
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 U.S. District Court for the Western District of Pennsylvania (McVerry, J.) at Magistrate No. 07-524M

OPPOSITION OF AMICI CURIAE ELECTRONIC FRONTIER FOUNDATION ET AL. TO PETITION FOR REHEARING EN BANC

Respectfully submitted,

Kevin S. Bankston
Matthew Zimmerman
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333
bankston@eff.org
mattz@eff.org

Attorneys for *Amici Curiae*

On the brief:

Witold J. Walczak
ACLU of Pennsylvania
313 Atwood Street
Pittsburgh, PA 15213
412-681-7864
vwalczak@aclupgh.org

Catherine Crump
American Civil Liberties Union Found.
125 Broad Street, 18th Floor
New York, NY 10004
212-519-7806
ccrump@aclu.org

James X. Dempsey
Center for Democracy & Technology
1634 I Street NW, Suite 1100
Washington, DC 20006
202-637-9800
jdempsey@cdt.org

DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER ENTITIES WITH A DIRECT FINANCIAL INTEREST IN LITIGATION

Pursuant to Federal Rule of Appellate Procedure 26.1, *Amici* Electronic Frontier Foundation ("EFF"), ACLU-Foundation of Pennsylvania, Inc. ("ACLU of Pennsylvania"), American Civil Liberties Union, and Center for Democracy & Technology ("CDT"), non-profit corporations, make the following disclosure:

1. No *Amicus* is a publicly held corporation or other publicly held entity.

2. *Amici* have no parent corporations.

3. No publicly held corporation or other publicly held entity owns 10% or more of any *Amicus*.

4. No *Amicus* is a trade association.

DATED: November 29, 2010

By /s/ Kevin S. Bankston

Kevin S. Bankston
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333
bankston@eff.org

Attorneys for *Amici Curiae*

STATEMENT OF AMICI CURIAE

Amici are non-profit public interest organizations seeking to ensure the preservation of Fourth Amendment and statutory privacy protections in the face of advancing technology. This *amicus* brief is submitted at the request and by the order of this Court, under its Briefing Order dated November 1, 2010.

The Electronic Frontier Foundation ("EFF") is a non-profit, member-supported civil liberties organization working to protect free speech and privacy rights in the online world. As part of that mission, EFF has served as counsel or *amicus* in key cases addressing electronic privacy statutes and the Fourth Amendment as applied to the Internet and other new technologies. With more than 13,000 dues-paying members, EFF represents the interests of technology users in both court cases and in broader policy debates surrounding the application of law in the digital age, and publishes a comprehensive archive of digital civil liberties information at www.eff.org.

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization with over 500,000 members dedicated to the principles of liberty and equality embodied in the U.S. Constitution. The protection of privacy as guaranteed by the Fourth Amendment is an area of special concern to the ACLU. In this connection, the ACLU has been at the forefront of numerous state and federal cases addressing the right of privacy in Internet communications.

The ACLU-Foundation of Pennsylvania, Inc. ("ACLU of Pennsylvania") is a non-profit organization with about 19,000 members in Pennsylvania. The organization is devoted to the preservation and advancement of civil liberties for all Pennsylvanians through public

education, legislative advocacy and litigation. The ACLU of Pennsylvania regularly appears in this Court and the Third Circuit as either direct counsel or amicus to serve those ends. Because of its particular commitment to rights of privacy and due process, the ACLU of Pennsylvania has a special interest in, and expertise to address, the application of the law in this case.

The Center for Democracy & Technology ("CDT") is a non-profit public interest organization focused on privacy and other civil liberties issues affecting the Internet and other communications networks. CDT represents the public's interest in an open, decentralized Internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty.

STATEMENT OF CASE AND SUMMARY OF ARGUMENT

Amici respectfully urge this Court to reject the Government's application for rehearing *en banc* of the precedential opinion issued in this appeal on September 7, 2010. Rehearing *en banc* "is not favored," 3d Cir. L.A.R. 35.4 (2010), and is only proper where rehearing is "necessary to secure and maintain uniformity of the court's decisions" or where "the proceeding involves one or more questions of exceptional importance." Fed. R. App. P. 35(b)(1). Neither condition is met here.

The question of purportedly exceptional importance offered by the Government—"whether an order under 18 U.S.C. § 2703(d) must issue when the Government makes a factual showing meeting the standard set forth in that provision," Gov. Br. 1—does not warrant *en banc* review. The panel in this case unanimously answered that question in the negative based on the plain language, structure and history of the statute, consistent with Third Circuit and Supreme Court precedent. Such a straightforward case of statutory construction is not of sufficient importance to merit *en banc* review, particularly where the Government cannot point to a single court opinion that conflicts with the panel's statutory analysis. *See* Fed. R. App. P. 35(b)(1) (a panel decision poses a question of exceptional importance if it conflicts with those of other Courts of Appeals). The Government's unsubstantiated fear that magistrates will arbitrarily modify the showing required of the Government "on a whim" also does not create a question of exceptional importance, considering that judges are barred from abusing their discretion and that the statute in combination with the Federal Rules of Criminal Procedure requires magistrates to issue a search warrant when the Government has shown probable cause. The fact that the panel opinion may

impact law enforcement practice in some cases does not transform the issue into one of exceptional importance, or else practically every decision the Government disagrees with would merit *en banc* review and no panel decision restricting law enforcement's authority would ever be final.

Nor is *en banc* review "necessary to secure and maintain uniformity of the court's decisions," since the purported conflict between the panel decision and a following opinion, *U.S. v. Christie*, ___ F.3d ___, 2010 WL 4026817 (3d Cir. Sept. 15, 2010), does not exist. The *Christie* court held only that an Internet Protocol (IP) address assigned by an Internet service provider is not protected by the Fourth Amendment. *See Christie*, slip op. 29-30. The panel majority here found that a completely different kind of data, cell site location information (CSLI) held by a cell phone service provider, may be protected by the Fourth Amendment depending on the particular facts. These narrow holdings, both citing the same Supreme Court decision but applying it differently to different types of records, do not conflict. Particularly in light of the Supreme Court's recent admonition that courts should avoid unnecessary rulings on how the Fourth Amendment applies to new technologies, *see City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2629, 177 L. Ed. 2d 216 (2010), this Court should decline the Government's invitation to establish a broad Fourth Amendment rule for all "non-content networking information," a term that appears in neither opinion.

ARGUMENT

I. 18 U.S.C. § 2703(d) Plainly Vests Magistrate Judges With Discretion to Deny Government Applications for Orders Under That Section.

"[E]very exercise of statutory interpretation begins with an examination of the plain language of the statute," and where statutory language is "plain and unambiguous," no further inquiry is necessary. *Rosenberg v. XM Ventures,* 274 F.3d 137, 141 (3d Cir. 2001). Reading the plain language of 18 U.S.C. § 2703(d) in a manner consistent with Third Circuit and Supreme Court precedents, the panel was correct to conclude that the statute grants courts the discretion to deny Government applications for orders under that section. Section 2703(d) reads:

> A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue *only if* the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

18 U.S.C. § 2703(d) (emphasis added). As the panel unanimously held, Congress' instruction that the court shall issue an order "only if" the Government makes the requisite showing also grants the court discretion to deny a Government application even when that showing has been made. Slip op. 21-24, 28; *see also id*. at 30-31 (Judge Tashima agreeing in concurrence that statute provides discretion, though disagreeing on the scope of that discretion).

This straightforward holding—that the "only if" in section 2703(d) states a necessary but not sufficient condition for the issuance of a Section 2703(d) order—isn't at all "unprecedented" as the Government claims. Gov. Br. 5. The Government ignores a directly on-point opinion, issued by this

very Circuit just last year, on which the panel explicitly relied. *See* slip op. 22-23, *citing Township of Tinicum v. U.S. Dept. of Transp.*, 582 F.3d 482, 488 (3d Cir. 2009) ("The phrase 'only if' describes a necessary condition, not a sufficient condition."). That decision follows the Supreme Court's consistent reading of the same phrase. *See, e.g., California v. Hodari D.*, 499 U.S. 621, 628 (1991) ("'only if' . . . states a *necessary*, but not a *sufficient*, condition….") (emphasis in original); *accord Miller-El v. Cockrell*, 537 U.S. 322, 349 (2003).

By choosing the phrase "only if" rather than simply "if" in section 2703(d), Congress made clear that a court may issue but is not required to issue a Section 2703(d) order when the Government has made a specific and articulable facts showing. Section 2703(d)'s plain meaning is made all the clearer by comparison to Section 3123's mandatory language where there is no "only" and the court simply "shall issue [an order for pen register surveillance] if" the Government makes the required certification. *See* 18 U.S.C. § 3123(a)(1). As the panel correctly noted, reading Section 2703(d)'s "shall" as a command rather than a permission would render "only" surplusage: "[T]he difference between 'shall…if'… and 'shall…*only* if'… is dispositive…. The difficulty with the Government's argument is that the statute does contain the world 'only' and neither we nor the Government is free to rewrite it." Slip op. 22, 24 (emphasis added).

That Congress chose to use the phrase "shall issue" rather than the more obviously permissive "may issue" does not change the discretionary nature of the provision. Although the Government claims without qualification that "shall" is "the nondiscretionary language of command," Gov. Br. 5, the Supreme Court has long recognized that Congress often uses "shall" as a synonym for "may": "[S]hall" and "may" are frequently treated

as synonyms and their meaning depends on context…. [C]ourts in virtually every English-speaking jurisdiction have held-by necessity-that shall means may in some contexts, and vice versa." *Gutierrez de Martinez v. Lamagno*, 515 U.S. 417, 432 n.9 (1995) (internal citations and quotations omitted) (reading "shall" as "may"); *see also Hecht Co. v. Bowles*, 321 U.S. 321, 329 (1944) (same). Read in context as the Supreme Court has instructed, the "shall' in Section 2703(d)—when paired with the clearly permissive phrase "only if"—must itself be permissive. Indeed, it can be read in no other way without reading "only" out of the statute.[1]

Equally unpersuasive is the Government's claim that the panel's reading of Section 2703(d), extended to Section 2703(c)'s language regarding search warrants, would allow courts to deny applications for warrants even when supported by probable cause. Gov. Br. 6-7. The relevant language of 2703(c)(1) does not speak to the standard for court action at all. Instead, it dictates what authorization the *Government* must obtain before requiring disclosure of information under the statute. *See* 18 U.S.C. 2703(c)(1) ("A *governmental entity* may require [disclosure] only when….")

[1] The Government ignores the history of the statute when it claims that Congress' use of "may" elsewhere in Section 2703(d) requires an opposite conclusion. Gov. Br. 5. The portion of Section 2703(d) that clarifies which courts have authority to issue orders under that section—in particular, the phrase "may be issued by any court that is a court of competent jurisdiction and"—did not exist in the original statute but rather was added in 1994. *Compare* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat 1848, Title II, § 201 (establishing Section 2703) *and* Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat 4279, Title II, § 207(a)(2) (amending Section 2703(d) to add clause regarding jurisdiction); *see also* USA PATRIOT Act of 2001, Pub.L. 107-56, 115 Stat 272, Title II, § 220(b) (striking "described in section 3127(2)(A)" after "court of competent jurisdiction"). The "may be issued" language that the Government argues makes surplusage of the panel's reading of "shall" was added later, and the different clauses were clearly intended to serve different functions. Because one specifies which courts have jurisdiction to issue Section 2703(d) orders and the other defines the necessary though not necessarily sufficient condition for issuance of such an order, neither is surplus to the other.

(emphasis added). To the extent the Government exercises its option to seek a warrant under the Federal Rules of Criminal Procedure pursuant to Section 2703(c)(1)(A), those Rules make perfectly clear the limits of the court's discretion: "After receiving an affidavit or other information, a magistrate judge…*must* issue the warrant if there is probable cause…." Fed. R. Crim. P. 41(d)(1) (emphasis added).

The Government's purported fear that courts will misuse their discretion to require whatever showing suits their fancy—even above and beyond probable cause—is therefore unfounded. The court has the discretion only to grant or deny the Government's application for a Section 2703(d) order based on a specific and articulable facts showing; nothing in the statute or the panel opinion grants courts permission to fashion an alternative standard for such an order. If the court denies a Section 2703(d) application and the Government then seeks a warrant under Section 2702(c)(1)(A), that warrant must issue if the Government demonstrates probable cause.

This "sliding scale" structure, whereby the court may at its discretion require the Government to obtain a warrant by denying its application under Section 2703(d), does not make the Government's 2702(c)(1)(A) warrant option superfluous, as the Government argues, but instead plainly relies on it and gives it purpose. Slip op. 23-24. The Government's contrary argument—that Congress provided the warrant option "so that the Government may proceed on one paper rather than two" when it seeks both information for which the statute requires a warrant and information that requires a Section 2703(d) order—is simply implausible, as the panel correctly held. *Id*. The Government has failed to demonstrate that attaching Section 2703(d) applications to warrant applications supported by probable cause would impose any meaningful burden beyond a slight change in paperwork, much

less a burden that Congress intended to alleviate. Nor does the panel's reading disrupt the statute's basic distinction between warrants based on probable cause and Section 2703(d) orders based on specific and articulable facts, as the Government warns. Gov. Br. 5-6. Rather, it merely clarifies the court's discretion to issue them.

The most plausible explanation for the "sliding scale" construction of 2703 is that Congress recognized that some records that would otherwise be available to the Government under Section 2703(d) may be protected by the Fourth Amendment. As the Senate Judiciary Committee's report on the Electronic Communications Privacy Act explained:

> With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information. . . . For the person or business whose records are involved, the privacy or proprietary interest in that information should not change. Nevertheless, because it is subject to control by a third party computer operator, the information *may* be subject to no constitutional privacy protection.

S. Rep. No. 99-541 at 3 (1986) (emphasis added); *see also, e.g.,* S. Hrg. 98-1266 at 17 (1984) ("In this rapidly developing area of communications which range from cellular non-wire telephone connections to microwave-fed computer terminals, distinctions such as [whether a participant to an electronic communication can claim a reasonable expectation of privacy] *are not always clear or obvious*.") (emphasis added). It makes perfect sense that Congress would provide a constitutional safety-valve for judges considering Government applications under Section 2703(d), future-proofing the statute by allowing courts the discretion to deny such applications in order to avoid potential constitutional violations or unnecessary constitutional rulings.

Reading the statute to allow courts to avoid serious constitutional questions—by giving them the discretion to require warrants in questionable

cases—is not only consistent with but is *required* by the doctrine of constitutional avoidance. The constitutional avoidance doctrine "rest[s] on the reasonable presumption that Congress did not intend" any meaning of a statute "which raises serious constitutional doubts," *Clark v. Martinez*, 543 U.S. 371, 381 (2005), and "[i]t is therefore incumbent upon [the Court] to read the statute to eliminate those doubts so long as such a reading is not plainly contrary to the intent of Congress." *United States v. X-Citement Videos, Inc.*, 513 U.S. 64, 78 (1994); *see also Clark*, 543 U.S. at 384 (courts must adopt any "plausible" construction that would avoid a serious constitutional concern).

By contrast, the Government's inflexible, non-discretionary reading of the statute would force magistrates—and ultimately, this Court—to directly confront whether information sought by the Government via Section 2703(d) is protected by the Fourth Amendment, and consequently to directly confront the constitutionality of the statute. The Government's approach is particularly misguided in light of the Supreme Court's recent admonition that courts should avoid unnecessary rulings on how the Fourth Amendment applies to new technologies. *See City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2629, 177 L. Ed. 2d 216 (2010) ("The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.").

II. Magistrate Judges Cannot Abuse Their Discretion by Arbitrarily Denying Section 2703(d) Applications, but May Require Probable Cause Where Necessary to Avoid a Serious Constitutional Question.

The Government expresses anxiety that magistrates will irresponsibly wield the discretion granted to them by the statute, hyperbolically claiming that judges could "arbitrarily deny" an application (Gov. Br. 6), "on a whim"

(*id*.), "for any reason or no reason at all" (*id*.), with "no legitimate statutory or constitutional reason" (*id*. at 11). It further worries that judges would have "carte blanche" (*id*. at 6) to require whatever showing is dictated by their "personal predilections" or "suit[s] their individual notions of sound policy" (*id*. at 7). However, this sky-is-falling rhetoric flatly ignores the obvious: courts may not abuse their discretion. Or, as the panel put it: "[N]o judge in the federal courts has *arbitrary* discretion…." *Id*. at 24 (emphasis added).

As the Supreme Court has explained, "[d]iscretion is not whim…." *Martin v. Franklin Capital Corp*., 546 U.S. 132, 139 (2005). A court must have a reason to support its use of discretion, and that reason cannot be based on an error of law or fact. Rather, a court abuses its discretion when "'it base[s] its ruling on an erroneous view of the law or on a clearly erroneous assessment of the evidence.'" *Bowers v. Nat'l Collegiate Athletic Ass'n*, 475 F.3d 524, 538 (3d Cir. 2007), *quoting Cooter & Gell v. Hartmarx Corp*., 496 U.S. 384, 405 (1990). The panel majority, mindful of these limits on discretion, concluded that the magistrate judge had exceeded them by reaching a legal conclusion not supported by the factual record. In particular, the panel majority held that the magistrate's legal conclusion that cell site location information (CSLI) is protected by the Fourth Amendment was based on a factual premise that the sparse factual record did not support, *i.e.*, the premise that CSLI by definition is precise enough to reveal information about the interior of Fourth Amendment-protected spaces such as the home. *See* slip op. 16-17 (considering whether there was "any basis" for the magistrate's holding and concluding that "there [was] no evidence in this record" that CSLI was so revealing); *see also id.* at 24 (faulting the magistrate for "declin[ing] to issue a § 2703(d) order on legal grounds without developing a factual record"). In other words, the panel concluded

that by "bas[ing] its ruling on…a clearly erroneous assessment of the evidence," *Bowers,* 475 F.3d at 538, the magistrate court had abused its discretion. It therefore remanded to the magistrate with a caution that any further exercise of discretion must be supported by factual findings and a "full explanation" of the court's reasoning. Slip op. 29.

Importantly, the panel majority did *not* hold that the magistrate must conclude that the Fourth Amendment definitely *would* be violated by issuance of the Section 2703(d) order before she may exercise her discretion to deny the application, as both the Government (Gov. Br. 7) and Judge Tashima (slip op. 31) recognize. Rather, the panel plainly expects the magistrate to determine whether the requested order *may* violate the Fourth Amendment. Read in this manner, the panel majority's final directive to the magistrate—that any conclusion that a warrant is "required" be supported by factual findings and a full explanation, slip op. 28-29—makes perfect sense. To the extent the magistrate were to conclude that government acquisition of CSLI absent probable cause may possibly violate the Fourth Amendment, it would indeed be *required* by the doctrine of constitutional avoidance to use the constitutional safety valve provided by Congress and avoid that serious Fourth Amendment question by requiring a warrant.

Conversely, the alternative holding proposed by Judge Tashima in his concurrence—that the magistrate court must "find[] that the order *would* violate the Fourth Amendment" before exercising it discretion, slip op. 31 (emphasis added)—would lead to countless violations of the constitutional avoidance doctrine and frustrate Congress' intent, which was to preserve the constitutionality of the statute in the face of changing technology by providing courts with a sliding scale by which such weighty constitutional questions could be avoided. The rule proposed by Judge Tashima would

force every magistrate concerned about the Fourth Amendment status of information sought under Section 2703(d) to explicitly and unnecessarily rule on whether there is a constitutional expectation of privacy in that information before granting or denying a Government application. Not only would this make surplus out of the discretion provided in the statute—to the extent a court concludes that a requested order would violate the Fourth Amendment, it would be required to deny the Government's request regardless of the statute's authorization—it would also defeat Congress' purpose in granting that discretion, by necessarily requiring courts to rule on the constitutionality of the statute's application.

The Government, ignoring the simple rule that courts may not abuse their discretion, purportedly fears that the majority opinion will "sow widespread confusion and uncertainty." Gov. Br. 11. Yet it is the rule proposed by Judge Tashima that would truly lead to judicial chaos, as countless lower courts would be required to needlessly rule on the Fourth Amendment's applicability to all the various types of communications content and records that are available under Section 2703(d).

In contrast, and consistent with the doctrine of constitutional avoidance, Congressional intent, and the Supreme Court's caution in *Quon*, the panel majority's holding provides lower courts the discretion necessary to avoid broad holdings on how the Fourth Amendment applies to new technologies while clearly warning them not to abuse that discretion by denying applications without a clear legal rationale grounded in the facts. This narrow statutory holding, based on the plain language of Section 2703(d) read in manner consistent with Supreme Court and Third Circuit precedents, does not pose an issue of exceptional importance meriting *en banc* review by this Court.

III. The Panel's Opinion Does Not Conflict With Circuit Precedent.

The Government claims that the panel decision "conflicts sharply" with this Court's opinion in *U.S. v. Christie*, ___ F.3d ___, 2010 WL 026817 (3d Cir. Sept. 15, 2010). Gov. Br. 13. In particular, the Government points to the *Christie* court's holding that the Fourth Amendment does not protect the privacy of an Internet Protocol (IP) address assigned to a particular subscriber by an Internet service provider. Gov. Br. 12-14, *citing Christie*, slip op. 29. However, this "conflict" is entirely imaginary and does not warrant *en banc* review. [2]

First and most obviously, there is no conflict between this panel's opinion and *Christie* because the panel majority's application of the Fourth Amendment to CSLI is likely dicta, as Judge Tashima notes in his concurrence. Slip op. 31 n.11 ("I would also leave the expectation of privacy issue for the MJ on remand, in the first instance, *if* determination of that issue becomes relevant") (internal citation and quotation omitted) (emphasis added). After holding that the magistrate had abused her discretion under Section 2703(d) by relying on an inadequate factual record, the panel simply could have remanded to the magistrate for new factual findings and a full explanation of any further exercise of discretion. Therefore, in Judge Tashima's view, the panel majority's opinions on whether CSLI may implicate the Fourth Amendment depending on the facts were not necessary to dispose of the present appeal and were premature. Slip op. 31 n.11. In

[2] Importantly, the Government's underlying rationale for *en banc* rehearing—that the panel's opinion conflicted with existing precedent—is flatly incorrect as a matter of fact. The Government repeatedly mischaracterizes the timing of the *Christie* decision, inexplicably providing in its citations the date on which the case was submitted for decision, July 16, 2010, rather than the opinion's filing date. Gov. Br. 1, 3, 13. The *Christie* opinion was not actually filed until September 15th, a week after the opinion in this case, and was not designated as "precedential" until October 15. Gov. Br. 3 n.1.

other words, they were dicta, and "the standards for rehearing *en banc* look to the panel's *decision*, not to the panel's dicta. *See Am. Civil Liberties Union of New Jersey ex rel. Lander v. Schundler*, 168 F.3d 92, 98 n.6 (3d Cir. 1999) (emphasis added), *citing* Fed. R. App. P. 35 (rehearing in banc may be ordered "to secure or maintain uniformity of its *decisions*....") (emphasis added).

Furthermore, even if the panel majority's Fourth Amendment discussion is not dicta, it still does not warrant *en banc* review by virtue of its purported conflict with *Christie*. "This court does not ordinarily grant rehearing *en banc* when the panel's statement of law is correct and the controverted issue is solely the application of the law to the circumstances of the case," 3d Cir. IOP 9.3.2, yet that is exactly the situation here. *Christie* ruled on the Fourth Amendment status of an IP address, *not* CSLI, and in applying the holdings of *Smith v. Maryland*, 442 U.S. 435 (1976), concluded that the Fourth Amendment did not protect that information. *See Christie*, slip op. 29-30. Faced with distinctly different records, the panel here distinguished *Smith* on the facts—after spending a paragraph fully and correctly stating the law of that case, slip op. 25-26—and reached the very narrow conclusion that the Fourth Amendment *may* protect CSLI depending on how revealing it proves to be. Slip op. 17 ("We cannot reject the *hypothesis* that CSLI *may*, under certain circumstances, be used to approximate the past location of a person" in a manner that implicates the Fourth Amendment.) (emphasis added). These different results, based on markedly different circumstances, do not pose a conflict warranting *en banc* review. Indeed, in practical terms these narrow holdings pose no conflict *at all*: judges faced with applications to obtain IP address information without probable cause are bound by *Christie*, while those faced with applications

for CSLI will follow this panel's opinion.[3]

Without any true conflict to point to, the Government instead claims that the *Christie* panel's decision—through its glancingly brief Fourth Amendment discussion of IP addresses—stands for the "clear proposition…that non-content networking information…relayed from a customer to a service provider as an essential step in enabling the routing of communications" is unprotected by the Fourth Amendment under *Smith.* Gov. Br. 13-14. Such an over-reading of the *Christie* panel's narrow decision—denying Fourth Amendment protection to any "non-content networking information" of any kind on any network, regardless of how revealing that information is—flies in the face of the Supreme Court's caution in *Quon* that courts avoid unnecessary decisions on how the Fourth Amendment applies to newer technologies. 130 S. Ct. at 2629. This Court should not allow the Government to use a manufactured conflict between two exceedingly narrow holdings to justify the crafting of an overbroad application of *Smith*—a decades-old decision dealing solely with surveillance of manually dialed telephone numbers—to eliminate Fourth Amendment protection in any and all non-content networking information. Indeed, to the extent the *Christie* panel or this Court endeavored to do so, such a broad rule untethered to any facts would clearly be dicta.

This Court need not and should not consider the question of whether CSLI is protected by the Fourth Amendment unless and until the magistrate,

[3] Notably, the Ninth Circuit decision on which the *Christie* panel primarily relied, *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2008), explicitly limited its Fourth Amendment holding to the pen register and trap & trace surveillance of IP and e-mail addresses that was before it: "[O]ur holding extends only to these particular techniques and does not imply that more intrusive techniques…are also constitutionally identical to the use of a pen register" such as that used in *Smith*. 512 F.3d at 511.

on remand, has made such a ruling based on a full factual record. However, and as explained above, such a ruling will ultimately be unnecessary to the extent the magistrate identifies a serious constitutional question that can be avoided by the use of her discretion. This Court therefore should decline the Government's invitation to rule on such a serious constitutional question unnecessarily, and certainly in light of *Quon* must decline its invitation to craft an overbroad application of *Smith* for all networking technologies, past, present and future.

IV. The Panel Did Not Materially Misstate The Record Below.

In a final bid to generate an exceptionally important question or conflict where there is none, the Government claims that the magistrate court held that the Government has met its factual burden under Section 2703(d) such that remand is unnecessary. Notably, the Government never thought to make this argument to the panel itself, which unanimously found that the magistrate did no such thing. Slip op. 24, 28 (majority), 31 n.11 (concurrence). Rather, by saying in a footnote that "[t]he Government *may* reasonably expect that information as to the Criminal Suspect's historic whereabouts will provide valuable evidence of the locations of that person's sources of supply, 'stash sites', and distribution networks," 534 F. Supp. 2d 585, 588 n.12 (W.D.Pa. 2008) (emphasis added), it is clear in context that the magistrate was merely noting the possibility that the Government might be able to satisfy its "specific and articulable facts" burden under Section 2703(d), not that it had already done so.

CONCLUSION

For the foregoing reasons, *amici* respectfully urge the Court to deny the Government's request for a rehearing *en banc* in this matter.

DATED: November 29, 2010

By /s/ Kevin S. Bankston

Kevin S. Bankston
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333
bankston@eff.org

Attorneys for *Amici Curiae*

CERTIFICATE OF SERVICE

I certify that, on this 29th day of November, 2010, the OPPOSITION OF AMICI CURIAE ELECTRONIC FRONTIER FOUNDATION ET AL. TO PETITION FOR REHEARING EN BANC was served on all parties via electronic filing.

DATED: November 29, 2010

By /s/ Kevin S. Bankston
Kevin S. Bankston
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333
bankston@eff.org

Attorneys for *Amici Curiae*