.pdf.

> The Government attempts to salvage its position by insisting that where content is collected, "no affirmative investigative use shall be made of that information except to prevent immediate danger of death, serious bodily injury, or harm to the national security." Yet the need for such a voluntary pledge only underscores the fact that the Pen/Trap Statute lacks any 'minimization' requirement because it does not contemplate the 'overcollection' of content—unlike the Wiretap Act,

Judge Smith was therefore not swayed by the existence of the government's voluntary policy, and two unpublished decisions[54] that came to light during the proceeding in front of Judge Azrack demonstrated how the government's reliance on that policy had backfired in front of other courts as well. The two Florida judges that issued those decisions in the summer of 2006, like Judge Smith, had not been convinced by the government's assurances that it would voluntarily avoid using any PCTDD content, and therefore had rejected the government's application for a Pen-Trap Order to acquire all PCTDDs.[55] As Magistrate Karla R. Spaulding in Orlando had dismissively put it: "The Department of Justice's unenforceable policy not to use content captured by pen register and trap and trace devices, except when it really needs to, cannot override the clear requirements of the statute [that such devices by definition not collect content]."[56] District Court Judge Anne C. Conway, to whom the DOJ appealed Spaulding's decision, agreed. She affirmed the denial of the government's application and noted that the court could not "cede to the executive branch its responsibility to safeguard the Fourth Amendment" based on the DOJ's policy.[57]

---

which specifically provides for post-collection minimization. Had Congress anticipated that content could be swept up by a pen/trap device, it would certainly have required minimization. The absence of such a requirement makes clear that Congress did not expect content to be collected.

Id. (internal citations omitted).

54. *In re* Application of the United States of America for an Order Authorizing the Installation & Use of an Electronic Computerized Data Collection Device Equivalent to a Pen Register & Trap & Trace Device, No. 6:06-MJ-1130 (M.D. Fla. June 20, 2006) (Conway, J.), *aff'g* magistrate judge's decision in *In re* Application of the United States of America for an Order Authorizing the Installation & Use of an Electronic Computerized Data Collection Device Equivalent to a Pen Register & Trap & Trace Device, No. 6:06-MJ-1130 (M.D. Fla. May 23, 2006) (Spaulding, Mag.) (both decisions on file with author).

55. *See In re* Application of the United States of America for an Order Authorizing the Installation & Use of an Electronic Computerized Data Collection Device Equivalent to a Pen Register & Trap & Trace Device, No. 6:06-MJ-1130 at 2 (M.D. Fla. May 23, 2006) (Spaulding, Mag.) (on file with author); *In re* Application of the United States of America for an Order Authorizing the Installation & Use of an Electronic Computerized Data Collection Device Equivalent to a Pen Register & Trap & Trace Device, No. 6:06-MJ-1130 at 5–6 (M.D. Fla. June 20, 2006) (Conway, J.) (on file with author).

56. *In re* Application of the United States of America for an Order Authorizing the Installation & Use of an Electronic Computerized Data Collection Device Equivalent to a Pen Register & Trap & Trace Device, No. 6:06-MJ-1130 at 2 (M.D. Fla. May 23, 2006) (Spaulding, Mag.) (on file with author).

57. *In re* Application of the United States of America for an Order Authorizing the Installation & Use of an Electronic Computerized Data Collection Device Equivalent to a Pen Register & Trap & Trace Device, No. 6:06-MJ-1130 at 5–6 (M.D. Fla. June 20, 2006) (Conway, J.) (on file with author).

The reactions of Judges Smith, Spaulding, and Conway to the invocation of internal DOJ policies must have indicated to the Government that its approach was not working. Therefore, when the government appeared before Judge Azrack, it debuted a new and seemingly straightforward argument to support its claim that section 3121(c) of the PRS, rather than "disallow[ing] all content" as Judge Smith had concluded, allows agents to collect all PCTDDs.[58] The government claimed, for the first time, that the *Wiretap Act*'s statutory exclusionary rule, codified at 18 U.S.C. § 2515, applied to content collected by pen register.[59]

Under the DOJ's new argument, the Wiretap Act's statutory exclusionary rule prohibits the government from making use of PCTDD content that it acquires while implementing a Pen-Trap Order. Courts therefore need not worry that the DOJ will make use of content "incidentally" collected by a pen register, because such content and any evidence derived from it can only be used a trial when its interception is authorized under the Wiretap Act. This interpretation, if correct, would reassuringly eliminate the concern that the DOJ might violate its voluntary policy and would conveniently explain the lack of an exclusionary rule in the PRS itself. As the government's brief summarized,

> Since Title III's inception, [the Wiretap Act] has contained the following comprehensive prohibition on use by the government of the contents of wire communications in the event they are acquired without Title III's requisites for interception having been satisfied:
>
> > Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee or any other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.
>
> 18 U.S.C.[A.] § 2515 (West 2006). Accordingly, [the Wiretap Act] precludes the government from making direct or derivative use [of

58. *See* Brief of DOJ Regarding PCTDD in EDNY, *supra* note 46, at 12–14; *Smith Opinion II*, 441 F. Supp. 2d at 824-25.

59. *See* Brief of DOJ Regarding PCTDD in EDNY, *supra* note 46, at 11–12 (arguing that courts can construe the PRS "to permit a pen register to access PCTDD content incidental to collecting non-content" because that content is subject to the Wiretap Act's exclusionary remedy for surveillance that does not satisfy its requirements).

> any PCTDD content unless its interception was authorized by Title III].[60]

Again, this seems pretty straightforward; right?

There is only one problem: This new argument contradicts the DOJ's own official position on the scope of the Wiretap Act's exclusionary rule. As the DOJ has successfully argued in front of numerous courts, that rule requires only the exclusion of unlawfully intercepted *wire* and *oral* communications and does not apply to *electronic* communications.[61] Because PCTDDs do not contain the human voice, it seems clear that the government would view them as electronic communications[62] rather than wire communications[63] or oral communications.[64] To be consistent with its well-established positions, then, the government would have to argue that the Wiretap Act's exclusionary rule does *not* apply when pen registers acquire PCTDDs that convey content. Yet the government's brief to Judge Azrack repeatedly claims

60. Brief of DOJ Regarding PCTDD in EDNY, *supra* note 46, at 6.

61. *See* United States v. Forest, 355 F.3d 942, 949 (6th Cir. 2004) (finding that cell phone location information was not a wire or oral communication and therefore could not be suppressed under the statute), *cert. denied*, 543 U.S. 856 (2004); United States v. Steiger, 318 F.3d 1039, 1050–51 (11th Cir. 2003) (finding that e-mails, as electronic communications, could not be suppressed under the statute), *cert. denied*, 538 U.S. 1051 (2003); United States v. Meriwether, 917 F.2d 955, 960 (6th Cir. 1990) (finding that statute did not require suppression of electronic communications such as numbers transmitted to pagers); United States v. Wells, 2000 WL 1231722, at *5–7 (S.D. Ind. Aug. 29, 2000) (same); United States v. Reyes, 922 F. Supp. 818, 837 (S.D.N.Y. 1996) (same). The Senate Report on ECPA further makes clear that this exclusionary rule was not intended to cover electronic communications. *See* S. REP. No. 99-541, at 23 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3577. Indeed, this omission has garnered a fair amount of academic criticism, including from a former DOJ computer crime trial attorney. *See* Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805 (2003) [hereinafter Kerr, *Lifting the "Fog" of Internet Surveillance*]; Michael S. Leib, *E-mail & the Wiretap Laws: Why Congress Should Add Electronic Communication to Title III's Statutory Exclusionary Rule & Expressly Reject a "Good Faith" Exception*, 34 HARV. J. ON LEGIS. 393 (1997).

62. An "electronic communication" is "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce," but does not include wire communications, i.e., transfers containing the human voice. 18 U.S.C. § 2510(12) (2000).

63. A "wire communication" is "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection. . . ." 18 U.S.C.A. § 2510(1) (West Supp. 2006). An "aural transfer" is "a transfer containing the human voice." *Id.* § 2510(18).

64. An "oral communication" is defined as a communication "uttered by a person" and "does not include any electronic communication." 18 U.S.C. § 2510(2) (2000).

that the availability of the Wiretap Act's exclusionary rule supports its application to collect PCTDD content via pen register.[65]

Reading its brief closely, however, one can see that the government directly asserts only that the Wiretap Act's exclusionary remedy applies to wire communications and then implies—without stating outright—that PCTDDs are wire communications.[66] The government's failure to explicitly argue that PCTDDs are wire communications covered by the Wiretap Act's exclusionary rule appears designed to give it the benefit of that rule's application when seeking authorization for surveillance, while preserving its ability to later argue that PCTDDs are electronic communications after all and therefore cannot be excluded from evidence.[67]

Even assuming that the government's implicit argument that PCTDDs are wire communications is correct, though, the Wiretap Act's exclusionary rule still would not apply under the government's logic. If devices that collect all PCTDDs are "pen registers,"[68] as the government claims, then content collected by such devices is not subject to the Wiretap Act's exclusionary rule. This is because the exclusionary rule reaches only communications intercepted in violation of the Wiretap Act,[69] and the Act explicitly exempts pen register investigations from its prohibitions on interception. In particular, the Wiretap Act provides: "It shall not be unlawful under this chapter . . . to use a pen register or a trap and trace device."[70]

This provision is yet another indicator of Congress's original and continuing understanding that pen registers and trap and trace devices by definition cannot intercept content.[71] This understanding

65. *See* Brief of DOJ Regarding PCTDD in EDNY, *supra* note 46, at 3, 4, 6, 11–12, 17–18.

66. *See id.*

67. To be clear, as a privacy activist, I would be delighted if the government's new argument represented a concession by the DOJ to a definition of excludable "wire communications" that is broad enough to include PCTDDs and similar information. However, based on its evasive language, no such concession is apparent.

68. *See* Brief of DOJ Regarding PCTDD in EDNY, *supra* note 46, at 4 (arguing that the definition of "pen register" at 18 U.S.C. § 3127(3) must "be read . . . to permit a pen register incidental access to content"); *id.* at 5 (arguing that "the Pen/Trap Statute permits . . . pen registers to access PCTDD content.").

69. *See* 18 U.S.C. § 2515 (West Supp. 2006).

70. 18 U.S.C.A. § 2511(2)(h)(i) (West 2000 & Supp. 2006).

71. *See* H.R. REP. No. 99-647, at 78 (1986) (stating that a pen register "does not [record] the contents of a communication, rather it records the numbers dialed"); 18 U.S.C.A. §§ 3127(3)–(4) (West Supp. 2006) (requiring that information recorded, decoded, or captured by pen registers or trap and trace devices, respectively, "shall not include the contents of any communication").

runs completely counter to the DOJ's argument that a pen register is any device that acquires non-content dialing information, regardless of whether it also (or even mostly) acquires content.[72] Such a strained reading simply cannot be squared with Congress's intent to strictly regulate the interception of content under the Wiretap Act, as it would allow the government to conduct an enormous amount of content surveillance without ever conforming to the Wiretap Act's requirements or ever being subject to the statutory exclusionary rule.

As Judge Smith conceded, an argument can be made that the PRS contemplates such incidental content acquisition, although ultimately that argument must fail.[73] But when the DOJ went further to claim that such acquisition could be excused based on application of the Wiretap Act's exclusionary remedy, it overplayed its hand. Not only does its novel argument to Judge Azrack flatly contradict the DOJ's long-held position in other cases, but the indirect manner in which it was made suggests that the DOJ is trying to hide that contradiction and prevail by misleading the court.

F. Conclusion

This case study should lead one to wonder: How often has the government obtained the authority to collect PCTDD content using the PRS, without question from a magistrate? How many times, when questioned, has the government avoided briefing altogether? How many times, when asked to brief a magistrate, has the government relied on dubious or even misleading arguments such as those described above? How often has the DOJ used its particularly misleading exclusionary rule argument in support of its sealed, *ex parte* applications? How much content has been collected over the years in violation of Congress's repeated prohibitions and in probable violation of *Katz* and *Smith*'s holdings that communication content is protected by the Fourth Amendment, and where is that content now? Has any of it been used in any criminal investigations, contrary to the DOJ's volun-

72. Notably, the DOJ has a long history of aggressively expanding the definition of pen registers to benefit from the greater power of technologies of surveillance without submitting to any heightened requirements. *See* Freiwald, *Uncertain Privacy*, *supra* note 26, at 982–89 (describing the evolution of the pen register); *see also* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 54–63 (2004) [hereinafter Freiwald, *Online Surveillance*] (describing the government's "aggressive interpretations" of the electronic surveillance statutes).

73. *See Smith Opinion II*, 441 F. Supp. 2d 816, 824–25 (S.D. Tex. 2006) (noting that the DOJ's "minimize content, but allow all non-content" gloss on the statute "is admittedly one possible way to read § 3121(c)," but ultimately finding it implausible).

tary policies and its new argument that the Wiretap Act mandates the exclusion of such contents? How many judges have continued signing off on these applications even after Judge Smith's decision revealed the DOJ's routine, continuing abuse of the *ex parte* surveillance process?

Only the DOJ knows.

II. Case Study: Warrantless Cell Phone Location Tracking

A. Introduction to Cell Phones, Location Tracking, and the Law

Many people are unaware of the fact that when they carry a cell phone, they are carrying a location-tracking device. Even if the phone does not have a Global Positioning System ("GPS") chip, information derived from the cell towers that communicate with a cellular phone can indicate the phone's location,[74] sometimes quite accurately.[75]

Although the government had been known to use this capability as an investigative technique before, it was never clear what legal process justified such tracking.[76] The Wiretap Act does not appear to require (or authorize) Wiretap Orders for such tracking,[77] while the PRS clearly does not provide the requisite authority.[78] Before 2005, the most likely theory was that the government was using search warrants under Rule 41 of the Federal Rules of Criminal Procedure for cell phone tracking. Considering that such surveillance would likely reveal the cell phone's location while it was out of public view, one

74. *See, e.g., In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747, 750–51 (S.D. Tex. 2005) [hereinafter *Smith Opinion I*] (describing tracking capabilities of cell phones based on cell tower information).

75. Indeed, federal law *requires* that cell phone providers whose phones do not contain GPS chips or similar "handset-based" tracking technologies be able to use "network-based" methods such as cell triangulation to locate a cell phone to within at least 100 meters for most calls, so that emergency services can locate 911 callers. 47 C.F.R. § 20.18(h)(1) (2005). *See also id.* § 20.18.

76. *See, e.g.*, United States v. Forest, 355 F.3d 942, 947–49 (6th Cir. 2004) (describing the Government's use of cell site data but only vaguely referring to "court authorization").

77. *See* 18 U.S.C. §§ 2510(12), 3117(b) (2000) (excluding from definition of "electronic communication" "any communication from a tracking device," which is defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object"). Nor would cell site location signals appear to fit the definitions of "wire communications" or "oral communications," the only other communications regulated by the Wiretap Act. *See* 18 U.S.C.A. §§ 2510(1), (2) (West 2000 & Supp. 2006) (definitions); *see also* 18 U.S.C.A. § 2511 (West 2000 & Supp. 2006) (generally prohibiting interception of electronic, wire or oral communications).

78. *See* 47 U.S.C. § 1002(a)(2)(B) (2000) ("[I]nformation acquired solely pursuant to the authority for pen registers and trap and trace devices . . . shall not include any information that may disclose the physical location of [a telephone service] subscriber.").

assumed that the prudent prosecutor would want to obtain a warrant before conducting such surveillance to avoid suppression of the evidence based on the Fourth Amendment.[79]

As described below, however, events in 2005 revealed that DOJ prosecutors have tracked cell phones for years without obtaining the necessary warrants. Before surveying the government's imprudence in this area, however, it is necessary to address another component of electronic surveillance law: the Stored Communications Act ("SCA") passed as part of the ECPA.

B. Primer: The Stored Communications Act

In 1986, in addition to creating the PRS and updating the Wiretap Act to protect electronic communications as well as wire and oral communications, Congress created a new chapter in the criminal code.[80] Congress formulated this new chapter as part of the ECPA to deal with new privacy problems resulting from changes in communications technology. In particular, Congress sought to remedy the proliferation of stored communications content and records. Therefore, the SCA portion of the ECPA protects private communications that are in "electronic storage" with a third party communications service provider, by requiring the government to obtain a search warrant before accessing communications that have been in storage for 180 days or less.[81] The SCA also requires that the government obtain a

79. Under the Fourth Amendment, the government must "obtain warrants prior to monitoring a [location-tracking device] when it has been withdrawn from public view," and "warrants for the installation and monitoring of a [location-tracking device] will obviously be desirable since it may be useful, even critical, to monitor the [location-tracking device] to determine that it is actually located in a place not open to visual surveillance." United States v. Karo, 468 U.S. 705, 718, 713 n.3 (1984) (holding that monitoring of location-tracking "beeper" attached to drum of chemicals in suspect's possession was a search under the Fourth Amendment when the drum was withdrawn from public view). Or, as Judge Smith would later put it when confronting the issue of cell phone tracking: "As in any tracking situation, it is impossible to know in advance whether the requested phone monitoring will invade the target's Fourth Amendment rights. The mere possibility of such an invasion is sufficient to require the prudent prosecutor to seek a Rule 41 search warrant." *Smith Opinion I*, 396 F. Supp. 2d 747, 757 (S.D. Tex. 2005).

80. *See* Stored Wire & Electronic Communications & Transactional Records Access, Pub. L. 99-508, § 201, 100 Stat. 1861 (1986) (codified as amended at 18 U.S.C. §§ 2701–10 (2000)).

81. *See* 18 U.S.C.A. § 2703(a) (West 2000 & Supp. 2006). *See also*, Freiwald, *Online Surveillance*, *supra* note 72, at 49-51 (discussing the government's claim that it may access such stored communications without using a warrant); Susan Freiwald & Patricia Bellia, *The Fourth Amendment Status of Stored E-mail: The Law Professors' Brief in* Warshak v. United States, 41 U.S.F. L. REV. 559 (addressing the constitutional status of the government's claim).

subpoena or an intermediate, non-probable-cause court order (a "D Order", named after the code subsection authorizing such orders) before accessing any non-content records or other subscriber information stored by service providers.[82]

Although the SCA (like the Wiretap Act and the PRS) is intimidating in its details, the key distinction between it and the other statutes is a simple one: unlike the Wiretap Act and the PRS, which authorize *prospective*, real-time surveillance of communications contents and non-content information, respectively, the SCA only authorizes *retrospective* access to previously stored communications contents and non-content information.[83]

This reading of the SCA is supported by its structure as compared to the Wiretap Act and the PRS,[84] the legislative history,[85] the case

82. *See* 18 U.S.C.A. § 2703(c) (West 2000 & Supp. 2006).

83. See Kerr, *supra* note 14, at 616–19 for a discussion of the distinction between retrospective and prospective surveillance; Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1565 (2004) ("The Wiretap Act and Pen Register statute regulate prospective surveillance . . . and the SCA governs retrospective surveillance . . . ."). *See also* United States Internet Service Provider Association, *Electronic Evidence Compliance—A Guide for Internet Service Providers*, 18 BERKELEY TECH. L.J. 945, 951, 957 (2003) (D Orders, authorized under the SCA, are for "historical" non-content records, while Pen-Trap Orders are for "any prospective noncontent information"). *See generally* Freiwald, *Online Surveillance*, *supra* note 72, at 46-52 (providing an overview of different categories of surveillance).

84. Unlike the PRS and the Wiretap Act, the SCA has none of the features one would associate with prospective surveillance, and several features that only make sense in the context of retrospective surveillance. *See, e.g.*, *Smith Opinion I*, 396 F. Supp. 2d 747, 760 (S.D. Tex. 2005) (comparing features of SCA with Wiretap Act and PRS):

> Unlike wiretap and pen/trap orders, which are inherently prospective in nature, § 2703(d) orders are inherently retrospective. This distinction is most clearly seen in the duration periods which Congress mandated for wiretap and pen/trap orders. Wiretap orders authorize a maximum surveillance period of 30 days, which begins to run no later than 10 days after the order is entered. 18 U.S.C. § 2518(5). Pen/trap orders authorize the installation and use of a pen register for a period "not to exceed sixty days." 18 U.S.C. § 3123(c)(1). By contrast, Congress imposed no duration period whatsoever for § 2703(d) orders. Likewise, Congress expressly provided that both wiretap orders and pen/trap orders may be extended by the court for limited periods of time. 18 U.S.C. §§ 2518(5), 3123(c)(2). There is no similar provision for extending § 2703(d) orders. Pen/trap results are ordinarily required to be furnished to law enforcement "at reasonable intervals during regular business hours for the duration of the order." 18 U.S.C. § 3124(b). The wiretap statute authorizes periodic reports to the court concerning the progress of the surveillance. 18 U.S.C. § 2518(6). Again, nothing resembling such ongoing reporting requirements exists in the SCA.

Id.

85. The SCA's legislative history repeatedly refers to "records" being "maintained," "kept," or "stored." *See* S. REP. No. 99-541, at 3 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3557; H.R. REP. No. 99-647, at 25, 72, 73 (1986). The bill's sponsor, Rep. Robert W.

law,[86] and the Supreme Court's holding that prospective surveillance is more intrusive under the Fourth Amendment than an individual search.[87] This reading was also—at least until 2005—the DOJ's own public take on the SCA.[88] Outside of the public eye, however, in *ex parte* proceedings before magistrate judges, the DOJ has routinely relied on a completely contradictory argument, as one magistrate revealed in 2005.

C. Magistrate Judge Orenstein's Revelation: Government Using SCA to Track Cell Phones

Declan McCullagh, of www.news.com, first broke the news in September 2005.[89] The previous month, a New York magistrate uncharacteristically had published the denial of an *ex parte* surveillance application, representing the first published decision addressing the appropriate legal process for cell phone tracking.[90] That opinion, from Magistrate Judge James Orenstein of the Eastern District of New York, contained a stunning revelation to those who follow surveillance law: the government was seeking in that case, and had apparently routinely sought and received in front of other magistrates, authorization

Kastenmeier, emphasized that one of the "fundamental principles" guiding the legislation is that "the nature of modern recordkeeping requires that some level of privacy protection be extended to records about us which are stored outside the home." 99 CONG. REC. H14875, 14886 (daily ed. June 23, 1986).

86. No reported case regarding the SCA prior to the cell phone tracking controversy approved of—or even considered—the possibility that the statute could authorize real-time or prospective disclosure of information.

87. *See* Berger v. New York, 388 U.S. 41, 59 (1967) (likening ongoing electronic eavesdropping to "a series of intrusions").

88. "Any real-time interception of electronically transmitted data . . . must comply strictly with the requirements of Title III, 18 U.S.C. §§ 2510–2522 [the Wiretap Act], or the Pen/Trap statute, 18 U.S.C. §§ 3121–3127." Computer Crime & Intellectual Prop. Section, Criminal Div., United States Dep't of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 24 (July 2002), *available at* http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.pdf. Meanwhile, "18 U.S.C. §§ 2701–2712 [the Stored Communications Act] . . . governs how investigators can obtain stored account records and contents . . . ." *Id.* at ix.

89. Declan McCullagh, *Police Blotter: Cell Phone Tracking Rejected*, CNET News.com, Sept. 2, 2005, http://news.com.com/Police£lotter+Cell+phone+tracking+rejected/2100-1030_3-5846037.html.

90. *See In re* Application of the United States for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info., 384 F. Supp. 2d 562, 563 (E.D.N.Y. 2005) [hereinafter *Orenstein Opinion I*].

to track cell phones prospectively and in real-time *using D Orders under the SCA.*[91]

Based on what he later admitted was a misreading of the SCA,[92] Judge Orenstein had denied the government's application. That Judge Orenstein initially misread the SCA is somewhat understandable, considering the government declined his specific request that it prepare a brief on the statute.[93] Following his opinion, the government quickly moved for reconsideration.[94] EFF saw the McCullagh story, read Judge Orenstein's opinion, noted the revelation about cell-tracking D Orders, and realized that Judge Orenstein had reached the right result based on the wrong reasoning. Accordingly, EFF asked for and was given leave to submit an amicus brief in opposition to the government's motion for reconsideration.[95]

In its brief on reconsideration, however, the DOJ retreated from its initial argument that a D Order alone could authorize prospective, real-time cell phone tracking. Instead, the DOJ proposed a wholly unprecedented argument and claimed that Judge Orenstein misunderstood its original application. The DOJ argued that its application sought—and Congress had intended for courts to grant—authorization for cell phone tracking based on the *combination* of a D Order

91. *Id.* at 566. *See also* Matt Richtel, *Live Tracking of Mobile Phones Prompts Court Fights on Privacy*, N.Y. TIMES, Dec. 10, 2005, at A1, C13 ("In recent years, law enforcement officials have turned to [cell phone tracking] cellular technology as a tool for easily and secretly monitoring the movements of suspects as they occur. . . . [I]nvestigators have been able to conduct [this kind of surveillance] with easily obtained court orders . . . . [T]he number of requests had become more prevalent in the last two years—and the requests have often been granted with a stroke of a magistrate's pen.").

92. *See Orenstein Opinion I*, 384 F. Supp. 2d at 563–64 (mistakenly finding that D Orders could only be used to obtain content, despite plain language of statute authorizing D Orders for non-content information); Orenstein Order Granting Leave for EFF to Submit Brief Amicus Curiae, *USA v. Pen Register*, MJ 05-1093 (JO) (E.D.N.Y. Sept. 19, 2005), *available at* http://www.eff.org/legal/cases/USA_v_PenRegister/celltracking_amicusorder.pdf (acknowledging that error); *Orenstein Opinion II*, 396 F. Supp. 2d 294, 302 n.4 (E.D.N.Y. 2005) (acknowledging that error).

93. *Orenstein Opinion I*, 384 F. Supp. 2d at 563.

94. *See* Government's Motion for Reconsideration, *In re* Application for Pen Register & Trap & Trace Device with Cell Site Location Authority, MJ 05-1093 (JO) (E.D.N.Y. Sept. 9, 2005), *available at* http://www.eff.org/legal/cases/USA_v_PenRegister/celltracking_reconmotion.pdf [hereinafter Government's Motion for Reconsideration of Cell Tracking Denial].

95. *See* EFF Motion for Leave to File Amicus Brief, *In re* Application for Pen Register & Trap & Trace Device with Cell Site Location Authority, MJ 05-1093 (JO) (E.D.N.Y. Sept. 16, 2005), *available at* http://www.eff.org/legal/cases/USA_v_PenRegister/celltracking_EFF letter.pdf; Orenstein Order Granting Leave for EFF to Submit Brief Amicus Curiae, United States of America v. Pen Register, MJ 05-1093 (JO) (E.D.N.Y. Sept. 19, 2005), *available at* http://www.eff.org/legal/cases/USA_v_PenRegister/celltracking_amicusorder.pdf.

and a Pen-Trap Order.[96] The government argued that such an order, issued under the authority of both the PRS and the SCA, would satisfy the privacy provision passed as part of CALEA, which requires that "information acquired *solely* pursuant to the authority for pen registers and trap and trace devices . . . shall not include any information that may disclose the physical location of the [telephone service] subscriber."[97]

The government argued that Congress's inclusion of the word "solely" necessarily meant that the PRS, in combination with some other authority, could authorize cell site location tracking.[98] However, the word "solely" was the only textual support the government could muster for its all-new, never-before-contemplated hybrid order.[99] Nothing else in the PRS or any other statute even hinted at the possibility of a marriage between Pen-Trap Orders and other surveillance authorities. Certainly nothing in the PRS or any other statute indicated a congressional preference for wedding the Pen-Trap Order with a D Order as opposed to a subpoena, search warrant, Wiretap Order, or any other legal authority.

After debuting its hybrid order argument before Judge Orenstein, the government would soon be arguing it in front of additional judges—several of whom would note that despite the DOJ's claims, the government's initial applications for cell phone tracking authority all appeared to seek only D Orders under the SCA and did not even refer to the PRS.[100] As Judge Orenstein would later put it:

> Notwithstanding the government's claim that its current explicit reliance on the hybrid theory serves merely to "dispel" what it allows may have been an initial "lack of clarity on that score," it is

96. *See* Government's Motion for Reconsideration of Cell Tracking Denial, *supra* note 94, at 5–6.

97. *See id.* (quoting 47 U.S.C. § 1002(a)(2)(B) (2000)).

98. *See id.*

99. *See id.* at 5–7.

100. *See Smith Opinion I*, 396 F. Supp. 2d 747, 749, 752, 761 (S.D. Tex. 2005) (application did not cite the PRS as authority for cell-site order, only the SCA); *Orenstein Opinion I*, 384 F. Supp. 2d 562, 564–65 (E.D.N.Y. 2005); *Orenstein Opinion II*, 396 F. Supp. 2d 294, 316–18 (E.D.N.Y. 2005); *see also In re* Application of the United States of America for an Order Authorizing the Installation & Use of a Pen Register & a Caller Identification System on Telephone Nos. [sealed] & [sealed] & the Production of Real Time Cell Site Info., 402 F. Supp. 2d 597, 598 (D. Md. 2005) [hereinafter *Bredar Opinion I*] (failing to specify the statutes referenced in the application but citing only the SCA's section 2703(d) when referring to its contents); *In re* Application of the United States of America for an Order Authorizing the Installation & Use of a Pen Register with Caller Identification Device & Cell Site Location Authority on a Certain Cellular Telephone, 415 F. Supp. 2d 663, 664 (S.D. W. Va. 2006) (indicating that prior to the instant hybrid application, the government's "usual application" relied only on the SCA).

> apparent that the theory is either an afterthought offered to salvage an application . . . or alternatively the theory that the government relied on all along but hesitated to expose to judicial scrutiny.[101]

As discussed below, later revelations have proven the former over the latter and demonstrated that the DOJ has long believed that a D Order alone can authorize cell phone tracking. Therefore, an extended analysis of the hybrid theory's shortcomings, already well-chronicled by others,[102] is unnecessary to demonstrate the core lesson of this case study: the government succeeded for over a decade in obtaining court approval of cell phone tracking based on a weak and never-articulated argument that contradicted not only the DOJ's own publicly-articulated understanding of the SCA, but everyone else's as well. Some brief discussion of this legal afterthought's progression through the courts is necessary, though, if only to show why the hybrid theory should end up as a curious footnote in the history of surveillance law.

D. Much Ado About Nothing: The Courts Dissect the "Hybrid" Argument for Cell Phone Tracking

The stage was set: Judge Orenstein had rejected the original application for a D Order authorizing cell phone tracking,[103] but based the rejection on incorrect reasoning. The government moved for him to reconsider. EFF filed an amicus brief explaining how neither a D Order, a Pen-Trap Order, nor some shotgun marriage of the two, could authorize such surveillance, and explained how Judge Oren-

101. *Orenstein Opinion II*, 396 F. Supp. 2d at 317–18; *see also Smith Opinion I*, 396 F. Supp. 2d at 765 (finding the Government's hybrid theory "amounts to little more than a retrospective assemblage of disparate statutory parts to achieve a desired result").

102. *See, e.g.*, *Smith Opinion I*, 396 F. Supp. 2d at 761–65 (rejecting government's hybrid theory after extended analysis); *Orenstein Opinion II*, 396 F. Supp. 2d at 307–21; *Bredar Opinion I*, 402 F. Supp. 2d at 600-03; *In re* Application of the United States for an Order Authorizing the Disclosure of Prospective Cell Site Info., 412 F. Supp. 2d 947, 951–58 (E.D. Wis. 2006); *In re* Application of the United States for an Order Authorizing the Installation & Use of a Pen Register &/or Trap & Trace for Mobile Identification No. (585) 111-1111 & the Disclosure of Subscriber & Activity Info. Under 18 U.S.C. § 2703, 415 F. Supp. 2d 211, 214–19 (W.D.N.Y. 2006); *In re* Application of the United States of America for Orders Authorizing the Installation & Use of Pen Registers & Caller Identification Devices on Telephone Nos. [sealed] & [sealed], 416 F. Supp. 2d 390, 392–97 (D. Md. 2006) [hereinafter *Bredar Opinion II*]; *Smith Opinion II*, 441 F. Supp. 2d 816, 827–36 (S.D. Tex. 2006); *In re* Application of the United States of America for an Order Authorizing the Disclosure of Prospective Cell Site Info., No. 06-MISC-004, 2006 WL 2871743, at *949–58 (E.D. Wis. Oct. 6, 2006).

103. *Orenstein Opinion I*, 384 F. Supp. 2d at 566.

stein's first decision was correct in the result even if not in the reasoning.[104] Which way would Judge Orenstein go?

As EFF waited for Judge Orenstein's new decision with bated breath, Magistrate Judge Smith of Houston—the very same judge who would publish the first PCTDD decision a year later—surprised us with his own decision denying a similar cell-tracking application. Judge Smith's decision lacked Judge Orenstein's original mistakes and agreed with EFF that cell tracking requires probable cause.[105] A new improved decision by Judge Orenstein quickly followed.[106] Both judges required at least a probable cause warrant issued under Rule 41 of the Federal Rules of Criminal Procedure before they would authorize cell phone tracking.[107] Neither decision was kind to the government's arguments for a hybrid order, variously describing them as "unsupported,"[108] "misleading,"[109] and "contrived,"[110] calling the government's desperate attempt to create such a legal "chimera"[111] a "Hail Mary play."[112] Judge Smith found the government's hybrid argument so convoluted as to be "perverse" and likened it to "a three-rail bank shot,"[113] "undeniably creative [but] amount[ing] to little more than a retrospective assemblage of disparate statutory parts to achieve a desired result."[114]

The DOJ did not appeal these stinging rejections despite the judges' strongest encouragement.[115] Nor did these decisions prevent

104. *See* Brief for EFF as Amicus Curiae Opposing the Government, *In re* Application for Pen Register & Trap & Trace Device with Cell Site Location Authority, MJ 05-1093 (JO) (E.D.N.Y. Sept. 23, 2005), *available at* http://www.eff.org/legal/cases/USA_v_PenRegister/celltracking_EFFbrief.pdf.

105. *See Smith Opinion I*, 396 F. Supp. 2d at 765 (denying hybrid application but holding that a probable cause warrant would suffice to authorize such surveillance).

106. *See Orenstein Opinion II*, 396 F. Supp. 2d 294.

107. *See id.* at 321, 324–25 (finding that "[a]t a minimum, to the extent the government seeks a judicial imprimatur for its acquisition in real time of prospective cell site information, it must proceed under Rule 41," though not ruling out the possibility that the government must further satisfy "a standard comparable to the super-warrant requirement under Title III" in order to conduct real-time cell phone tracking); *Smith Opinion I*, 396 F. Supp. 2d at 765 ("This type of surveillance is unquestionably available upon a traditional probable cause showing under Rule 41.").

108. *Orenstein Opinion II*, 396 F. Supp. 2d at 314.

109. *Id.* at 325 n.23.

110. *Id.* at 321.

111. *Id.*

112. *Id.* at 326.

113. *Smith Opinion I*, 396 F. Supp. 2d 747, 765 (S.D. Tex. 2005).

114. *Id.*

115. *See id.* at 765 (encouraging appeal); *Orenstein Opinion II*, 396 F. Supp. 2d 294, 327 (E.D.N.Y. 2005).

the DOJ from continuing to seek cell-tracking authority from other magistrate judges without showing probable cause, using applications that now explicitly cited both the PRS and the SCA.[116] However, Judges Orenstein and Smith had started something of a magisterial revolution. In the remaining months of 2005, three more judges would publish decisions rejecting hybrid applications.[117]

Of course, the DOJ did not appeal those decisions either, but it did keep plugging away in front of other judges. The persistence of the government's lawyers finally paid off at the end of the year, when they found a judge in Manhattan that would endorse their hybrid theory. That court's decision, issued on December 20, must have felt like a Christmas present to the DOJ: not only was it the first published decision to allow the combination of a D Order and a Pen-Trap Order in order to authorize cell phone tracking, but as described below, its reasoning also provided the government with a path back to its original practice of relying solely upon D Orders.[118]

E. What a Difference a "G" Makes: Magistrate Judge Gorenstein Signs Off on the DOJ's Hybrid Theory

In December 2005, after five magistrates had published decisions rejecting the government's hybrid applications,[119] Magistrate Judge Gabriel W. Gorenstein became the first to publish a decision approv-

116. *See, e.g., In re* Applications of the United States of America for Orders Authorizing the Disclosure of Cell Cite [sic] Info., Nos. 05-403, 05-404, 05-407, 05-408, 05-410, 05-411, 2005 WL 3658531, at *1 (D.D.C. Oct. 26, 2005) (stating that the instant applications and others submitted in October 2005 relied on "dual authority" of the SCA and the PRS); *In re* Application of the United States for an Order Authorizing the Disclosure of Prospective Cell Site Info., 412 F. Supp. 2d 947, 948 (E.D. Wis. 2006) (stating that the application filed in December 2005 requested prospective cell site information pursuant to both the SCA and the PRS).

117. *See Bredar Opinion I*, 402 F. Supp. 2d 597 (D. Md. 2005); *In re* Applications of the United States of America for Orders Authorizing the Disclosure of Cell Cite [sic] Info., Nos. 05-403, 05-404, 05-407, 05-408, 05-410, 05-411, 2005 WL 3658531, at *1 (D.D.C. Oct. 26, 2005); *In re* Application of the United States of America for an Order Authorizing the Release of Prospective Cell Site Info., 407 F. Supp. 2d 132, 133 (D.D.C. 2005).

118. *See In re* Application of the United States of America for an Order for Disclosure of Telecommunications Records & Authorizing the Use of a Pen Register & Trap & Trace, 405 F. Supp. 2d 435 (S.D.N.Y. 2005) [hereinafter *Gorenstein Opinion*].

119. *See Smith Opinion II*, 441 F. Supp. 2d 816 (S.D. Tex. 2006); *Orenstein Opinion II*, 396 F. Supp. 2d at 320; *Bredar Opinion I*, 402 F. Supp. 2d 597; *In re* Applications of the United States of America for Orders Authorizing the Disclosure of Cell Cite [sic] Info., Nos. 05-403, 05-404, 05-407, 05-408, 05-410, 05-411, 2005 WL 3658531, at *1 (D.D.C. Oct. 26, 2005); *In re* Application of the United States of America for an Order Authorizing the Release of Prospective Cell Site Info., 407 F. Supp. 2d 132, 133 (D.D.C. 2005).

ing such an application.[120] Judge Gorenstein somewhat reluctantly held that Congress's use of the word "solely" in its prohibition against cell phone tracking based "solely" on a Pen-Trap Order, necessarily meant that a Pen-Trap Order in combination with another source of legal authority could authorize the government to track a cell phone's location.[121] Therefore, and despite his recognition that Congress had failed to specify the legal authority with which the Pen-Trap Order could or should be combined,[122] Judge Gorenstein held that the combination of a Pen-Trap Order with a D Order would suffice. The judge based his decision on two findings. First, like most of the judges who had rejected hybrid applications, he found that the government could at least obtain *stored* records of cell phone location data using the SCA.[123] Second, unlike those other judges, he found that the SCA also authorizes *prospective* surveillance.[124]

Judges who have published subsequent decisions have not viewed Judge Gorenstein's decision with high regard. Although two magistrates and two district court judges have now published opinions that adopt Judge Gorenstein's reasoning,[125] six magistrates and two district

120. *Gorenstein Opinion*, 405 F. Supp. 2d 435.

121. *See id.* at 442 (relying on the dictionary definition of "solely"); *but see Smith Opinion II*, 441 F. Supp. 2d at 832–33 (rebutting this argument at length).

122. *See Gorenstein Opinion*, 405 F. Supp. 2d at 442–43.

> [W]e are left with the conclusion that Congress has given a direction that cell site information may be obtained through some unexplained combination of the Pen Register Statute with some other unspecified mechanism. . . . The idea of combining some mechanism with as yet undetermined features of the Pen Register Statute is certainly an unattractive choice. After all, no guidance is provided as to how this 'combination' is to be achieved.

Id.

123. *See id.* at 446 (*citing Smith Opinion I*, 396 F. Supp. 2d 747, 759 n.16 (S.D. Tex. 2005)); *Orenstein Opinion II*, 396 F. Supp. 2d at 313; *Bredar Opinion I*, 402 F. Supp. 2d at 601.

124. *See Gorenstein Opinion*, 405 F. Supp. 2d at 446–49.

> The heart of the [relevant portion of the SCA, 18 U.S.C. §§ 2703(c)(1), (d) (Supp. 2000)]—granting authority to obtain "information" about cell phone customers—does not on its face contain any limitation regarding when such information may come into being. It is thus susceptible to an interpretation that the "information" sought might come into being in the future . . . . Thus . . . the statute permits the Government to obtain cell site data on a continuing or ongoing basis even under a narrow reading of section 2703.

Id. at 447.

125. *See In re* Application of the United States for an Order: (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device; & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info., 411 F. Supp. 2d 678 (W.D. La. 2006); *In re* Application for an Order Authorizing the Installation & Use of a Pen Register Device, Dialed No. Interceptor, No. Search Device, & Caller Identification Service, & the Disclosure of Billing, Subscriber, & Air Time Info., No. S-06-SW-0041 (E.D. Cal. Mar. 15, 2006) (on file with the author); *In re* Application of the United States for an Order: (1) Authorizing the Installa-

court judges have since published orders denying hybrid applications.[126] Judge Smith even published another decision to respond to Judge Gorenstein's opinion.[127] As of this writing, however, and as discussed below, the judge that started this all—Judge Orenstein—is still considering his next public response. This brings us finally to the latest (but certainly not the last) chapter in the cell phone tracking saga.

F. D Order Cell Tracking (Re-)Ascendant?

In the late summer of 2006, Judge Orenstein presided over a novel proceeding in the Eastern District of New York, where he considered a third and presumably final decision on the government's hybrid theory.[128] As a part of this "test case," Judge Orenstein held an evidentiary hearing attended by most of the district's magistrate

tion & Use of a Pen Register & Trap & Trace Device, & (2) Authorizing Release of Subscriber & Other Info., 433 F. Supp. 2d 804 (S.D. Tex. 2006); *In re* Application of the United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448 (S.D.N.Y. 2006).

126. *In re* Application of the United States for an Order Authorizing the Release of Prospective Cell Site Info., 407 F. Supp. 2d 134 (D.D.C. 2006); *In re* Application of the United States for an Order Authorizing the Disclosure of Prospective Cell Site Info., 412 F. Supp. 2d 947 (E.D. Wis. 2006); *In re* Application of the United States for an Order Authorizing the Installation & Use of a Pen Register &/or Trap & Trace for Mobile Identification No. (585) 111-1111 & the Disclosure of Subscriber & Activity Info. Under 18 U.S.C. § 2703, 415 F. Supp. 2d 211 (W.D.N.Y. 2006); *In re* Application of the United States of America for an Order Authorizing the Installation & Use of a Pen Register with Caller Identification Device & Cell Site Location Authority on a Certain Cellular Telephone, 415 F. Supp. 2d 663 (S.D. W. Va. 2006) (rejecting hybrid theory but authorizing surveillance on different reasoning); *Bredar Opinion II*, 416 F. Supp. 2d 390 (D. Md. 2006); *In re* Application of the United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Telephone, No. 06 Crim. Misc. 01, 2006 WL 468300, at *1 (S.D.N.Y. Feb. 28, 2006); *In re* Application of the United States of America for an Order: (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device; (2) Authorizing the Release of Subscriber & Other Information; & (3) Location of Cell Site Origination &/or Termination, *In re* Application of the United States of America for an Order: (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device; (2) Authorizing the Release of Subscriber & Other Info.; & (3) Authorizing the Disclosure of Location-Based Services Case Nos. 1:06-MC-6, 1:06-MC-7, 2006 WL 1876847, at *1 (N.D. Ind. July 5, 2006); *In re* Application for an Order Authorizing the Installation & Use of a Pen Register & Directing the Disclosure of Telecommunications Records for the Cellular Phone Assigned the No. [sealed], 439 F. Supp. 2d 456 (D. Md. 2006) [hereinafter *Bredar Opinion III*]; *In re* Application of the United States of America for an Order Authorizing the Disclosure of Prospective Cell Site Info., No. 06-MISC-004, 2006 WL 2871743, at *1 (E.D. Wis. Oct. 6, 2006).

127. *See Smith Opinion II*, 441 F. Supp. 2d 816, 827–37 (S.D. Tex. 2006).

128. *See* E-mails from Yuanchung Lee, Federal Defenders of New York to Kevin Bankston (Dec. 21, 2006 at 05:57:28 PST, 12:22:10 PST, 12:23:47 PST, and 12:24:28 PST; Jan. 24, 2007, at 13:07:52 PST; and Jan. 25, 2007, at 6:01:50 PST) (describing hearing and providing copies of Government and amicus curiae briefs) (on file with author).

judges,[129] who had reportedly reached an informal agreement to reject any hybrid applications pending the new decision.[130] Judge Orenstein also accepted briefs from the government[131] and from the Federal Defenders of New York,[132] which was invited to participate as an amicus in opposition to the government.

As of this writing, Judge Orenstein has not published a new decision based on this latest round of briefing. However, the government's last brief to Judge Orenstein contains an important new argument that finally reveals the government's original practice when it comes to cell phone tracking:

> The SCA has furnished authority for [prospective] disclosure since CALEA's enactment in 1994, and likely even before 1994. *Accordingly, for a decade or more, the government applied for and the courts routinely granted orders for tower/sector and MSC Records [i.e., cell location data] under sole authority of the SCA.*[133]

This admission stands in stark contrast to what the government originally represented to Judge Orenstein when it moved for him to reconsider his first cell-tracking decision. The government, in its first known brief on the subject, claimed that its practice was to seek orders for cell tracking based on the *combined* authority of the SCA and PRS.[134] The government further conceded that the SCA alone was not sufficient legal authority to authorize such surveillance.[135]

129. *See id.*

130. *See id.*

131. *See* Government's Memorandum of Law in Support of Its Request for an Order Directing the Carrier to Disclose Location Records Prospectively Under Joint Authority of the SCA & the Pen/Trap Statute, *In re* Application of the United States of America for an Order Authorizing (1) The Use of a Pen Register & a Trap & Trace Device with Tower/Sector & MSC Authority & (2) The Release of Other Subscriber Info., 06-MSC-370 (E.D.N.Y. July 19, 2006) [hereinafter Government's EDNY Memorandum] (on file with author).

132. *See* Letter Brief of Federal Defenders of New York, Inc., *In re* Government Request for an Order Directing the Wireless Carrier to Disclose Location Records Prospectively, 06-MSC-370 (E.D.N.Y. Aug. 22, 2006) (on file with author).

133. Government's EDNY Memorandum, *supra* note 131, at 24 (emphasis added).

134. Government's Motion for Reconsideration of Cell Tracking Denial, *supra* note 94, at 7 ("In this case, *as is our practice,* the government has not sought to acquire cell-site information 'solely pursuant' to the Pen/Trap statute, but as well under the more demanding requirements of the SCA.") (emphasis added).

135. *Id.* ("That is not to say that the [cell tracking] order we propose could or should issue based solely on the authority of the SCA. We agree [with the Court] that . . . the Pen/Trap statute plays a governing role in the issuance of orders requiring the prospective disclosure of cell site [information] . . . ."); *id.* at 8 ("Accordingly, orders directing the prospective collection of cell-site information *must* issue under the complementary authority of [the PRS] and [the SCA].") (emphasis added).

Why did the government finally admit to Orenstein that its practice all along was to use D Orders for cell tracking (and thereby also admit that it's hybrid theory was—as originally suspected[136]—never its actual legal rationale)? Perhaps the magistrates finally demanded an answer to the question of why the government has been applying only for D Orders over the past decade if it is actually the combination of the PRS and SCA that allows cell tracking. Or, perhaps Judge Gorenstein's support for the use of D Orders alone for prospective surveillance[137] emboldened the government. Judge Gorenstein's decision may have signaled to the DOJ that it could finally reveal, and find support for, its understanding of the SCA after over a decade of concealment from the public view.

Regardless, the latest brief represents a clear retreat from the hybrid theory and a rallying to the sole reliance on prospective D Orders. Certainly, the brief still pays significant lip service to the hybrid theory, arguing that the court can authorize cell phone tracking by combining a Pen-Trap Order with a D Order.[138] The government had to acknowledge its previous adherence to the hybrid theory before the same court to maintain credibility. As mentioned previously, however, and for the first time, the government now also argues that the SCA *alone* can authorize the prospective disclosure of cell site information[139] (and presumably any other type of content or non-content information covered by the SCA).

In stating this new argument, the government directly contradicts its previous argument that, when Congress passed CALEA in 1994, it specifically intended for the combination of a Pen-Trap Order and a D Order to authorize cell phone tracking.[140] The government's diffi-

136. *Orenstein Opinion II*, 396 F. Supp. 2d 294, 317–18 (E.D.N.Y. 2005) ("[I]t is apparent that the [hybrid] theory is . . . an afterthought offered to salvage an application.").

137. *See* Gorenstein Opinion, 405 F. Supp. 2d 435, 446 (S.D.N.Y. 2005) (holding, despite previous decisions questioning whether "prospective" or "real time" cell site information is obtainable under the SCA, that the SCA is not limited to historical records: "The statute itself contains no limitation of this kind."); *see also In re* Application of the United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 459 (S.D.N.Y. 2006) ("The Stored Communications Act contains no explicit limitation on the disclosure of prospective data.").

138. *See, e.g.*, Government's EDNY Memorandum, *supra* note 131, at 51–54.

139. *Id.* at 32–34.

140. *Compare* Letter from United States Attorney Eastern District of New York to the Honorable James Orenstein (Oct. 11, 2005), *available at* http://www.eff.org/legal/cases/USA_v_PenRegister/celltracking_govt_reply.pdf (arguing that CALEA originally authorized the combination of a Pen-Trap Order with a D Order for cell phone tracking), *with* Government's EDNY Memorandum, *supra* note 131, at 59 (arguing that "the drafters of CALEA in 1994 intended to authorize the disclosure of location records on a prospective

culty accounting for either the birth or death of the hybrid order requirement further suggests that its hybrid theory was only ever "an afterthought offered to salvage" its original application to Judge Orenstein, while its vision of an SCA that authorizes prospective surveillance is "the theory that the government relied on all along but hesitated to expose to judicial scrutiny."[141]

More importantly, the government's position contradicts a basic premise of the electronic surveillance statutes, one that was—until now and at least in public—unanimously agreed to by every commentator, including the DOJ: the SCA reaches only previously stored contents and records, and only the Wiretap Act and the PRS can authorize prospective, real-time surveillance.[142] If that premise is no longer true, then the government may easily circumvent the myriad protections provided in the Wiretap Act and, to a lesser degree, the PRS, merely by proceeding under the SCA.

Returning to Judge Orenstein's original question posed in the introduction—"How long has this been going on?"—we finally have an answer: all along. But there are plenty of other questions: How many judges (if any) had said "no" privately to government requests to track cell phones without warrants, before Judge Orenstein did so publicly? How many judges are now saying "yes" to such warrantless surveillance, but choosing not to publish decisions? Are these judges issuing hybrid orders or D Orders? Did the magisterial revolt against warrantless cell phone tracking change anything, or does the government still routinely obtain permission to track cell phones without probable cause? How many times since 1994 has the government convinced judges to issue D Orders for cell phone tracking without ever putting its legal argument to paper, a legal argument that contradicts all

basis under the SCA," alone, while it was the PATRIOT Act's amendments to the PRS that created the hybrid authority by making authorization under the PRS a "mandatory complement" to authorization under the SCA). Notably, the government's newly admitted practice of using the SCA as its sole cell tracking authority for "a decade or more," Government's EDNY Memorandum, *supra* note 131, at 24, contradicts both its initial argument to Orenstein that CALEA created the hybrid authority in 1994 and its current argument to Orenstein that the PATRIOT Act created the hybrid authority in 2001.

141. See Orenstein Opinion II, 396 F. Supp. 2d at 317–18 (questioning the provenance of the government's hybrid theory).

142. *See, e.g.*, Kerr, *supra* note 14, at 616–19; Mulligan, *supra* note 83, at 1565; United States Internet Service Provider Association, *supra* note 83, at 951, 957; Computer Crime & Intellectual Prop. Section, Criminal Div., United States Dep't of Justice, *supra* note 88, at 24.

known authorities' understanding of the SCA and likely violates the Fourth Amendment?[143]

Only the DOJ knows.

III. Case Study: Warrantless Internet Surveillance

A. April 2000: Carnivore Revealed

The last case study is brief and dispiriting. It demonstrates that the new revelations of warrantless cell phone tracking and PCTDD surveillance are only the latest examples in a long-standing trend. Moreover, it shows that Congress may react to revelations of government overreaching by reinforcing rather than reining in the government's surveillance authority.

143. Although the Government contends that the cell site data it is currently seeking is not precise enough to raise Fourth Amendment concerns, it also admits that it only started seeking this less-precise cell site data to quell the unrest among the magistrates that had been sparked by Orenstein, that it may again seek more precise data in the future, and that the precision of the location data is ultimately irrelevant to the validity of its statutory argument. *See In re* Application of the United States of America for an Order Authorizing the Installation & Use of a Pen Register &/or Trap and Trace for Mobile Identification No. (585) 111-1111 & the Disclosure of Subscriber & Activity Info. under 18 U.S.C. § 2703, 415 F. Supp. 2d 211, 218, 218 n.5 (W.D.N.Y. 2006).

> Indeed, during oral argument, [G]overnment counsel conceded that in previous "hybrid" applications the [G]overnment has sought prospective cell location data that could be used by law enforcement to triangulate the location of a cell phone to a degree perhaps beyond "general location information." . . . When pressed whether it has formally abandoned the position that a hybrid application is appropriate for anything more than "general location information" captured by the pen register, the [G]overnment's answer was commendably candid but less than legally enlightening.
>
> Q: (by the Court): The reason I'm pressing you on this is the whole point of your hybrid analysis would apply with equal force to triangulation information. You may not be wanting to exercise that, but you're telling me that even though we collect triangulation information under the cell [pen] statute and even though 2703 allows us to pair it with the pen register statute, we're not going to go and get that extra information? Why? If your argument makes sense, why doesn't it make sense for all the information you can collect?
>
> A: (AUSA Littlefield): Well there's a couple of practical things going on. One, we're before magistrate judges that are the gatekeepers—we're trying to convince them that the [G]overnment isn't being some ruthless, overbearing entity—we're trying to be reasonable. So, therefore, if we can get the magistrate's ear and we don't have to fight this fight a zillion times, we'll back off. If you have this internal radar that's going on "privacy interest, privacy interest", okay, we'll back off. But is it possible the argument could be made that we could be here on another day having gotten floor one and now we're trying to get floor two? Yes.

Id.

In this case, however, it was not a magistrate judge or a journalist who informed the public of the DOJ's secret surveillance practice—it was an internet service provider's lawyer, Robert Corn-Revere. Mr. Corn-Revere, while testifying before Congress in the spring of 2000, revealed that the government had recently asked his client to assist in implementing a previously unknown type of pen register surveillance.[144]

Pen registers—as defined by the ECPA originally and at the time of Corn-Revere's testimony—were limited to devices that acquired the numbers dialed over a telephone line.[145] Indeed, a report from the White House had recently complained that the PRS was outdated because it did not authorize the installation of devices that collected internet routing and addressing information.[146] But on April 6, 2000, in a congressional hearing on the Fourth Amendment and the Internet, Mr. Corn-Revere testified that the government was using the PRS to do just that.[147]

Mr. Corn-Revere first testified at some length that he doubted whether the PRS could authorize internet surveillance because its language specifically pertained to telephones.[148] Nonetheless, in December 1999, federal marshals had served his client (later identified as Earthlink[149]) with a Pen-Trap Order authorizing the government to "'install a pen register and trap and trace device to regis-

144. *See* Robert Corn-Revere, Testimony Before the Subcommittee on the Constitution of the Committee on the Judiciary, United States House of Representatives, "The Fourth Amendment and the Internet" (Apr. 6, 2000) [hereinafter Corn-Revere Testimony], http://judiciary.house.gov/legacy/corn0406.htm (without pagination); http://www.dwt.com/lawdir/publications/CR-Internet(4-6-00).pdf (with pagination and author's corrections and supporting footnotes).

145. *See* 18 U.S.C. § 3127(3) (2000).

146. *See* The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet A Report of the President's Working Group on Unlawful Conduct on the Internet (Mar. 2000), http://www.usdoj.gov/criminal/cybercrime/unlawful.htm#PEN ("Unfortunately, the statute that governs [pen registers] is not technology-neutral and has become outdated. . . . [T]he statute focuses specifically on telephone 'numbers,' a concept made out-of-date by the need to trace communications over the Internet that may use other means to identify users' accounts.") (internal citations omitted).

147. *See* Corn-Revere Testimony, *supra* note 144, at 23–24.

148. *See id.* at 16–21.

149. Corn-Revere did not identify Earthlink in his testimony because the relevant court orders were still under seal at the time, *see id.* at 21–22, but one of the orders which was eventually disclosed via a Freedom of Information Act request did identify Earthlink. *See In re* United States of America for an Order Authorizing the Installation of a Pen Register & Trap & Trace Device, Cr. No. 99-2713M (C.D. Cal. Feb. 4, 2000) (McMahon, Mag. J.) [hereinafter *McMahon Opinion*], *available at* http://www.epic.org/privacy/carnivore/cd_cal_order.html.

ter . . . addressing information of electronic mail messages sent to and from the subject internet account . . . .' "[150] Mr. Corn-Revere described how Earthlink moved for the court to quash the Pen-Trap Order because it was uncomfortable with the government installing a device on its network that had the capability of collecting all network traffic including content.[151] However, the court accepted the government's argument, "the essential thrust" of which was that the PRS—despite its plain language—empowered the government to obtain e-mail addressing information because such information is the "conceptual equivalent of a telephone number."[152] The court authorized the installation of the government's device, which was "a proprietary software program with the not-very-reassuring name of 'Carnivore.' "[153]

Mr. Corn-Revere's testimony raised some familiar questions: How often had this happened? Had any judges said "no"? Were the ones who said "yes" approving Pen-Trap Orders or hybrid orders? Were there any other sealed written opinions on the issue? Only the DOJ knew, of course.

Notably, despite lobbying by the DOJ that year, Congress did not update the law to reflect the government's practice.[154] However, Congress did fail to amend the pen register definition to conclude with the phrase, "we really mean it!" Apparently, that failure was sufficient to convince the DOJ that it was in the right, because it continued to seek and obtain orders to install internet pen registers, like Carnivore, under the PRS. Furthermore, and in contrast to the magisterial revolt

150. Corn-Revere Testimony, *supra* note 144, at 23. Very notably, and mirroring its strategy in the cell phone tracking context, the Government originally had sought this order based on a hybridization of the SCA and the PRS:

> As an apparent indication of some doubt about its authority in this regard, the Assistant United States Attorney applied for this Order not just under § 3122 of ECPA [i.e., applying for a Pen-Trap Order under the PRS], but also under 18 U.S.C. §§ 2703(c)–(d) [i.e., applying for a D Order under the SCA for non-content information], which applies to stored electronic data and transactional information about subscribers, and which requires the Government to offer "specific and articulable facts showing that there are reasonable grounds to believe" that the information sought is "relevant and material to an ongoing criminal investigation." In granting the Order, however, the Magistrate determined that the applicant had met only the lower standard of § 3122—a certification that the information likely to be obtained is relevant to an ongoing criminal investigation.

Id. at 23–24.

151. *See id.* at 24–25.

152. *See id.* at 26.

153. *See id.* at 25–26.

154. *See* Kerr, *supra* note 14, at 635–38 (describing attempts by DOJ to amend the PRS prior to the PATRIOT Act).

that followed Judge Orenstein's cell phone tracking decision, Corn-Revere's revelation did not lead any courts to publish decisions that rejected such internet pen register applications.

The next year, on September 11th, 2001, the world turned upside down.

B. Internet Pen-Traps and the PATRIOT Act

It was wholly unsurprising that the DOJ included in its post-9/11 legislative proposals several amendments to the PRS designed to authorize internet pen-traps. The DOJ had already written most of the statutory language for such a "fix" and had even introduced the language in Congress in previous years, although that language had failed to muster enough support to pass.[155] After the terrorist attacks of 9/11, however, Congress sought to give law enforcement and intelligence agencies any tools they claimed were necessary to prevent future attacks,[156] and provided such "tools" in the PATRIOT Act.[157] The Act, *inter alia*, amended the definitions of pen register and trap and trace devices to include devices that intercept any type of dialing, routing, addressing or signaling information.[158]

In supporting the PATRIOT Act's amendments to the PRS, the DOJ revealed that Earthlink had not been alone in receiving government requests to install internet pen registers. In fact, the DOJ had routinely sought and received authorization for internet pen registers from numerous judges across the country.[159] Based on this history, the government claimed that updating the PRS to authorize such surveillance represented a mere clarification rather than a change in the

155. *See id.*

156. *See* Beryl A. Howell, *Seven Weeks: The Making of the USA PATRIOT Act*, 72 GEO. WASH. L. REV. 1145, 1146 (2004) (describing how in the weeks following the 9/11 attacks, "Congress and the administration worked around-the-clock to craft legislation to respond to the stated needs of government agencies to prevent additional terrorist attacks on U.S. soil.").

157. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("PATRIOT Act") of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

158. *See* 18 U.S.C.A. § 3127(3)–(4) (West Supp. 2006).

159. *See, e.g.*, Computer Crime & Intellectual Prop. Section, Criminal Div., United States Dep't of Justice, *Field Guidance on New Authorities that Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001*, Nov. 5, 2001, http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm (noting that "numerous courts across the country have applied the [pre-PATRIOT] pen/trap statu[t]e to communications on computer networks," and that PATRIOT Act "clarif[ied] that the pen/trap statute applies to a broad variety of communications technologies").

law.[160] By amending the PRS to authorize internet pen registers, however, Congress actually expanded the government's surveillance power and effectively rewarded the government's prior overreaching.

The history of the PATRIOT Act amendment raises the question: Upon what legal basis had judges previously granted the government's requests for internet pen register authority? After all, as Mr. Corn-Revere had persuasively argued, the pre-PATRIOT wording of the PRS clearly applied to telephones and not computers.[161] How did all of those judges over all of those years justify the authorization of internet surveillance based on a telephone surveillance statute?

The answer, as shown below, is that they didn't justify it. With one notable exception, they simply signed the orders put before them.

C. Internet Pen-Traps Before the PATRIOT Act

As best we know, prior to the PATRIOT Act, only one magistrate judge followed the PRS's plain, telephone-centric language and denied an application for an internet pen register.[162] Unfortunately, that Judge—Magistrate Judge Patricia Trumbull—never published her written opinion on the matter, and the DOJ chose to "keep quiet" about it at the time.[163] Assuming that the DOJ was not still "keep[ing] quiet" about other denials, every other magistrate to consider the issue chose to sign off on the government's pre-PATRIOT internet pen-trap applications, and most did so without even asking the prosecutors any questions.[164]

Only one judge ever actually wrote an opinion explaining his approval of such an application, although it was not published. That one decision, the same decision described by Corn-Revere in his congressional testimony, was written by Central District of California Magis-

160. *See id.*

161. *See supra* text accompanying note 148.

162. *See In re* United States, Cr-00-6091 (N.D. Cal. Nov. 17, 2000) (Trumbull, Mag.) (unpublished opinion on file with Orin S. Kerr); *see* Kerr, *supra* note 14, at 635 n.134.

163. Kerr, *supra* note 14, at 636. Indeed, the Government has never publicly disclosed Trumbull's decision, leaving Kerr's as the only published account of its contents. *See id.* at 635–36 (describing Judge Trumbull's decision).

164. *Id.* at 633–34 ("Justice Department practice had embraced the pen register statute for several years as the means of conducting Internet [ ] surveillance. Federal judges had at least implicitly agreed: judges had signed pen register orders authorizing Internet email and packet surveillance hundreds, if not thousands, of times in the years leading up to the Patriot Act. While some magistrate judges had asked prosecutors whether the statute applied to the Internet, the judges always satisfied themselves that it did and signed the order.").

trate Judge James McMahon in February of 2000.[165] Judge McMahon's opinion, which he likely wrote only because Earthlink pressed for it, came to light in 2002 in response to a Freedom of Information Act request.[166]

Upon examination, Judge McMahon's decision is rather astonishing. The opinion's legal analysis plainly supports the *rejection* of the application, and most of the decision seems headed that way.[167] Judge McMahon even admits that Congress never intended to authorize such surveillance.[168] Yet the opinion abruptly reverses course, ultimately finding that even though the PRS clearly was not meant to authorize internet surveillance, the court would allow it anyway because it saw "no significant difference" between surveillance of phone numbers and surveillance of e-mail addresses[169]—except, of course, that the PRS authorized one and not the other.

165. *See McMahon Opinion*, Cr. No. 99-2713M (C.D. Cal. Feb. 4, 2000) *available at* http://www.epic.org/privacy/carnivore/cd_cal_order.html (authorizing installation of a pen register to collect addressing information about an Earthlink customer's e-mails in an unpublished opinion). *See also* Kerr, *supra* note 14, at 635 n.134 (describing Judge McMahon's opinion).

166. The decision was FOIA'd by attorneys at the Electronic Privacy Information Center (EPIC), one of whom is now employed at EFF. *See* Electronic Privacy Information Center v. Department of Justice, 2002 WL 1227268, at *1 (D.D.C. Mar. 25, 2002) (ordering FBI to conduct search for documents responsive to EPIC's FOIA request); *see also* EPIC, *Carnivore FOIA Documents*, http://www.epic.org/privacy/carnivore/foia_documents.html (last visited Apr. 6, 2007) (publishing and summarizing documents produced by the FBI).

167. *See, e.g.*, *McMahon Opinion*, Cr. No. 99-2713M, at 6 (C.D. Cal. Feb. 4, 2000) (noting that "one of the evident purposes of [the PRS] is to regulate government intrusion into private communications, and that the statute should be strictly construed"); *id.* at 5 (finding that pen registers and trap and trace devices "include only devices that are attached to a telephone line," and noting that Pen-Trap Orders must include "the number and, if known, physical location of the telephone line" to be monitored).

168. The court repeatedly admits that the statute was not intended for such use. For example:

> It is apparent that a pen register, as defined in the statute, is intended to be a device which captures the telephone numbers dialed by a target phone. . . . It is also fairly clear that the drafters of the pen register statute did not contemplate that the statute would be used to authorize the issuance of court orders to capture the e-mail addresses of persons sending e-mail to and receiving e-mail from a targeted e-mail address.

See McMahon Opinion, Cr. No. 99-2713M at 4–5; *see also id.* at 7 (use of Pen-Trap Orders for internet surveillance was "apparently not contemplated by the drafters of the original statute."). Notably, when Congress fashioned its intent on this score in 1986, it was already well aware of e-mail technology, *see, e.g.*, S. REP. 99-541, at 3556–58, 3562, 3568 (1986) (discussing electronic mail), and could easily have written the PRS to extend to internet surveillance. It chose not to.

169. *See McMahon Opinion*, Cr. No. 99-2713M, at 6; *see also id.* at 6–7 ("This court finds that the intrusion into otherwise private activity which would be allowed by the issuance of

McMahon's decision, the lone legal artifact excavated from this secret history of internet surveillance, remains the only known written analysis justifying a court's issuance of a pre-PATRIOT Act Internet Pen-Trap Order. Considering that example, which reads like a document from beyond the looking glass, how much mileage might the DOJ get out of longer and better-reasoned opinions such as Judge Gorenstein's cell phone tracking decision? And how might the DOJ convince Congress to "clarify" the law in the aftermath of a future national crisis, based on its years of secret reliance on D Orders for cell tracking? Will it be able to convince Congress to "clarify" that the SCA authorizes prospective surveillance, thereby up-ending the entire structure of surveillance law and rendering the Wiretap Act and the PRS irrelevant?

No one knows.

IV. Breaking the Pattern: Causes and Prescriptions

A. The "Ratcheting Up" of Government Surveillance Authority

The DOJ's successful bid to expand its internet surveillance authority as part of the PATRIOT Act illustrates a phenomena that is key to the DOJ's above-described successes before the magistrate bar. Professor Peter Swire calls this phenomenon the "ratchet[ing]-up" effect: "a systemic tendency toward permitting greater surveillance over time . . . ."[170] Although Professor Swire focuses on the "ratcheting up" of surveillance authority by Congress,[171] the case studies above demonstrate that the DOJ has also been successful at prevailing upon judges to ratchet up its surveillance authority.

The case studies demonstrate that the DOJ has routinely secured court approval under the PRS and SCA for surveillance that on a correct reading of the law would require a probable cause warrant or even a Wiretap Act "super-warrant,"[172] based on arguments that have

the government's requested order is no greater than the intrusion created by the issuance of a conventional pen register order.").

170. Peter P. Swire, *Katz is Dead. Long Live Katz*, 102 MICH. L. REV. 904, 914 (2004) [hereinafter Swire, *Katz Is Dead*]. *See also* Peter P. Swire, *The System of Foreign Intelligence Law*, 72 GEO. WASH. L. REV. 1306, 1348–49 (2004) [hereinafter Swire, *Foreign Intelligence Law*] (discussing same "ratcheting-up" effect).

171. *See, e.g.*, Swire, *Foreign Intelligence Law*, *supra* note 170, at 1348-49.

172. *See* discussion *supra* Part I.A. (describing government's routine use of PRS to obtain PCTDDs that include content without getting Wiretap Order, based on argument that contradicts plain language of PRS, which prohibits collection of content); discussion *supra* Part II.C. (describing government's routine tracking of cell-phones in real time without a warrant, based on the unsupported argument that the SCA authorizes the prospective ac-

often flatly contradicted the DOJ's public positions.[173] The case studies further show that the government has used these strained arguments for years at a stretch,[174] sometimes radically shifting arguments in response to enhanced judicial scrutiny.[175] Undoubtedly with that in mind, the DOJ has often sought to avoid such scrutiny by withholding briefing and failing to seek appellate review.[176] Furthermore, the internet pen register case study demonstrates how, depending on the political climate, the exposure of the DOJ's years of "ratcheted up" surveillance can ironically serve to fuel congressional approval its practices, reinforcing rather than weakening the legislative ratcheting-up effect.[177]

Professor Swire describes the legislative ratcheting-up effect in terms equally applicable to the judicial ratcheting-up demonstrated by the case studies:

> This tilt toward surveillance comes in part from expertise and institutional staffing in federal law-enforcement agencies. As these agencies face the detailed requirements of the Electronic Commu-

quisition of information, or based on the widely rejected *post-hoc* hybrid theory); discussion *supra* Part III.A. (describing government's routine internet surveillance based on PRS prior to 2001, when PRS's plain language only authorized Pen Register surveillance of telephones).

173. *See* discussion *supra* Parts II.B. and II.C. (describing how government publicly interpreted SCA to only authorize acquisition of information retrospectively, while using it to obtain information prospectively); discussion *supra* Part I.C. (describing government's implicit argument that Wiretap Act's exclusionary rule applies to electronic communications despite longstanding position to the contrary).

174. *See* discussion *supra* Part I.C. (describing how full PCTDD surveillance via PRS was routine practice in 2000 when government briefed Leahy, despite 1994 amendment requiring filtering of content); discussion *supra* Part I.D. (describing how full PCTDD surveillance via PRS was routine practice in 2006 when government briefed Judge Smith, despite 2001 amendments explicitly forbidding the use of Pen Registers to collect content); discussion *supra* Part II.F. (describing how government used D Orders for cell phone tracking for "a decade or more" after 1994); discussion *supra* Part III.A. (describing how internet pen-traps were routinely authorized under the PRS before the statute was amended in 2001 to allow such surveillance).

175. *See* discussion *supra* Part II.C. (describing how government, after a decade or more of obtaining cell tracking authority via D Orders, shifted to the hybrid argument as soon as Judge Orenstein publishes his first decision on the issue); discussion *supra* Part I.E. (describing how government, after failing to convince several courts to allow surveillance of PCTDD content based on its voluntary guidelines concerning the use of content, began to argue that the Wiretap Act's exclusionary rule applies).

176. *See* discussion *supra* Part II.D. (describing DOJ's failure to appeal repeated denials of cell tracking applications); *supra* note 188 and accompanying text (describing how DOJ chose to "keep quiet" rather than appeal Judge Trumbull's denial of its application for an Internet Pen-Trap Order).

177. *See* discussion *supra* Part III.B. (describing how DOJ's Internet pen register practice was legitimized by passage of PATRIOT Act in 2001); *see also* Swire, *Katz Is Dead*, *supra* note 170, at 914 (discussing PATRIOT Act as example of legislative "ratcheting up" effect).

> nications Privacy Act and similar statutes, they use their expertise much as any other regulated industry would in response to regulations that limit its preferred behavior. *The regulated industry of law enforcement has a concentrated interest in reducing regulation—pushing for fewer warrants, less onerous reporting requirements, and so on.* The concentrated interest in reducing regulation contrasts with the dispersed interest the general public has in protecting privacy over the long term.[178]

DOJ has the same "concentrated interest" in court that it has in Congress: an interest in obtaining more surveillance authority with less accountability, which typically means being able to conduct surveillance without first establishing probable cause. And although potent in the legislative process, this ratcheting-up effect may be even more potent in the *ex parte* surveillance application process, where the general public's interest in protecting privacy—more than simply being dispersed—is wholly unrepresented.

The DOJ's position as the sole stakeholder in the application process is further strengthened by the fabled complexity of the ECPA[179] and the difficulty of applying it to new technologies that may be new and unfamiliar to the court. These complications require the court to rely even more heavily on the DOJ's (oft-withheld) expertise and take its word that the government's position is correct. Faced with such a complex statutory and technological landscape, an undoubtedly heavy workload, and only one self-interested stakeholder to provide advice, it is no surprise that the magistrate bar—just like Congress, under Swire's theory[180]—has ended up behaving like a captured regulatory

178. *See* Swire, *Katz Is Dead*, *supra* note 170, at 914 (citation omitted) (emphasis added).

179. For example, Professor Kerr summarizes repeated judicial complaints about ECPA's lack of clarity:

> The law of electronic surveillance is famously complex, if not entirely impenetrable. Even before Congress added the Internet to the surveillance laws in 1986 [with ECPA], the Fifth Circuit described the Wiretap Act as "a fog of inclusions and exclusions" that frustrated the judicial search for "lightning bolts of comprehension." The same court has since explained that that "construction of the Wiretap Act [as amended by ECPA] is fraught with trip wires," and in a case involving the intersection between the Wiretap Act [as amended by the ECPA] and the Stored Communications Act, that the law is "famous (if not infamous) for its lack of clarity." The Ninth Circuit has remarked that the Fifth Circuit's complaints "might have put the matter too mildly," and agreed that the surveillance laws involve "a complex, often convoluted, area of the law." More recently, the Ninth Circuit reversed its own panel decision applying the Wiretap Act [as amended by ECPA] and the Stored Communications Act to the Internet, explaining in its latter opinion that Internet surveillance remained "a confusing and uncertain area of the law."

See Kerr, *Lifting the "Fog" of Internet Surveillance*, *supra* note 61, at 820–21 (citations omitted).

180. *See* Swire, *Katz Is Dead*, *supra* note 170, at 914.

agency that legitimates rather than limits the DOJ's behavior. The easiest and most natural path for the magistrate court is to trust the process: to simply sign the papers that are put in front of it, and hope that the prosecutor is honestly advising it as to the substance of the law rather than hiding the ball.[181]

As recounted in the case studies, a number of judges—after previously signing off on the DOJ's applications without question—have finally escaped their "capture" by the DOJ, uncovering and rejecting previously unstated legal arguments behind the DOJ's surveillance applications. This magisterial revolt, particularly in the context of cell phone tracking, represents a heartening new development that may point the way toward greater accountability by the DOJ about its surveillance practices. To fully bring that about, however, courts and Congress need to do more to fully expose the shoddy rationales behind the DOJ's other surveillance practices. For now, only the DOJ knows what those are.

B. How Can the Courts Combat the DOJ's Secret Law?

As the case studies show, there are a number of steps that the magistrate bar can take to weaken the concentrated interest of the DOJ when it comes to the surveillance application process and thereby better regulate the DOJ's behavior.

First, magistrates should share information with each other. The DOJ derives part of its advantage in the surveillance application process from the dispersed interest, not just of the public, but also of the magistrate bar itself. As discussed further below, there is no centralized reporting available to the judges about how the SCA and PRS are used. Therefore, unless the magistrates are comparing notes with their colleagues, they have no way of knowing the DOJ's surveillance arguments and practices in front of other courts and no way of catching the DOJ when it contradicts itself or begins to overreach. For example, the magisterial revolt against the DOJ's cell phone tracking practice likely would not have occurred if Judge Orenstein had not first begun discussing the issue with his colleagues.[182]

181. *See id.* at 926, *citing* HERBERT A. SIMON, THE SCIENCES OF THE ARTIFICIAL (1981) (noting that when decision makers are faced with complex problems, they begin to forego "substantive rationality," i.e., getting the correct answer, for "procedural rationality," relying on process and the expertise of others in place of independent substantive analysis).

182. *See, e.g., Orenstein Opinion I*, 384 F. Supp. 2d at 566 ("[I]t is my understanding based on anecdotal information that magistrate judges in other jurisdictions are being confronted with the same issue").

Second, magistrates should require the DOJ to articulate its legal arguments. As demonstrated above, the government does not typically brief its surveillance applications, and many magistrates don't even ask the government any questions about its legal rationales. Of course, neither the DOJ nor the magistrates have the time or resources to fully litigate the propriety of every application. However, when faced with a novel surveillance application or when reconsidering types of applications that it has routinely signed without question in the past, a magistrate judge should require briefing by the government. Ideally, the court should place that briefing and the application text itself—minus any identifying details that might harm the government's investigation—on the public docket so that Congress, providers, and the public, as well as other magistrates, can learn of the DOJ's positions. If just one of the first judges to consider issuing a D Order for cell phone tracking had taken these steps, the DOJ's radical interpretation of the SCA could have been uncovered and corrected over a decade ago.

Third, magistrates should seek out adversarial voices to counter the lack of adversity inherent in the *ex parte* surveillance application process. Again, neither the DOJ nor the magistrates have the time or resources to fully litigate the propriety of every application. Nonetheless, when faced with particularly novel or troublesome applications, magistrates should follow the lead of Judges Orenstein, Smith, and Azrack and invite or appoint amici to argue against the government. This way, courts can offset the DOJ's advantage as the sole stakeholder in the application process and hear from a representative of the dispersed public interest in preserving privacy against government overreaching.

Finally, and most importantly, after requiring briefing by the government, and ideally soliciting or appointing adversarial amici, magistrates should publish opinions explaining their approvals or denials of the government's more novel or troublesome surveillance applications. By doing so, they can foster dialogue within the magistrate bar about the practices in question, establish a body of published law to counter the DOJ's secret law, and alert the public and policy makers to any government overreaching. The publication of denials may also prompt the government to appeal, which would generate higher court precedent to help guide the magistrates.

By taking these steps in select cases, the magistrate bar may help to stem the "ratcheting up" of government surveillance authority in the *ex parte* process. However, there are limits to what magistrate

judges alone can accomplish, considering the practical constraints on their time and resources (as well as those of the government and potential amici). Magistrates cannot fully consider the legality of every application crossing their desks, or even every type of application, and by necessity must place a great deal of trust in the prosecutors before them. Therefore, Congress must add new accountability mechanisms to the relevant statutes to effectively beat back the growth of the DOJ's secret body of electronic surveillance law.

C. How Can Congress Combat the DOJ's Secret Law?

The PRS and the SCA sorely lack procedural safeguards and accountability measures to ensure that the surveillance conducted under their authority actually satisfies their legal requirements. This lack stands in sharp contrast to the Wiretap Act.[183] Congress could better rein in the government's overreaching, enhance accountability, and spur litigation to establish precedent simply by updating the SCA and PRS to include safeguards similar to those in the Wiretap Act.

First, Congress should expand the Wiretap Act's exclusionary rule to include electronic communications and records. As already discussed, the Wiretap Act's exclusionary rule applies only when agents obtain the content of oral or wire communications in violation of the Act. It does not require the exclusion of ill-gotten electronic communications. Due to this limitation, there is a lack of litigation, and therefore court precedent, on key ECPA questions.[184] Professor Orin Kerr has referred to this continuing lack of precedent as a "fog" surrounding surveillance law.[185] The case studies demonstrate that this fog has increased the DOJ's advantage when it applies to the courts for surveillance authority. Congress should dispel this fog—not merely by requiring the exclusion of illegally obtained electronic communications, as Professor Kerr and others have proposed,[186] but by also requiring the exclusion of non-content communications records and

183. *See* Freiwald, *Online Surveillance*, *supra* note 72 (comparing the Wiretap Act to the SCA and PRS and arguing that the latter two statutes should be amended to include more of the Wiretap Act's protections).

184. *See* Kerr, *Lifting the "Fog" of Internet Surveillance*, *supra* note 61, at 807.

185. *Id.*

186. *See, e.g.*, *id.* at 836-41 (explaining and defending proposals to broaden exclusionary rule); Leib, *supra* note 61, at 410-11; Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1436 (2004) (recommending a statutory suppression remedy under the SCA and for electronic communications under the Wiretap Act).

other information obtained in violation of the PRS or SCA.[187] Not only would such a measure help spur litigation of unresolved ECPA issues in suppression hearings, it would also strongly deter government overreaching. Knowing that information obtained in violation of the PRS or SCA may be excluded, the government would be less likely to attempt illegal surveillance.

Second, Congress should strengthen the civil causes of action for violations of the ECPA. The minimal amount of civil court precedent interpreting the ECPA exists thanks to the civil causes of action that exist in the statute.[188] However, although there are civil remedies for violations of the Wiretap Act and the SCA,[189] there is no corresponding civil action for violation of the PRS. Furthermore, the existing civil remedies for Wiretap Act and SCA violations were significantly and unjustifiably weakened by the PATRIOT Act.[190] Congress could spur the development of surveillance case law and thereby provide precedent to guide the magistrate bar if it reversed the changes made by the PATRIOT Act and created an additional civil cause of action for violation of the PRS.

Third, Congress should strengthen the notice requirements in the PRS and the SCA. In order for those who have been illegally surveilled to take advantage of statutory causes of action, they first have to know that they were surveilled. Under the Wiretap Act, within ninety days after a wiretap has ended, the court that authorized the wiretap must notify the surveilled parties.[191] In sharp contrast, the PRS does not include any notification requirement. And although the SCA nominally requires prior notice when the government uses a D Order or a subpoena to obtain content,[192] the government can easily obtain a court order delaying that notice merely by certifying that

187. *See* Freiwald, *Online Surveillance, supra* note 72, at 79-84 (making a similar proposal to Professor Kerr's).

188. *See id.* at 807, 829.

189. *See* 18 U.S.C. § 2707 (authorizing civil actions against parties other than the United States for violations of the SCA); § 2511 (authorizing civil actions against parties other than the United States for violations of the Wiretap Act); § 2712 (authorizing civil actions against the United States for violations of the Wiretap Act and the SCA). There are no corresponding provisions in the PRS.

190. *See* USA PATRIOT Act, Pub. L. No. 107-56, § 223 (amending civil action provisions in Wiretap Act and SCA); *see also* EFF, *Let the Sun Set on PATRIOT—Section 223: "Civil Liability for Certain Unauthorized Disclosures," available at* http://www.eff.org/patriot/sunset/223.php (summarizing and criticizing those amendments).

191. *See* 18 U.S.C. § 2518(8)(d) (2000).

192. *See* 18 U.S.C. § 2703(a)-(b) (2000).

prior notice to the target would harm its investigation.[193] Moreover, providing notice remains the responsibility of the government, rather than the court,[194] and neither prior notice nor after-the-fact notice is ever required when the government obtains non-content records and other information.[195] Congress should require at least post-acquisition notice for all investigations under the PRS and SCA, and should allow delayed notice under the SCA only when the government can articulate specific facts that support its contention that notice would harm the investigation. Furthermore, Congress should place the responsibility for providing notice in the hands of the court and not the government, which has no incentive to follow through on its own.

Finally, Congress should require more reporting about how the PRS and the SCA are used. As recent events surrounding the FBI's use of its national security-related surveillance authorities have shown, the government cannot be relied upon accurately to report on its own conduct.[196] Yet, just as it has left the fox in charge of the hen house when it comes to notice under the SCA, Congress has similarly ceded to the government control over reporting when it comes to the PRS. The Wiretap Act requires that the courts submit detailed annual reports on how that statute is being used by state and federal law enforcement,[197] and those reports are made publicly available for review by Congress, the courts, communications providers, and interested members of the public.[198] Under the reporting requirements of the

193. *See* 18 U.S.C. § 2705 (2000) (allowing government to delay notice by obtaining a court order based only on a certification from a supervisory official that notice would adversely affect the investigation).

194. *See* 18 U.S.C. § 2703(b) (2000) (prior notice comes "from the governmental entity" seeking information from the communications provider). *See also* Freiwald & Bellia, *supra* note 81 (describing a case in which a court criticized the government for long delaying notice to the target of a search under the SCA).

195. *See* 18 U.S.C. § 2703(c)(3) (2000) ("[A] governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.").

196. *See, e.g.*, U.S. Department of Justice, Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of National Security Letters*, at 34, Mar. 2007, *available at* http://www.usdoj.gov/oig/special/s0703b/final.pdf (finding that the Attorney General's semiannual reports to Congress on the FBI's use of National Security Letters ("NSLs"), secret government requests for communications and financial records that are used in national security investigations, "significantly understated" the number of NSLs actually issued by the FBI).

197. 18 U.S.C §§ 2519(2)–(3) (2000).

198. *E.g.*, United States Courts, Wiretap Reports, http://www.uscourts.gov/library/wiretap.html (last visited May 2, 2007) (providing the reports from 1997 to 2006).

PRS,[199] however, it is the Attorney General, rather than the courts, that reports directly to Congress.[200] Furthermore, the reports, which contain similar but less detailed information than the reports on wiretaps, are not published.[201] The SCA, meanwhile, does not require *any* reporting to Congress about how the government uses the statute. In order to foster accountability and break the DOJ's practical monopoly on information about how it is using its surveillance authority, Congress should strengthen the PRS reporting requirement by requiring more details, placing reporting in the hands of the courts, and requiring publication of the reports. Then, it should introduce the exact same requirements into the SCA.

V. Conclusion

If more magistrates follow the lead of newly vigilant magistrate judges such as Smith and Orenstein, and if Congress passes accountability-enhancing amendments such as those proposed here, the DOJ's "ratcheting up" of its surveillance authority through the *ex parte* process might be significantly slowed, if not halted outright. And, perhaps, we may finally uncover the DOJ's secret law of electronic surveillance in its entirety and prevent the development of such secret law in the future. Until then, though, only the DOJ will know the whole story.

199. *See* 18 U.S.C. § 3126 (2000) (describing mandatory reporting under PRS); *compare* 18 U.S.C. § 3126 *with* 18 U.S.C. § 2519(2) (describing mandatory reporting under Wiretap Act).

200. *See* 18 U.S.C. § 3126 (2000).

201. EFF is currently seeking to obtain the government's PRS reports under the Freedom of Information Act. *See* Letter from Marcia Hofmann, Staff Attorney, Electronic Frontier Foundation, to Melanie Ann Pustay, Deputy Director, U.S. Department of Justice Office of Information and Privacy (Feb. 6, 2007) (on file with author); Letter from Laurie Ann Day, Senior FOIA Specialist, U.S. Department of Justice Office of Information and Privacy, to Marcia Hofmann, Electronic Frontier Foundation (Mar. 2, 2007) (on file with author).