No. 08-4227

IN THE UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER DIRECTING A PROVIDER OF ELECTRONIC COMMUNICATION SERVICE TO DISCLOSE RECORDS TO THE GOVERNMENT

Appeal from Memorandum Order
Entered by the United States District Court
for the Western District of Pennsylvania (McVerry, J.)
at Magistrate No. 07-524M

GOVERNMENT REPLY BRIEF

MARY BETH BUCHANAN
United States Attorney

Robert L. Eberhardt
Assistant U.S. Attorney

Mark Eckenwiler
Associate Director
United States Department of Justice
Office of Enforcement Operations
Criminal Division

700 Grant Street, Suite 4000
Pittsburgh, Pennsylvania 15219

Tel: (412) 894-7353
Fax: (412) 644-5870

E-Mail: Robert.Eberhardt@usdoj.gov

TABLE OF CONTENTS

Pages

SUMMARY OF ARGUMENT.. 1

ARGUMENT

I. THE FOURTH AMENDMENT DOES NOT BAR COMPELLED DISCLOSURE OF HISTORICAL CELL-SITE RECORDS PURSUANT TO A 2703(d) ORDER.. 2

A. Historical Cell-Site Records Are Created and Retained By Wireless Carriers in the Ordinary Course of Business, And Therefore Do Not Enjoy a Reasonable Expectation of Privacy. 2

B. Cell-Site Records Are Too Imprecise To Indicate That A Wireless Phone Is Within a Constitutionally Protected Private Area. 4

II. A COURT MAY NOT ARBITRARILY DEMAND THAT AN APPLICATION FOR A 2703(D) ORDER MAKE A SHOWING OF PROBABLE CAUSE. 10

A. Allowing a Magistrate Judge to Demand Probable Cause In a 2703(d) Application Ignores the Language and Structure of the Statute and Impairs Its Purpose.. 11

B. The Legislative History of Section 2703(d) Fatally Contradicts the Claims of Amici and the Opinion Below. 15

C. Amici's Misreading of the Statute Cannot be Saved By Resort to Principles of "Constitutional Avoidance". 18

CONCLUSION. 22

CERTIFICATE OF COMPLIANCE AND CERTIFICATE OF SERVICE

TABLE OF AUTHORITIES

Federal Cases **Pages**

Alabama v. Bozeman, 533 U.S. 146 (2001). 11

Clark v. Martinez, 543 U.S. 371 (2005). 18, 19, 20, 21

Duncan v. Walker, 533 U.S. 167 (2001).. 15

In re Application of the United States, 2008 WL 5082506 (E.D.N.Y. Nov. 26, 2008) "Garaufis E.D.N.Y. Opinion". 6, 20

In re Application of United States for an Order for Disclosure of Telecommunications Records, 405 F. Supp. 2d 435 (S.D.N.Y. 2005) . . . 5, 6

Katz v. United States, 389 U.S. 347 (1967). 3

King v. St. Vincent's Hosp., 502 U.S. 215 (1991). 13

London-Sire Records, Inc. v. Doe 1, 542 F. Supp. 2d. 153 (D. Mass. 2008).. 4

Miller-El v. Cockrell, 537 U.S. 322 (2003). 12

Sibron v. New York, 392 U.S. 40 (1968). 19, 21

Smith v. Maryland, 442 U.S. 735 (1979). 3

Tavarez v. Klingensmith, 372 F.3d 188 (3d Cir. 2004). 12, 13

United States v. Christie, 2009 WL 742720 (D.N.J. Mar. 18, 2009). 4

United States v. Hubbell, 530 U.S. 27 (2000).. 10

United States v. Karo, 468 U.S. 705 (1984). 4, 5, 8, 9

United States v. Knotts, 460 U.S. 276 (1983).. . . . . 4, 8

Warshak v. United States, 532 F.3d 521 (6th Cir. 2008).. 20

Whitman v. Am. Trucking Ass'n, 531 U.S. 457 (2001).. 13

Zadvydas v. Davis, 533 U.S. 678 (2001). 19

Federal Statutes **Pages**

8 U.S.C. § 1231(a). 19

18 U.S.C. § 2703. . . . . ***passim***

Other Authorities **Pages**

In re Alltel Corp., 22 FCC Rcd. 16432 (Aug. 30, 2007). 5

In re Sprint Nextel Corp., 22 FCC Rcd. 16414 (Aug. 30, 2007). 5

In re United States Cellular Corp., 22 FCC Rcd. 16424 (Aug. 30, 2007). . . 5

Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services, 1994: Joint Hearings on H.R. 4922 and S. 2375 Before the Subcomm. on Technology and the Law of the Senate Comm. on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary, 103d Cong., 2d Sess. 160-61 (1994).. 16

Network Wiretapping Capabilities, 1994: Hearings Before the Subcomm. on Telecommunications and Finance of the House Comm. on Energy & Commerce, 103d Cong., 2d Sess. 122-23 (1994). 17

SUMMARY OF ARGUMENT

At the outset, the Government commends amicus Electronic Frontier Foundation ("EFF") for acknowledging an essential legal error in the reasoning of the Opinion and Order below. Amicus EFF admits that historical cell-site information is "a record or other information pertaining to a subscriber," and that it therefore falls within the scope of section 2703, contrary to the ruling below. See Brief of Amici Curiae Electronic Frontier Foundation et al. ("EFF Mem.") at 1-2 & n.1.

Notwithstanding this concession, amici put forward two main arguments in an attempt to defend the lower court's ill-reasoned denial of the Government's Application. First, amici argue that disclosure of routine business records – historical cell-site information relating to a wireless customer's calls – violates the Fourth Amendment. In the alternative, amici suggest that a court may, consistent with the statute, deny a 2703(d) application and demand a showing of probable cause based upon hypothetical and speculative Fourth Amendment concerns that might arise in other circumstances. Neither set of claims survives examination, and the Court should therefore reverse the Opinion and Order below and remand with instructions to grant the Application.

ARGUMENT

I. THE FOURTH AMENDMENT DOES NOT BAR COMPELLED DISCLOSURE OF HISTORICAL CELL-SITE RECORDS PURSUANT TO A 2703(d) ORDER.

Amici argue at length that historical cell-site records enjoy Fourth Amendment protection. As explained below, these contentions are wholly without merit.

A. Historical Cell-Site Records Are Created and Retained By Wireless Carriers in the Ordinary Course of Business, And Therefore Do Not Enjoy a Reasonable Expectation of Privacy

Cellular telephone companies keep, in the regular course of their business, records of certain information associated with their customers' calls. Those records include cell-site information: the location of the antenna tower (and, where applicable, which of the tower's three "faces") carrying a given call at its beginning and end. Amici do not dispute that carriers do so routinely,[1] and indeed cannot dispute this fact: if the records in question were not routinely generated and retained, they would not now be available for the Government to obtain after the fact and amici would not object to disclosure of such non-existent records. The exemplar provided to the court below (App. 63) illustrates these records, which are the same class of records sought in the Application denied by the Opinion and Order below.

Amici attempt to avoid the inevitable legal consequence of these facts

---

[1] In its amicus brief below, EFF freely conceded these points. See Brief of Amici Curiae The Electronic Frontier Foundation et al. (Docket No. 28) at 6 ("Amici agree with the government that stored CSLI such as that at issue here ... is routinely generated and recorded by the cell phone service provider in the ordinary course of providing communications service to its customer") & 30 ("CSLI is ... generated by the provider itself as part of its provision of service. ... The provider decides what historical tower call records to keep.").

– specifically, that government compulsion of such routine business records implicates no Fourth Amendment interest – through obfuscation. For example, amicus EFF makes much of the fact that "a wireless provider [is not] a party to a user's cell phone communications." EFF Mem. at 19. In a similar vein, amicus Susan Freiwald remarks that "[a]s to true third parties [sic] intermediaries like cell phone providers, their mere access to their customers' data cannot defeat those customers' reasonable expectations of privacy in that data." Brief of Amicus Curiae Susan Freiwald ("Freiwald Mem.") at 16 (citing Katz v. United States, 389 U.S. 347 (1967)).

These arguments miss the mark for the simple reason that this appeal involves government access to **non-content records**, and not to the contents of communications. Thus, the "data" enjoying Fourth Amendment protection in Katz were the phone conversations themselves, not the non-content records associated with those calls. And amici fare no better in their attempts to avoid the consequences of the applicable Fourth Amendment precedents such as Smith v. Maryland, 442 U.S. 735 (1979) (finding no reasonable expectation of privacy in non-content telephone transaction records). Amicus EFF offers the observation that "the average cell phone user does not even know the location of the nearest cell phone tower or which tower their phone may be ... communicating through." EFF Mem. at 21. But this fact does nothing to alter the constitutionally unprotected status of a carrier's routine records about usage of its facilities; otherwise, a user who walks up to a bank of payphones and places a call – not knowing or caring about the number of the payphone he has fortuitously chosen – would have a reasonable expectation of privacy in the phone company's routine record of that call. No support for this outlandish

proposition exists in the vast body of Fourth Amendment case law.[2]

Nor is it relevant that cell-site location information does not appear in a typical cell phone customer's bill. Many telephone customers, especially those with landline service, have unlimited local or long distance calling plans, and accordingly do not receive a monthly bill detailing each call. (Likewise, it would be unusual for an Internet user to be billed for each and every email message he sends or receives.) Under the novel position advanced by amici, these routine non-content phone records would receive full Fourth Amendment protection, and a subpoena could not be used to compel their production. Amici can locate no authority supporting this extraordinary result, and this Court should accordingly reject it.

B. Cell-Site Records Are Too Imprecise To Indicate That A Wireless Phone Is Within a Constitutionally Protected Private Area

As discussed above, and in the Government's opening brief ("Gov't Mem.") at pages 26-28, the issues in this appeal are controlled by well-established precedent finding no Fourth Amendment privacy interest in routine non-content records retained by a service provider or other third party. Cases such as United States v. Knotts, 460 U.S. 276 (1983), and United States v. Karo, 468 U.S. 705 (1984) – involving **prospective** location-tracking by means of physical transmitters surreptitiously installed in private property by direct

---

[2] Similarly, Internet service providers routinely assign Internet Protocol addresses to their customers' computers in order to enable those customers to communicate over the network. See, e.g., London-Sire Records, Inc. v. Doe 1, 542 F. Supp. 2d. 153, 160 (D. Mass. 2008). But notwithstanding the typical end user's complete lack of awareness of which IP address he has been assigned, there is no Fourth Amendment expectation of privacy in an ISP's records of such assignments. See United States v. Christie, 2009 WL 742720, at *3 (D.N.J. Mar. 18, 2009).

Government action – are simply inapposite to Government requests for **historical** records generated independently by a telephone company.

However, even if this Court were to analyze the Application under these tracking device precedents, the result would be the same. As explained in detail previously, Gov't Mem. at 28-30, Karo holds squarely that the use of a tracking device constitutes a Fourth Amendment search only where it reveals the presence of an object within a **particular** private space. Because historical cell-site records are far too imprecise to do so, the Government's Application for an order to compel those records cannot in any event infringe a constitutional interest. As a result, this Court should grant the appeal and reverse the Opinion and Order.

Amici offer a half-hearted response to the showing that historical cell-site records are precise only to a range of hundreds of feet at best. Amicus EFF disingenuously insists that "there is no evidence before the Court" that cell-site records are so imprecise. See EFF Mem. at 12. It accomplishes this sleight-of-hand by dismissing multiple recent FCC reports[3] and entirely ignoring the other evidence properly before this Court, including but not limited to In re Application of United States for an Order for Disclosure of

[3] Those reports, cited at page 33 & n.18 of the Government's opening brief, date from 1999-2001. Contrary to EFF's assertion that this evidence is "woefully out-of-date," EFF Mem. at 22, the FCC has repeatedly reaffirmed these findings in recent years. See, e.g., In re Alltel Corp., 22 FCC Rcd. 16432, 16436 n.32 (Aug. 30, 2007) ("Phase I E911 service provides ... the location of the cell site or base station receiving the 911 call.... **Thus, the actual location of the caller can be miles distant from the location information provided** ....") (emphasis added); In re United States Cellular Corp., 22 FCC Rcd. 16424, 16428 n.31 (Aug. 30, 2007) (same); In re Sprint Nextel Corp., 22 FCC Rcd. 16414, 16418 n.34 (Aug. 30, 2007) (same).

Telecommunications Records, 405 F. Supp. 2d 435, 437 (S.D.N.Y. 2005) (describing that court's personal examination of a map of cellular towers in densely occupied lower Manhattan and finding them "several hundred feet apart" at their closest) and the exemplar included in the record on appeal (App. 63). EFF also conspicuously ignores a recent district decision, which expressly rejected arguments made by EFF as amicus, holding that "information identifying the one antenna tower (and portion of such tower receiving transmissions from the SUBJECT WIRELESS TELEPHONES at the beginning and end of calls made from those phones ... **is not precise enough to enable tracking of a telephone's movements within a home**." In re Application of the United States, 2008 WL 5082506, at *5 (E.D.N.Y. Nov. 26, 2008) ("Garaufis E.D.N.Y. Opinion") (emphasis added).

Unable to muster factual support for its position, EFF contends that the March 2008 testimony of FBI Special Agent William Shute[4] rebuts all of these authorities and proves that cell-site information is precise enough to intrude upon a constitutional interest. But the Shute transcript, instead of supporting this tendentious claim, only reinforces the Government's position.

First, Special Agent Shute confirms that the historical cell-site records – precisely the records sought by the Application at issue here – are the carrier's "normal business records." EFF Add. at 10.[5] Likewise, his testimony

---

[4]A transcript of Special Agent Shute's testimony appears in the proposed Addendum to EFF's brief ("EFF Add."). As of the filing date of the Government's reply brief, EFF's request for this document to be considered (Motion for Judicial Notice or in the Alternative for Leave to Augment the Record) is still pending.

[5]As EFF observes, the wireless carrier at issue in the Shute testimony is the same one whose records are the subject of the Government's current Application. See EFF Mem. at 15 n.10.

underscores the accuracy of the Government's description of these records and the workings of the underlying technology. Compare Gov't Mem. at 8 & nn.6-7 with EFF Add. at 8 (explaining cell-site sectors) and 12-13 (describing the elements of historical cell-site records).

Most importantly, Agent Shute scrupulously and repeatedly acknowledges that historical cell-site records by themselves provide only a rough indication of a user's location at the time a call in the past was made or received:

> In the essence of being fair in court purposes, I wanted to show [on the map used as a court exhibit] the greatest possible range of where that phone could be in that general area. [...]
>
> **I don't speculate where the person [**using the phone**] was**. I just show you where the cell site sectors are. [...]
>
> From my experience and utilization of this technology, [the records for several calls in sequence are] extremely consistent with the phone being **somewhere in the middle of the two cell site sectors**. [...]
>
> Q. Where was the phone?
> A. In the highlighted area. [...] It looks like somewhere between 1300 and 1400 Lehigh [Avenue]. [...]
>
> Q. Where is the phone?
> A. In the Northeast region, approximately three quarters of a mile from that tower.
> Q. Three quarters of a mile?
> A. In the area highlighted.
> Q. That's about eight blocks?
> A. Well, yes, it is, except for the fact that the phone also utilized [tower] 37884.
> Q. That tells us something. What's that?
> A. It tells us that it bounced back and forth from tower to tower.
> Q. Right.
> A. Therefore, the phone is actually in a very smaller [sic] area, in that overlapped area.
> Q. **But we don't know where?**
> A. **I could not tell you where.**

EFF Add. at 17, 20, 24, 27, & 27-28 (emphasis added).

EFF misrepresents Special Agent Shute's testimony as asserting that

cell-site information "is reliable evidence that a suspect is at his or her home." EFF Mem. at 15. In fact, the transcript does not go so far. At most, Agent Shute avers that it is "highly possible" that the user was at home, or that the user "was **in the vicinity** of her home." EFF Add. at 20 & 21 (emphasis added). For at least two reasons, neither statement supports EFF's claim that government access to such records invades a Fourth Amendment privacy interest.

First, the two controlling Supreme Court cases on tracking devices make clear that acquiring location information about an object in "the vicinity" of a home or other private space, but not within its interior, is not a "search." See Knotts, 460 U.S. at 278-79 (rejecting Fourth Amendment claim where "[t]he record before us does not reveal that the beeper was used after the location **in the area of the cabin** had been initially determined") (emphasis added); Karo, 468 U.S. 705 (holding that no "search" occurred where beeper revealed "only that the ether was somewhere in the [multi-unit storage] warehouse; **it did not identify the specific locker in which the ether was located**") (emphasis added); see also Gov't Mem. at 29-30 (discussing these cases).

Second, Agent Shute's speculation about the meaning of the historical cell-site records is plainly informed by his knowledge – in no way derived from the telephone records themselves – of the target's home address. The cell-site records are far too general, as the excerpted testimony above demonstrates, to pinpoint the phone within a specific residence; rather, the records indicate a general area, giving rise to the possibility – not a certainty, only a potential inference – that the phone was "in the vicinity" of the target's previously known residence.

In Karo, agents learned the precise location of the tracked can of ether

inside a specific storage locker only after subpoenaing the storage company for rental records; tracking the beeper to a specific row of lockers; and then using their sense of smell to detect the ether. See 468 U.S. at 708. When one of the targets moved the ether, a similar scenario played out again: agents traced the beeper to another self-storage facility, and then – using their noses – located the smell of ether coming from a given locker. Id. at 709.

As Karo itself makes explicit, the agents in that case were free to use the tracking device to track the beeper to a general area (the storage facility), and then to use a subpoena and their sense of smell to infer the precise location of the can of ether, all without conducting a "search." For the same reasons, law enforcement may obtain historical cell-site records – which do not by themselves disclose the presence of a phone or person within private space – and, by comparing them to other information (such as that derived from visual surveillance or other sources), draw additional conclusions.

Under the contrary rule urged by amici, government agents violate the Fourth Amendment when they use such powers of deduction. If the government subpoenas historical records showing landline telephone calls made from the home of criminal suspect Bob, who is known to live alone, it may infer that Bob was in his house at the time of those calls. Amici EFF and Freiwald would call this a constitutional violation absent a warrant based upon probable cause. Because the position of amici produces such absurd results, results that cannot be squared with decades of Fourth Amendment jurisprudence, this Court should reverse the Opinion and Order denying the Government's Application and remand to the district court with instructions to grant the Application.

II. A COURT MAY NOT ARBITRARILY DEMAND THAT AN APPLICATION FOR A 2703(D) ORDER MAKE A SHOWING OF PROBABLE CAUSE.

Recognizing the weakness of their constitutional arguments (and of the analysis in the Opinion and Order), amici contend in the alternative that section 2703(d) allows a magistrate judge to demand a showing of probable cause.

It is crucial to understand the breadth of this argument: Amici do not merely argue that a magistrate judge may deny a 2703(d) application where the requested order would infringe a clear constitutional right.[6] Instead, the argument, stripped to its essentials, is that a magistrate judge may, **even in the absence of a constitutional violation**, decide on a whim to reject a 2703(d) application even when it satisfies the statutory standard of "specific and articulable facts."

Amici creatively sugar-coat this extraordinary assertion by claiming that "Congress ... provided to courts a statutory safety-valve to ensure that privacy could always be adequately protected despite advances in technology [and] future-proofed the statute by permitting magistrates in their discretion to deny a D order application and instead require a probable cause showing." EFF Mem. at 8. Because that claim has no support in the text or legislative history of section 2703(d), this Court should reject it.

---

[6] Although the government does not believe that section 2703(d) could be misused in this manner, and (as set out above) emphatically rejects the suggestion that the instant Application does so, we think it obvious that a court need not issue or enforce compulsory process that violates a constitutional right. By analogy, a court could – indeed, would be obligated to – refuse to enforce a subpoena that would violate the Fifth Amendment privilege against self-incrimination. See United States v. Hubbell, 530 U.S. 27, 43-46 (2000).

A. Allowing a Magistrate Judge to Demand Probable Cause In a 2703(d) Application Ignores the Language and Structure of the Statute and Impairs Its Purpose

Because no other cases adopt its reading of the statute, amicus EFF attempts to bolster the decision below by placing enormous weight on the phrase "only if" in 2703(d). See EFF Mem. at 3-7 (arguing that a showing of "specific and articulable facts" is a necessary, but not sufficient, condition). For multiple reasons, this selective interpretation is not sustainable.

First, the statute includes two phrases which control when a court should issue a 2703(d) order. Such an order "**may** be issued by any court that is a court of competent jurisdiction," but such an order "**shall issue** only if the government entity offers specific and articulable facts showing that there are reasonable grounds to believe that the [records sought] are relevant and material to an ongoing criminal investigation" (emphasis added). As the Supreme Court has stated, "[t]he word 'shall' is ordinarily the 'language of command.'" Alabama v. Bozeman, 533 U.S. 146, 153 (2001). A court is therefore obligated to issue a 2703(d) order when the government satisfies the "specific and articulable facts" standard.

As used in 2703(d), the word "only" prevents a court from issuing 2703(d) orders when the government does not meet the "specific and articulable facts" threshold. Consider how the statute would read if the word "only" were omitted: "[A 2703(d) order] may be issued by any court that is a court of competent jurisdiction and shall issue if the government entity offers specific and articulable facts . . . ." Under this phrasing, a court would be required to issue 2703(d) orders when the government meets the "specific and articulable facts" showing, but would also have discretion to issue 2703(d) orders even when the government failed to make such a showing. The word

"only" eliminates this discretion and makes the "specific and articulable facts" standard mandatory. It does not give a court discretion to reject an application, such as the one in this case, that meets the"specific and articulable facts" standard.

Moreover, the district court and EFF's interpretation of 2703(d) renders the phrase "and shall issue" in 2703(d) superfluous. That is, they read the statute as if it were written: "[A 2703(d) order] may be issued by any court that is a court of competent jurisdiction if the government entity offers specific and articulable facts . . . ." Indeed, the primary authority relied upon by the district court and EFF, Miller-El v. Cockrell, 537 U.S. 322, 349 (2003),[7] interpreted a statute which used this precise "may issue . . . only if" formulation. But that is not how section 2703(d) is written: section 2703(d) includes "shall issue," the language of command. The interpretation of the district court and EFF should be rejected because it renders this critical language superfluous.

The reasoning of the Opinion and Order (and of amicus EFF) suffers from a second fatal defect. As this Court's precedents make clear, a selective reading of one portion of the statute, isolated from and incompatible with the surrounding provisions, cannot be correct.

Most obviously, in Tavarez v. Klingensmith, 372 F.3d 188 (3d Cir. 2004) – cited in the Government's opening brief (Gov't Mem. at 24), and even by EFF itself (EFF Mem. at 5) – this Court rejected a similarly strained statutory parsing. In that case, this Court was asked to decide whether an

---

[7] Both the Opinion and Order below (App. 43, n. 56) and Amicus (EFF Mem. at 4) fail to note that the passage on which they rely appears in Justice Scalia's concurrence, and not in the opinion of the Miller-El majority.

employee was entitled to sue his immediate supervisor under a worker's compensation statute stating that "an injured employee may sue any person responsible for his injuries other than the employer named in a [statutorily prescribed] certificate of insurance." 372 F.3d at 191. The panel conceded that "[a]t first blush, the apparent breadth of the term 'any person,' combined with the fact that [the supervisor] was not personally named in the certificate of insurance, appears to give [this] argument some support." Id.

However, this Court did not conclude its analysis with this simplistic reading. Rather, the Court undertook an "examination of the statutory scheme ... as a whole," id., concluding instead that allowing the suit would frustrate the broader purposes of the larger statutory framework. In doing so, the panel met its obligation to "look to the surrounding words and provisions and their context." Id. at 190 (citing Whitman v. Am. Trucking Ass'n, 531 U.S. 457 (2001)); see also King v. St. Vincent's Hosp., 502 U.S. 215, 221 (1991) (applying "cardinal rule that a statute is to be read as a whole ... since the meaning of statutory language, plain or not, depends on context")).

Viewed from this broader perspective, the facile reading of section 2703 put forward by Amicus EFF (and in the Opinion and Order below) does not survive scrutiny. As explained concisely in the Government's opening brief (at 24), in 1986 Congress clearly laid out three separate and distinct mechanisms in 18 U.S.C. § 2703 by which the Government could compel a service provider to turn over a customer's stored non-content records:

- a subpoena;
- a warrant based on probable cause; or
- a court order under 2703(d).

See H. Rep. No. 647, 99th Cong, 2d Sess. 69 (1986). But under the reading urged by amici, a magistrate judge may, for any reason or no reason at all, arbitrarily deny an application under 2703(d) and instead insist upon a warrant. As in Tavarez, such a reading ignores the overall structure of the statute and undercuts one explicit purpose of the framework crafted by Congress – here, to allow the Government to obtain non-content customer records without having to show probable cause.

Amicus EFF labors to invert this analysis, asserting that the Government's position makes section 2703(c)(1)(A) (use of a warrant to compel non-content records) superfluous because "there would never be any reason for the government to seek a warrant under that provision if it could in every case instead obtain a D Order under section 2703(d)'s more lenient standard." EFF Mem. at 7. Amicus is wrong. Section 2703(c)(1)(A) is alive and well for the simple reason that federal prosecutors use it in a frequently recurring scenario: where they seek to compel both stored communications content under § 2703(a) (generally requiring a warrant) and non-content records pertaining to a single customer. In that common situation, the prosecutor is able – at his or her option – to employ a single form of compulsory process (a warrant), rather than issuing a warrant for content and a separate subpoena or court order for the associated non-content records.

Finally, EFF's argument collapses under its own weight. If the phrase "only if" in § 2703(d) gives a magistrate judge carte blanche to demand more than "specific and articulable facts," he or she need not stop at probable cause. Under the reading urged by amici, which lacks any limiting principle, a magistrate could arbitrarily demand proof by a preponderance of the evidence,

clear and convincing evidence, or even beyond a reasonable doubt, given that § 2703(c) requires disclosure of customer non-content records "only when" the government uses a warrant. Such an interpretation does not give effect to every provision of the statute, as required. See Duncan v. Walker, 533 U.S. 167, 174 (2001). On the contrary, it substitutes a magistrate judge's personal predilections for the intricate framework duly enacted by Congress. Because the lower court was not free to rewrite the statute to suit its own notions of sound policy, this Court should reject these arguments and reverse the lower court's unprecedented reading of the statute.

B. The Legislative History of Section 2703(d) Fatally Contradicts the Claims of Amici and the Opinion Below

As noted above, amicus EFF alleges that Congress "future-proofed the statute by permitting magistrates in their discretion to deny a D order application and instead require a probable cause showing." EFF Mem. at 8. In reality, the legislative history of the crucial amendment to section 2703 in 1994[8] contains no reference to any such Congressional intent. Even more remarkably, **EFF itself made no such suggestion at the time**, even though it led the effort to establish the "specific and articulable facts" standard currently set forth in the statute.

According to EFF Executive Director Jerry Berman, appearing on August 11, 1994 before a joint House-Senate Judiciary Committee hearing on the pending legislation,

> the bill contains a number of significant privacy advances, including enhanced protection for the detailed transactional information records generated by on line [sic] information

[8] See Gov't Mem. at 24-25.

> services, email systems, and the Internet.
>
> *1. Expanded protection for transactional records sought by law enforcement*
>
> **Chief among these new protections is an enhanced protection for transactional records from indiscriminate law enforcement access.** ... Provisions in the bill recognize that this transactional information created by new digital communications systems is extremely sensitive and deserves a high degree of protection from casual law enforcement access which is currently possible without any independent judicial supervision. ...
>
> **In order to gain access to transactional records ... law enforcement will have to prove to a court, by the showing of "specific and articulable facts" that the records requested are relevant to an ongoing criminal investigation.** This means that the government may not request volumes of transactional records merely to see what it can find through traffic analysis. Rather, **law enforcement will have to prove to a court that it has reason to believe that it will find specific information relevant to an ongoing criminal investigation in the records it requested**. ...
>
> Court order protection will make it much more difficult for law enforcement to go on "fishing expeditions" through online transactional records, hoping to find evidence of a crime by accident. ...
>
> The most important change that these new provisions offer is that law enforcement will: (a) have to convince a judge that there is reason to look at a particular set of records, and; (b) have to expend the time and energy necessary to have a United States Attorney or District Attorney actually present a case before a court.

Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services, 1994: Joint Hearings on H.R. 4922 and S. 2375 Before the Subcomm. on Technology and the Law of the Senate Comm. on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary, 103d Cong., 2d Sess. 160-61

(1994) ("Joint CALEA Hearings") (prepared statement of Jerry J. Berman, Executive Director, Electronic Frontier Foundation) (emphasis added).[9]

One month later, EFF offered identical reassurances to a separate House subcommittee. See Network Wiretapping Capabilities, 1994: Hearings Before the Subcomm. on Telecommunications and Finance of the House Comm. on Energy & Commerce, 103d Cong., 2d Sess. 122-23 (1994) ("House CALEA Hearings") (prepared statement of Jerry J. Berman, Policy Director, Electronic Frontier Foundation).[10] And after Congress passed the legislation and transmitted it for the President's signature, EFF once again hailed the new 2703(d) standard's robust protection against "indiscriminate access" and "fishing expeditions" by law enforcement. See EFF Statement on and Analysis of Digital Telephony Act (Oct. 8, 1994).[11]

Moreover, in all three of the documents cited immediately above, EFF's Jerry Berman explicitly represented that "the burden or [sic] proof to be met by the government in such a proceeding [i.e., a 2703(d) application] is lower than required for access to the content of a communication [i.e., probable cause under 2703(a)]." Joint CALEA Hearings at 161; see also House CALEA

---

[9] The full record of the joint hearing is available online at http://www.lexisnexis.com/congcomp/getdoc?HEARING-ID= HRG-1994-SJS-0015.

[10] A version of Berman's statement (with minor typographical corrections) is available at http://w2.eff.org/Privacy/Surveillance/CALEA/eff_091394_digtel_ berman.testimony . The full record of the House hearing is available online at http://www.lexisnexis.com/congcomp/getdoc?HEARING-ID=HRG-1994-HEC-0049.

[11] A copy of the EFF statement is available at http://w2.eff.org/Privacy/Surveillance/CALEA/digtel94_passage_statement.eff .

Hearings at 123 (verbatim); EFF Statement on and Analysis of Digital Telephony Act (verbatim). In short, in its efforts to persuade Congress to raise the 2703(d) standard to its current level – "specific and articulable facts" – EFF publicly and repeatedly acknowledged that 2703(d) applications would not require probable cause.

It is profoundly telling that none of these statements – and indeed, nothing anywhere in the legislative history of the 1994 amendment – furnishes even a scintilla of support for EFF's extravagant claim that Congress "future-proofed" the statute to allow a magistrate to impose a probable cause requirement arbitrarily.[12]

C. Amici's Misreading of the Statute Cannot be Saved By Resort to Principles of "Constitutional Avoidance"

Finally, amicus EFF contends that this Court should adopt the novel and unnatural construction of section 2703 discussed above under the doctrine of constitutional avoidance. In particular, EFF pins its analysis on a remark in Clark v. Martinez, 543 U.S. 371, 380-81 (2005), that a court should interpret a statute so as to avoid constitutional problems "whether or not those constitutional problems pertain to the particular litigant before the Court." EFF Mem. at 11. For several reasons, this Court should soundly reject that suggestion.

---

[12] These same passages also underscore the absurdity and hypocrisy of EFF's current claim that the Government's reading of section 2703(d) – requiring "specific and articulable facts" – raises "the specter of 'dragnet surveillance' without warrants." EFF Mem. at 13 n.8.

First, the passage on which EFF relies is pure dicta. Clark involved the application of a statute[13] previously construed by the Court in Zadvydas v. Davis, 533 U.S. 678 (2001). In Zadvydas, a removable alien challenged the government's authority to detain him indefinitely; noting the absence of any time restriction in the statute, the Court construed the statute to contain an implicit "reasonable time" limitation in order to avoid "serious constitutional concerns." 533 U.S. at 682. Four years later in Clark, an alien removable on slightly different grounds argued that this same statute – and therefore the implicit time limitation on detention imposed in Zadvydas – applied to him as well and entitled him to release.

Thus, neither Clark nor Zadvydas involved construing a statute to avoid a potential constitutional problem not before the Court. On the contrary, each case involved an alien who claimed that **his own** detention presented a concrete instance of a constitutional violation. (Further, Clark does not rest on constitutional avoidance at all, but rather on the principle that having already construed the statute one way in Zadvydas, the Court had no textual or other basis for construing it differently in Clark.) In neither case did the Court adopt a saving construction of the statute to avoid hypothetical concerns that might arise in a different case, and Justice Scalia's aside on that question in Clark is a textbook example of dicta unnecessary to the decision.

Second, the Supreme Court has made clear that Fourth Amendment challenges are "pre-eminently the sort of question which can only be decided in the concrete factual context of the individual case." Sibron v. New York, 392 U.S. 40, 59 (1968). Indeed, the Sibron Court explicitly rejected the

[13] 8 U.S.C. § 1231(a)(6).

suggestion that it consider speculative, hypothetical concerns about a statute's validity: "[w]e decline ... to be drawn into what we view as the abstract and unproductive exercise of laying the extraordinarily elastic categories of [the statute] next to the categories of the Fourth Amendment in an effort to determine whether the two are in some sense compatible." Id.

Only last year, the Sixth Circuit (sitting en banc) adopted this same approach in rejecting a request for a nationwide injunction against the use of section 2703(d) to compel the contents of stored email. As that court observed,

> [c]oncerns about the premature resolution of legal disputes have particular resonance in the context of Fourth Amendment disputes. In determining the "reasonableness" of searches under the Fourth Amendment and the legitimacy of citizens' expectations of privacy, courts typically look at the "totality of the circumstances," ... reaching case-by-case determinations that turn on the concrete, not the general, and offering incremental, not sweeping, pronouncements of law.... [A] reviewing court looks at the claim in the context of an actual, not a hypothetical, search and in the context of a developed factual record of the reasons for and the nature of the search. A pre-enforcement challenge to future ... searches, by contrast, provides no such factual context. **The Fourth Amendment is designed to account for an unpredictable and limitless range of factual circumstances, and accordingly it generally should be applied after those circumstances unfold, not before.**

Warshak v. United States, 532 F.3d 521, 528 (6th Cir. 2008) (en banc; emphasis added).

Another court, also ruling last year, expressly rebuffed the efforts of amicus EFF to invoke Clark v. Martinez to bar government access to cell-site location information. See Garaufis E.D.N.Y. Opinion, 2008 WL 5082506 (E.D.N.Y. Nov. 26, 2008). In that decision, reversing a magistrate judge's denial of an order under section 2703(d) for prospective cell-site location information, the court noted that

> the "serious doubts" EFF is concerned about arise not in the present case, but in a hypothetical future case in which the Government might ... request far more detailed tracking information that would allow precise tracking of a target inside his or her home ... The specter of such precise location tracking does not loom over this case, because the Government is seeking only information identifying the one antenna tower (and portion of such tower) receiving transmissions from the SUBJECT WIRELESS TELEPHONES at the beginning and end of calls made by those phones. ... EFF argues, however, that this court should take into account in this case the possibility that in future cases the [government's] theory could be used to justify the disclosure of more precise tracking information.

Id. at *5. Citing Sibron, the district court held explicitly that "Clark v. Martinez is inapposite" to analysis of the constitutionality of 2703(d) orders for cell-site location information. Id. at *6-7.

Thus, this Court should not adopt the suggestion of amicus EFF to speculate idly about hypothetical future technologies. Rather, the Court should focus its analysis on the particular Application, for a particular class of records, at issue in this proceeding. As explained in the Government's opening brief (in part II), and as discussed in part I above, the disclosure of the records requested in the instant Application implicates **no** Fourth Amendment privacy interest, let alone the "multitude of constitutional problems," 543 U.S. at 380-81, necessary to trigger the Clark v. Martinez avoidance doctrine. For all these reasons, this Court should reverse the lower court's Opinion and Order.

CONCLUSION

For the foregoing reasons, the order of the district court denying the Application should be reversed and this case remanded with instructions to grant the Application.

Respectfully submitted,

MARY BETH BUCHANAN
United States Attorney

/s/Robert L. Eberhardt
Robert L. Eberhardt
Assistant United States Attorney

Mark Eckenwiler
Associate Director
United States Department of Justice
Office of Enforcement Operations
Criminal Division

CERTIFICATE OF COMPLIANCE

1. This reply brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains ***6,073*** words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

2. This reply brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because

this brief has been prepared in a proportional typeface using WordPerfect 12 in Times New Roman 14 point font.

3. The text of this e-brief and hard copies of the brief are identical.

4. A virus check was performed on both this e-brief with Trend Micro OfficeScan Version 6.5.

/s/Robert L. Eberhardt
Robert L. Eberhardt
Assistant U.S. Attorney

CERTIFICATE OF SERVICE

I hereby certify that the following are filing users and will be served electronically by the Notice of Docketing Activity. Two copies of this brief were also sent by First Class Mail to:

Witold J. Walczak, Esq.
Email: vwalczak@aclupa.org
American Civil Liberties Union
313 Atwood Street
Pittsburgh, PA 15213-0000

Lisa B. Freeland, Esq.
Email: Lisa_Freeland@fd.org
Federal Public Defender
1450 Liberty Center
1001 Liberty Avenue
Pittsburgh, PA 15222

Susan Freiwald
Professor of Law
USF School of Law
2130 Fulton Street
San Francisco, CA 94117

/s/Robert L. Eberhardt
Robert L. Eberhardt
Assistant U.S. Attorney

Dated: April 16, 2009