U.S. Department of Justice

United States Attorney
Eastern District of New York

156 Pierrepont Street

Brooklyn, New York 11201

Mailing Address: *147 Pierrepont Street*
Brooklyn, New York 11201

July 31, 2007

Hon. Joan M. Azrack
United States Magistrate Judge
Eastern District of New York
225 Cadman Plaza East
Brooklyn, New York 11215

Re: Applications And Orders For Pen Registers/ Trap and Trace Devices (Post-cut-through Dialed Digit Litigation), Docket Nos. 06-MC-547, 06-MC 561, 07 Misc. 120 (JMA)

Dear Magistrate Judge Azrack:

The government respectfully writes in reply to the supplemental memorandum of law dated July 16, 2007 submitted by amicus curiae Federal Defenders of New York, Inc. ("amicus").[1]

A. Introduction

The Court directed the government and amicus to brief "the issue of whether the Fourth Amendment acts as an absolute bar to Government access, pursuant to the Pen/Trap Statute, of post-cut-through dialed digits that may contain content." To the extent that its brief ("Amicus July 16 Br.") actually addresses this question (Id. at 6-27) rather than revisit covered ground (Id. at 29-45), amicus attempts to do what reason and principle preclude: avoid the analogy between this case and Smith v. Maryland, 442 U.S. 735 (1979), that makes incidental access to PCTDD content as permissible under the Fourth Amendment as the recording of directly-dialed telephone numbers is under Smith.

As detailed in our June 1, 2007 brief ("Gov. June 1 Br."), the Fourth Amendment does not prohibit operation the Pen/Trap Statute's provisions that authorize the government to use

[1] Amicus brief credits both Federal Defenders as well as another group, the Electronic Frontier Foundation ("EFF"). EFF has not sought permission to appear as amicus in this case, nor did Federal Defenders make any such request on EFF's behalf .

a pen register to collect and use PCTDD non-content, and as an incident thereof, permit the government to access -- but not to use -- PCTDD non-content, when there is no "technology reasonably available to" the government to prevent that incidental access. See 18 U.S.C. § 3121(c). Under Smith and the two principal cases on which it relies, Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J. concurring) and United States v. Miller, 425 U.S. 435 (1976) a caller has no reasonable expectation of privacy in the incidentally-accessed PCTDD content, and in the absence of such an expectation, the Fourth Amendment does not prohibit the government from obtaining such access without a warrant issued upon probable cause .

B. The Katz Test

Katz established a two-prong test of reasonable expectation that was decisive in Smith and that in the present similar circumstances, permits the government to access PCTDD content pursuant to 18 U.S.C. § 3121(c) in the course of collecting PCTDD non-content for investigative use. A reasonable expectation of privacy that triggers the warrant requirement of the Fourth Amendment exists only if the claimant of the expectation has an "actual [subjective] expectation of privacy" and that expectation is "'one that society is prepared to recognize as 'reasonable.'" Katz, 389 U.S. at 361.

1. No Subjective Expectation Of Privacy

In this case, no caller can credibly maintain a subjective expectation of privacy with respect to either PCTDD content or non-content. For as was the case with respect to the pre-cut-through digits at issue in Smith, it is obvious -- and therefore common knowledge -- that an originating telephone service provider can easily record all dialed digits that a caller enters on his telephone keypad and, if that provider suspects calling fraud or abuse over its network, it may well record them. Smith, 425 U.S. at 742-43, Govt. June 1 Br. at 9-10, 21-23. Thus, "it is too much to believe," Smith, 425 U.S. at 43, that any caller believes that a provider will not be exposed to and cannot record all of those digits, whether pre- or post-cut-through, non-content or content.

Accordingly, under Smith, amicus' emphasis on the fact that PCTDD content includes information of a confidential nature, such as credit card numbers (Amicus June 16 Br. at 10-11) is very much beside the point. A caller who wishes to telephone another person knows that he "must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." Smith, 425 U.S. at 742. The caller therefore has no credible subjective expectation of privacy that in the course of dialing, he will not reveal those numbers to that company. Id. By the same token, that caller also has no sustainable subjective expectation of privacy with respect to other digits that he dials, whether PCTDD content or non-content, since he knows that he must convey those digits to the originating service provider, through whose switch those digits must pass before reaching their ultimate intended recipient. Id.

2. No Expectation Of Privacy That Society Is Prepared To Recognize As Reasonable

Under Katz' other prong, an expectation of privacy in incidentally-accessed PCTDD is for several reasons, not "one that society is prepared to recognize as reasonable." Katz, 389 U.S. at 361. First, the harm to society of recognizing such an expectation is unacceptable. As previously explained, in many instances it would effectively condition the government's ability contemporaneously to collect and use PCTDD non-content under the Pen/Trap Statute on whether it could meet the far more demanding requisites of Title III necessary to obtain concurrent judicial authorization to collect and use PCTDD content. Thus, law enforcement's ability to use investigative tools that since Smith was decided in 1979, it has clearly been entitled to use to obtain non-content, would be thwarted. See Govt June 1 Br., at 31-34. Secondly, Congress' decision to permit incidental access to PCTDD content pursuant to 18 U.S.C. § 3121(c) is powerful evidence that society does not recognize an expectation of privacy in incidentally-accessed PCTDD as reasonable. That legislative determination is entitled to deference. See Govt June 1 Br. at 26-28.

Third and related, as in Smith, an expectation of privacy in incidentally-accessed PCTDD is antithetical to the bedrock principle of society that "a person has no legitimate expectation of privacy in information that he voluntarily turns over to third parties." Smith, 442 U.S. at 743-44. Relying principally on United States v. Miller, 425 U.S. 435, Smith held that a caller who voluntarily conveys digits needed to connect a call to a provider who has "facilities to record it and that it [is] free to record" assumes the risk that the provider "will reveal to the police the numbers that he dialed. 442 U.S. at 744-745.

In the instant circumstances, a caller assumes a similar risk with respect to the capture of PCTDD content. A caller transmits PCTDD content to his provider using the exact same mode as he uses to convey PCTDD non-content: by dialing digits on his telephone's keypad to a channel that carries PCTDD content and PCTDD non-content alike.[2] To detect fraud or other abuse of its network, a provider typically has facilities to record PCTDD carried over that channel. See Govt June 1 Br. at 9-10. As the Court is aware from earlier briefings, however, the limits of technology are such that the provider (like the government) cannot immediately differentiate PCTDD content from non-content, but rather, must record the entire string of PCTDD on a call, then analyze its components to identify which parts are which. Accordingly, a caller who voluntarily commingles PCTDD content with the PCTDD non-content that he conveys to his originating provider assumes the risk that the provider will disclose to the government not just PCTDD non-content, but also PCTDD content. Smith, 442 U.S. at 744-745.

Amicus denies this analogy using two flawed gambits: (a) insinuating what it would prefer the Fourth Amendment to require -- an absolute ban on the warrantless collection of

---

[2] By contrast, monitoring of PCTDD carried over the channel does not require interception of oral conversations because the PCTDD .s detected by tone decoders that recognize and record touch-tones, but not the sound of a human voice,

telephone content -- for the assumption of risk principles that under Katz, actually determine whether one has a reasonable expectation of privacy with respect to either content or non-content and (b) repeated citation to a recent Sixth Circuit case, Warshak v. United States, ___ F.3d ___ , 2007 WL 1730094 (6th Cir. June 18, 2007) that plainly errs by ignoring Smith's holding that a person assumes the risk that its service provider will disclose information to the police whenever the provider has capacity and right to record that information, without regard to how frequently the provider actually records it. (See Amicus July 16 Br. at 6-27)

--Only Telephone Content As To Which One
Has A Reasonable Expectation Of Privacy
Is Subject To The Fourth Amendment's Protection

Amicus posits that Katz established a rule in which "[t]he content of telephone calls enjoy "full Fourth Amendment protection." (Amicus July 16 Br., at 14, to similar effect, Id at 8-9, 11). It further purports that when Smith held that dialed telephone numbers are not so protected, it "affirm[ed]" the "rule" of "full" protection for telephone content when it observed that (as of the time Smith was decided) "a pen register differs significantly from the listening device employed in Katz, for the pen registers do not acquire the contents of communications," but rather, ". . . 'only the telephone numbers that have been dialed.'" Amicus July 16 Br. at 15 , quoting Smith v. Maryland, 442 U.S. at 741 (quoting citation omitted).

Thus, amicus hints that the Fourth Amendment imposes something that it plainly does not: an entirely content-focused rule in which telephone content always requires a warrant and telephone routing information does not. Conspicuously missing from the cited passages of amicus' brief, is any acknowledgment that the constitutional protections afforded telephonic content and non-content are both determined by the Katz test of whether the party's expectation of privacy is reasonable. With respect to telephone content, there is no absolute right of privacy requiring a warrant, anymore than the government is entitled in every instance to obtain telephone non-content without a warrant. For example, while Katz established that without more, the government cannot intercept a telephone conversation without a warrant, 389 U.S. at 353-54, obviously a caller assumes the risk that the person he calls has consented to the government's recording the call, in which case no warrant is required. See, e.g., United States v. Bonnano, 487 F.2d 654, 657-58 (2d Cir. 1973) (Friendly, J).[3] By the same token, in Smith, the Supreme Court did not end its inquiry upon observing that pen registers of that era registered only telephone numbers rather than conversation, 442 U.S. at 741. Rather, that observation was merely prefatory to Justice Blackmun's applying

[3] "[A]lthough a person having a telephone conversation with another in regard to criminal activities generally does not expect that the latter will reveal this to the police, he has no "justifiable" expectation, see Katz v. United States [389 U.S. at 353], that the latter may not do so or may not have consented to a government agent's listening in or making a recording. Bonanno, 487 F.2d at 658 (relying on United States v. White, 401 U.S. 745, 753 (1971) (plurality opinion)).

Katz' two-pronged test to ascertain whether a person has a reasonable expectation of privacy in the telephone numbers that he dials, 442 U.S. at 742-745.

Accordingly, however much amicus would prefer otherwise, the Court is obliged to inquire into whether a caller has a reasonable expectation of privacy in PCTDD content. Moreover, that inquiry must be conducted consistent with the analysis of assumption of risk of disclosure to the police that was followed in the precedent whose facts most closely parallel those here: Smith v. Maryland.

--Amicus' Reliance On Warshak Is Unavailing

Amicus is no more persuasive when it argues based on Warshak callers do not assume the risk that their provider will disclose incidentally-accessed PCTDD content unless the provider conducts "'wholesale inspection, auditing or monitoring'" of that content not in "'limited circumstances,'" but rather, routinely. Amicus Br. at 20-21 (quoting Warshak, 2007 WL 1730094 at *12). In Warshak the Sixth Circuit held that a holder of an e-mail account retains an expectation of privacy in the contents of messages that he stores with his Internet service provider ("ISP"), except when the ISP has "complete access" to the messages and "actually relies on utilizes this access in the normal course of business." Warshak, 2007 WL 1730094 at *15. In reaching that conclusion, the Sixth Circuit emphasized its view that such "regula[r]" access was necessary to a finding that a person had assumed the risk of disclosure by a provider receiving a communication and that by contrast, the mere ability of an "intermediary . . . to access that information" would result in no telephone conversations, letters deposited in the mail or safe deposits boxes at a bank being subject to an expectation of privacy. Id., 2007 WL 1730094 at *15. Pressing the analogy to Warshak, amicus asserts that like the e-mail accountholder in that case, a telephone caller does not assume the risk that his service provider will disclose PCTDD content to the police, for a typical telephone service provider does not record PCTDD routinely, but rather, deploys it when the provider suspects fraud or other abuse of its network. Amicus July 16 Br. at 19-21.

Warshak was erroneously decided, however and therefore amicus's arguments are likewise in error. Only by ignoring a key passage of Smith v. Maryland did the Sixth Circuit and now amicus reason to their questionable conclusions. Smith specifically holds that a caller's assumption of the risk that his provider will disclose the digits conveyed depends on the provider's capacity to record those digits, not the frequency with which recording occurs. Emphasizing that the Supreme Court declined "to make a crazy quilt of the Fourth Amendment," that "would be dictated by the billing practices of a" provider, Justice Blackmun emphasized that "the fortuity of whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed does not in our view, make any constitutional difference." Smith, 442 U.S. at 744-45.

In this case, it likewise makes no difference for Fourth Amendment purposes whether a provider elects to track potential fraud or other abuse by recording all PCTDD for every telephone using its network or instead records selectively, based on particular suspicion. A caller's assumption of the risk that PCTDD content that he conveys will be recorded depends on the confluence of two factors: (a) as in Smith, the provider's capacity to record non-content and (b) the

caller's decision to convey PCTDD content to its provider by the same mode as PCTDD non-content, when it is impossible for PCTDD content to be culled from non-content in advance of the provider (or the government) recording and examining both.

Accordingly, so long as the caller "voluntarily conveys" the entirety of the PCTDD to the provider, which "ha[s] facilities for recording and that it is free to record," Smith, 442 U.S. at 745, that caller assumes the risk that the provider will disclose PCTDD content and non-content alike to law enforcement. By contrast, the Sixth Circuit in Warshak and amicus in its most recent brief do precisely what Smith condemns: determine constitutional privacy based on the fortuity of whether a provider invariably records content, rather than on the provider's capacity to record.[4]

Moreover, even were Warshak correct that privacy protections for the content of e-mail and telephone conversation should depend on such fortuities (Id., 2007 WL 1730094 at *15), the risk that a caller assumes with respect to disclosure by its provider of PCTDD is materially different. Thus, Warshak is distinguishable on its own terms. Unlike persons who convey content via email or in a telephone conversation callers who transmit PCTDD content do not merely voluntarily convey content to their provider. Rather, they voluntarily commingle that content with PCTDD non-content on a channel in which the two forms of PCTDD are inextricable (until recorded, then examined). Accordingly, the risk that a caller bears that his provider will record of PCTDD content is determined by the risk that he assumes that the non-content with which it is mixed will be recorded.[5] Thus, however much amicus insists to the contrary based on Warshak, it is simply not the case that Fourth Amendment protections for other forms of content would be eroded by the Court holding that persons have no reasonable expectation of privacy in incidentally recorded PCTDD content. While we submit that the Fourth Amendment does not require it, the

---

[4] The principal authority cited by Warshak and amicus for their claim to the contrary largely is United States v. Heckenkamp, 481 F.3d 1142 (9th Cir. 2007). Heckenkamp, however, does not in fact stand for the proposition that the Sixth Circuit and amicus attribute to it. Heckenkamp held that "limited instances in which university administrators may access" the defendant's computer "in order to protect the university's systems"did not eliminate Heckenkamp's "expectation of privacy in his computer." 482 F.3d at 1147 (emphasis added). Thus, Heckenkamp did not decide whether a person has a reasonable expectation in information that he conveys to a service provider and that it has the capacity to record, but rather, that one retains a reasonable expectation in the evidence contained in one's own property, to which one gives another party access in limited circumstances. Id. Accordingly, Warshak's holding that one retains an expectation of privacy in information that one transmits to someone else's information system even if that someone else has the capacity to record that information is without precedent.

[5] For example, even as to a provider whose interest in PCTDD is limited to it non-content segments (e.g., when the provider investigates toll fraud), every caller runs the risk that as a necessary incident of record non-content dialed digits, his provider will also have to record the content interspersed with it.

Court may so hold only because a caller assumes the risk of disclosure to the government by conveying PCTDD content to his provider, but also because his decision to communicate that content by the same mode as PCTDD non-content results further deepens the risk of disclose that he assumes. That additional (and unusual) circumstance vitiates any claim under Warshak that pegging a caller's assumption of the risk with respect to PCTDD content to the frequency with which his provider records it undermines Fourth Amendment protections for other forms of content in which the same circumstance of the caller intermingling content with non-content is absent.

CONCLUSION

For all of the above reasons, the Court should grant the government's request to permit the subject pen registers to acquire PCTDD non-content and incidentally to access but not to use PCTDD content.

ROSLYNN R. MAUSKOPF
United States Attorney

By: _____
Jed Davis
Assistant U.S. Attorney
(718) 254-6298

cc: Yuanchung Lee, Esq.