---

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

---

# BRIEF OF *AMICIS CURIAE* SUSAN FREIWALD IN SUPPORT OF AFFIRMANCE OF THE DISTRICT COURT

---

Susan Freiwald
Professor of Law
University of San Francisco School of Law
2130 Fulton Street
San Francisco, CA 94117
(415) 422-6467
(415) 422-6433

## TABLE OF CONTENTS

TABLE OF AUTHORITIES ..... I

STATEMENT OF INTEREST ..... 1

SUMMARY OF ARGUMENT ..... 1

ARGUMENT ..... 2

I. GOVERNMENT ACQUISITION OF CELL SITE LOCATION INFORMATION "CSLI" CONSTITUTES A SEARCH UNDER THE FOURTH AMENDMENT ..... 2

A. Subjective Expectations of Privacy in CSLI ..... 3

B. Objective Expectations of Privacy ..... 5

1. People Are Entitled To Rely on the Privacy of Their CSLI ..... 5

2. Because CSLI Acquisition is Hidden, Continuous, Indiscriminate and Intrusive, It Must be Subject to the Warrant Requirement ..... 6

C. Acquisition of Historical CSLI Intrudes Upon Reasonable Expectations of Privacy ..... 12

II. NO "THIRD PARTY" RULE GOVERNS ACQUISITION OF CSLI ..... 13

A. The *Miller* Case Does Not Govern CSLI ..... 13

B. Smith v. Maryland Does Not Change the Analysis ..... 17

III. CSLI IS NOT TOO IMPRECISE FOR FOURTH AMENDMENT PROTECTION ..... 17

A. The Government Seeks More Than "Routine Business Records" ..... 18

B. Nothing in the Statute Limits the Content of CSLI ..... 19

C. Providers Lack a Statutory Obligation to Filter the CSLI They Disclose ..... 21

D. The Government's Self-Restraint Cannot Guarantee Fourth Amendment Protections ..... 22

CONCLUSION ..... 25

# TABLE OF AUTHORITIES

## Cases

*Berger v. New York*, 388 U.S. 41 (1967) ..... 7

*Hoffa v. United States*, 385 U.S. 293 (1966) ..... 16

*In Re Matter of Grand Jury Subpoenas to Southwestern Bell Mobile Sys.*, 894 F. Supp. 355 (W.D. Mo. 1995) ..... 19, 22

*In Re United States Application for an Order Authorizing Installation and Use of a Pen Register*, 415 F. Supp.2d 325 (W.D.N.Y. 2006) ..... 24

*In re: Applications of the United States for Orders*, 509 F. Supp.2d 64 (D. Mass. 2007) ..... 13

*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*, 534 F. Supp. 2d 585, 613 (W.D. Pa. 2008) passim

*In the Matter of the Application of the United States of America*, 515 F. Supp.2d 325 (E.D.N.Y. 2007) ..... 10, 20, 24

*Katz v. United States*, 389 U.S. 347 (1967) ..... 6, 14, 16, 25

*Kyllo v. United States*, 533 U.S. 27 (2001) ..... 2, 11, 21

*Quon v. Arch Wireless*, 529 F.3d 892, 905 (9th Cir. 2008) ..... 6, 17

*Smith v. Maryland*, 442 U.S. 735 (1979) ..... 13, 17

*United States v. Karo*, 468 U.S. 705 (1984) ..... 4, 9, 10, 11

*United States v. Knotts*, 460 U.S. 276 (1983) ..... 10

*United States v. Long*, 64 M.J. 57 (C.A.A.F. 2006) ..... 17

*United States v. Miller*, 425 U.S. 435 (1976) ..... passim

*United States v. Torres*, 751 F.2d 875 (7th Cir. 1984) ..... 7

*United States v. White*, 401 U.S. 745 (1971) ..... 15, 16

## Statutes

18 U.S.C. § 2518(7) ..... 4

18 U.S.C. § 2703(c) ..... 19, 20

18 U.S.C. § 2703(d) ..... 18, 23

47 U.S.C. § 1002 (b)(1) ..... 22

47 U.S.C. § 1002(a)(2)(B) ..... 22

**Other Authorities**

Al Gidari, Jr., *Symposium: Companies Caught in the Middle, Keynote Address*, 41 U.S.F. L. Rev. 535 (2007) ..... 9, 21, 22

Patricia L. Bellia and Susan Freiwald, *Fourth Amendment Protection for Stored E-mail*, 2008 U.Chi. L. Forum 121 ..... 16

Susan Freiwald, *First Principles of Communications Privacy*, Stanford J. Law & Tech. 2007 ..... 14

Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 Ala. L. Rev. 9 (2004) ..... 8

Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 So. Cal. L. Rev. 949 (1996) ..... 24

## STATEMENT OF INTEREST

Amicus is a law professor who teaches and writes scholarship in the areas of Cyberspace Law and Privacy Law. She has written several law review articles on how the Fourth Amendment and the federal surveillance statutes should apply to new communications technologies. She has also submitted amicus briefs in cases addressing the Fourth Amendment's application to newly emerging electronic surveillance techniques and has advised magistrate judges on the regulation of cell site location information. Amicus submitted an amicus brief in the District Court in this case. Amicus has no stake in the outcome of this case, but is interested in ensuring that electronic privacy law develops with due regard for the vital role electronic communications play in our lives.

## SUMMARY OF ARGUMENT

Government acquisition of cell-site location information ("CSLI"), whether historical or prospective, constitutes a Fourth Amendment search because it intrudes upon users' reasonable expectations of privacy. That third-party providers store CSLI does not detract from those expectations of privacy, contrary to the Government's claim of a broad "third-party" rule. The Government's further claim that the CSLI it sought in its application was insufficiently precise to implicate the Fourth Amendment should be rejected. To deny Fourth Amendment protection based on the Government's assurance that it

seeks only limited CSLI flouts the fundamental principle that Fourth Amendment protections may not be left in the hands of law enforcement agents. Because the government claims the ability to acquire CSLI without first procuring a probable cause warrant, the Court should affirm the District Court's decision to uphold the Magistrate Judge's Denial of the Government's Application. *See* McVerry Order of September 10, 2008 (Government Appendix 2, Docket No. 31), *aff'g 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*, 534 F. Supp. 2d 585 (W.D. Pa. 2008) ("*Lenihan Order*").

## ARGUMENT

### I. GOVERNMENT ACQUISITION OF CELL SITE LOCATION INFORMATION "CSLI" CONSTITUTES A SEARCH UNDER THE FOURTH AMENDMENT

When the "government violates a subjective expectation of privacy that society recognizes as reasonable," it conducts a Fourth Amendment search. *Kyllo v. United States*, 533 U.S. 27, 33 (2001). Because government agents intrude upon a cell phone user's reasonable expectation of privacy when they acquire his CSLI, they conduct a search under the Fourth Amendment and must either obtain a warrant based on probable cause or establish an exception to the warrant requirement. Common uses of cell phone technology support a subjective expectation of privacy in CSLI and applicable precedents support an

objective expectation. In particular, CSLI acquisition, like other forms of electronic surveillance, is hidden, continuous, indiscriminate and intrusive in ways that require extensive judicial supervision to protect Fourth Amendment rights. Acquisition of historical CSLI intrudes upon reasonable expectations of privacy no less than acquisition of prospective CSLI.

### A. Subjective Expectations of Privacy in CSLI

Most cell phone users would be unpleasantly surprised, if not outraged, to learn that a law enforcement agent could gain access to their location information without first obtaining a warrant based on a showing of probable cause. As the Magistrate Judge persuasively presented, CSLI may disclose to law enforcement agents that a cell phone user has attended an Alcoholics Anonymous meeting, sought AIDS treatment, or visited an abortion clinic. *See Lenihan Order*, 534 F. Supp. 2d at 586 & n.6. CSLI may divulge when and where a user gave confession, viewed an X-rated movie, or protested at a political rally. Knowledge that the government could keep track of such information could easily inhibit valuable and constitutionally protected activities.[1] Civil Liberties Amici clearly refute the government's contention that CSLI is insufficiently precise to yield these types of inferences.

[1] In addition to implicating 4th Amendment interests, CSLI disclosure may implicate 1st Amendment rights of expression and association.

EFF/ACLU/CDT Brief at 14-19.

Not surprisingly, cell phone users regard access to their CSLI records as yielding the data about their locations. A recent research report found that seventy-three percent of cell phone users surveyed favored "a law that required the police to convince a judge that a crime has been committed before obtaining [historical] location information from the cell phone company."[2] Seventy-two percent also supported a law requiring the police to give notice to the user whose CSLI they seek before obtaining historical CSLI.[3] Both findings demonstrate that most users view their CSLI as private information and expect it to remain private absent a compelling need for access.[4]

People surely entertain a subjective expectation or privacy in their CSLI, and would not expect police to have access to it without first demonstrating a compelling justification to a reviewing court. *See United States v. Karo*, 468 U.S. 705, 735 (1984) (Stevens, J., concurring in part and dissenting in part) ("As a general matter, the private citizen is entitled to assume, and in fact does

[2] Jennifer King and Chris Jay Hoofnagle, Research Report*: A Supermajority of Californians Supports Limits on Law Enforcement Access to Cell Phone Location Information* (April 18, 2008) (available at SSRN http://ssrn.com/abstract=1137988) ("*King and Hoofnagle report*").

[3] *Id*.

[4] Eighty-three percent of respondents agreed that police should be able to track them in an emergency, a view which statutes reflect. *See, e.g*., 18 U.S.C. § 2518(7) (providing a forty-eight hour period during which agents may wiretap without a warrant in an emergency).

assume, that his possessions are not infected with concealed electronic devices."). For the same reasons that people expect a law enforcement agent to obtain a warrant from a neutral magistrate before she may bug their conversations, monitor their phone calls or subject them to silent video surveillance, people would surely expect judicial oversight of that agent's use of their cell phones to track their every movement and activity.

### B. Objective Expectations of Privacy

#### 1. People Are Entitled To Rely on the Privacy of Their CSLI

The objective prong of the reasonable expectation of privacy test ultimately requires this Court to make a normative finding about whether users should be entitled to view the object of the search as private. As Justice Harlan, author of the reasonable expectation of privacy test explained. "The critical question, therefore, is whether under our system of government, as reflected in the Constitution, we should impose on our citizens, the risks of the electronic listener or observer without at least the protection of a warrant requirement." *United States v. White*, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting). The critical question in this case is whether in our society law enforcement agents may use cell phone technology as a window for constant surveillance of our citizens without the procedural limits imposed by the Fourth Amendment. The answer must be "no."

By analogy, the expectation of privacy users have in their CSLI must be objectively reasonable. Just as the Supreme Court recognized that warrantless government eavesdropping violated the privacy on which the target "justifiably relied" while using the telephone booth, *Katz v. United States*, 389 U.S. 347, 353 (1967), so too would warrantless access to CSLI violate the privacy on which cell phone users justifiably rely while using their cell phones. When describing government acquisition of telephone conversations as a search under the Fourth Amendment, the Supreme Court in *Katz* reasoned that "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in privacy communication," *Id.* at 352. To deny Fourth Amendment protection to CSLI would similarly ignore the vital role that mobile telephony has come to play today in the lives of the over 250 million subscribers in the United States.[5] *Cf. Quon v. Arch Wireless*, 529 F.3d 892, 905 (9th Cir. 2008) (finding that users of a text-messaging service have a reasonable expectation of privacy in their messages).

### 2. Because CSLI Acquisition is Hidden, Continuous, Indiscriminate and Intrusive, It Must be Subject to the Warrant Requirement

CSLI shares those features of other types of electronic surveillance that

[5] CTIA Semi-Annual Wireless Industry Survey at 2, (available at http://files.ctia.org/pdf/CTIA_Survey_Year_End_2007_Graphics.pdf) (reporting 255,395,599 cellular subscribers in the U.S at the end of 2007) ("CTIA Survey").

the Supreme Court and lower courts have found to require high procedural hurdles and extensive judicial oversight. In *Berger*, the Supreme Court explained that electronic eavesdropping techniques presented "inherent dangers" and therefore required more "judicial supervision" and "protective procedures" than even "conventional" searches. *See Berger v. New York*, 388 U.S. 41, 60 (1967); *see also id*. at 64 (noting that New York statute permitting eavesdropping with insufficient judicial oversight constituted a "general warrant" in violation of the Fourth Amendment).[6] When they determined that the Fourth Amendment required the same procedural hurdles for use of silent video surveillance, several federal Courts of Appeal elaborated on which features necessitated heightened judicial oversight. Judge Posner, in a widely-followed 7th Circuit decision, explained that the *hidden, continuous, indiscriminate,* and *intrusive* nature of electronic surveillance raises the likelihood and ramifications of law enforcement abuse. *See United States v. Torres*, 751 F.2d 875, 882-84 (7th Cir. 1984); *see id*. at 882 ("[I]t is inarguable that television surveillance is exceedingly intrusive . . . and inherently indiscriminate, and that it could be grossly abused — to eliminate personal privacy as understood in modern western nations,"); Susan Freiwald, *Online*

[6] In fact, law enforcement agents seeking CSLI should perhaps satisfy the heightened procedural requirements imposed on government wiretappers. See *Lenihan Order*, 534 F. Supp. 2d at 586 n.7.

*Surveillance: Remembering the Lessons of the Wiretap Act*, 56 Ala. L. Rev. 9, 789-80 (2004) (discussing cases and requirements).

When agents acquire CSLI they use a technique that is similarly hidden, continuous, indiscriminate and intrusive. Unlike the search of a home, which is usually subject to view either by the occupant of the home or his neighbors, government acquisition of CSLI is *hidden*. Just as a telephone user does not know when a law enforcement agent has wiretapped his call, a cell phone user does not know when a law enforcement agent has acquired his CSLI. That significantly raises the risk that agents will exceed the scope of a proper investigation with impunity. In addition, acquisition of CSLI is *continuous*, like the acquisition of telephone conversations and video surveillance footage. The longer the period an investigation spans, the greater the likelihood that the government will conduct surveillance without sufficient justification.

Besides being hidden and continuous, acquisition of CSLI is inherently *indiscriminate* in that much CSLI will not be incriminating but will rather reveal activities that are entirely unrelated to criminal actions. For example, in the case at bar the government seeks CSLI for a user upon whom apparently no individualized suspicion had fallen. *See Lenihan Order*, 534 F. Supp. 2d at 588 & n.11 (describing the subscriber whose CSLI they seek as having a cell phone apparently "used by" the target of the criminal investigation, but "provid[ing] no

specific information connecting these two individuals."). The government appears to seek information about apparently innocent parties regularly. According to an industry lawyer, "[w]ith respect to location information of specific users, many orders now require disclosure of the location of all of the associates who called or made calls to a target." *See* Al Gidari, Jr., *Symposium: Companies Caught in the Middle, Keynote Address*, 41 U.S.F. L. Rev. 535, 557 (2007). The risk of acquiring information about non-incriminating activities mandates substantial judicial oversight to reduce unwarranted invasions of privacy and to ensure that searches do not become government fishing expeditions.

The Government's assertion that CSLI is "far too imprecise by any measure to intrude upon a reasonable expectation of privacy," Gov. Br. at 26, and its claim that CSLI acquisition does not fall afoul of the *Karo* rule, Gov. Br. at 28-30, both pertain to the *intrusiveness* of CSLI. In Part III below, I argue that the Government has failed to establish that CSLI not precise. The Government's claim about the tracking device cases should not persuade this Court either.

As the Government recognizes in its brief, cell phones are much more than tracking devices.[7] Gov. Br. at 18-23. Cell phones are far more

[7] That is not to say that cell phones cannot be considered tracking devices

sophisticated than the homing device government agents attached to a container in an automobile and followed "on public streets and highways" in *United States v. Knotts*, 460 U.S. 276, 282 (1983). In addition, the agents in *Knotts* affixed the beeper to a five gallon drum of ether and monitored the drum rather than the individual suspects. Had the targets left the drum behind, monitoring of them would have been over. Cell phones, on the other hand, travel with and often on the users themselves. Thus the beeper monitoring the Supreme Court approved in *Knotts* was considerably less intrusive, by virtue of being considerably less reliable, than that afforded by acquisition of CSLI. *Cf. In the Matter of the Application of the United States of America*, 515 F. Supp.2d 325, 338 (E.D.N.Y. 2007) ("*Azrack Opinion*") (observing that "the evolution of technology and the potential degree of intrusion changes the [Fourth Amendment] analysis"). Moreover, because the *Knotts* Court focused on the lack of privacy in cars on public roads, its reasoning does not apply to CSLI which can reveal users' locations anywhere.

The monitoring the police conducted in *Karo*, and which the Supreme Court found to implicate the Fourth Amendment, comes closer to acquisition of CSLI. In *Karo*, the constitutional question turned on whether agents monitored the beeper in "a private residence, a location not open to visual surveillance."

---

for some purposes.

*Karo*, 468 U.S. at 714. The Court elaborated that agents determined that "the beeper was inside the house," which was "a fact that could not be visually verified." *Id*. at 715.[8] The Court imposed Fourth Amendment constraints on the Government's use of the beeper "to determine . . . whether a particular article – or a person, for that matter – is in an individual's home at a particular time." *Id.* at 716.

While it is not necessary for an investigative technique to penetrate the home to intrude upon a reasonable expectation of privacy, it is extremely likely that CSLI will reveal at least as much information about the inside of a home as the beeper revealed in *Karo*. With simple inferences, law enforcement agents may use even "imprecise" CSLI to reveal that a target is in his home, awake, and using the telephone. As Civil Liberties Amici present in their brief, agents have frequently used CSLI in court in just that way. EFF/ACLU/CDT Brief at 14-19. That evidence refutes the Government's assertion that CSLI is insufficiently precise to implicate the Fourth Amendment. *See Kyllo*, 553 U.S. at 36 (rejecting "dissent's extraordinary assertion that anything learned through 'an inference' cannot be a search"). CSLI acquisition is at least as intrusive, and likely much more so, than the information found subject to Fourth Amendment protection in *Karo*.

[8] In the case at bar, the Government apparently sought CSLI only after physical surveillance had "proven difficult." Gov. Br. at 5.

### C. Acquisition of Historical CSLI Intrudes Upon Reasonable Expectations of Privacy

Law enforcement acquisition of historical CSLI can intrude into personal privacy even more than acquisition of real-time or prospective CSLI. A law enforcement agent seeking prospective CSLI could get an order on August 1st to track the target's movements for three months, but then would have to wait until October 31st to obtain three months of CSLI to review. Alternatively, the agent could ask the provider for historical CSLI and immediately obtain a year's worth or more of the target's CSLI.[9] The length of time the target's cell phone generates records and the service provider stores them set the only limit on the scope of the historical records the law enforcement agent may acquire.

In addition, historical CSLI may be at least as informative to law enforcement agents as prospective CSLI. Historical data may indicate with whom targets have met, where, and for how long. It may put targets at a scene at the time a crime was committed there, and thereby refute the target's alibi. It should not be difficult to combine rich CSLI with other electronic data to reveal a user's complete digital profile. *See Lenihan Order*, 534 F. Supp. 2d at 612 ("[T]he privacy and associational interests implicated [by acquisition of CSLI] are not meaningfully diminished by a delay in disclosure."). Law enforcement acquisition of records of CSLI, or historical data, should receive the same Fourth

[9] Historical CSLI could contain data of quite recent vintage.

Amendment protection as acquisition of CSLI in real-time or prospectively. *See, e.g., In re: Applications of the United States for Orders,* 509 F. Supp.2d 64, 74 (D. Mass. 2007) ("[T]he same Fourth Amendment concerns that drive the necessity for a probable cause showing before authorization of a prospective tracking device apply equally to a 'historical' tracking device."); *see also id*. at 76 (finding no "material difference" between real time, prospective and historical tracking).

## II. NO "THIRD PARTY" RULE GOVERNS ACQUISITION OF CSLI

The Government rests much of its argument on a claim that historical CSLI is an unprotected third party record. *See* Gov. Brief at 26-28. It is no such thing. This Court should decline the Government's invitation to extend to CSLI the holding in *United States v. Miller*, 425 U.S. 435 (1976) (holding that customers lack a reasonable expectation of privacy in their bank records stored with the bank). The Government improperly reads *Miller* to posit a broad "third party" rule under which users forfeit constitutional protection of those things they voluntarily share with third parties. Its argument that *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979), also refutes subscribers' reasonable expectations of privacy in their CSLI merely extends their *Miller* argument.

### A. The *Miller* Case Does Not Govern CSLI

To determine whether subscribers have a reasonable expectation of

privacy in their CSLI, courts must engage in the two-part analysis outlined in *Katz*, rather than simply characterize the information as a third party record and consider the inquiry finished.[10] In *Miller*, the Supreme Court rejected defendant's claim of a reasonable expectation of privacy in the bank's records of his financial transactions. *Miller*, 425 U.S. at 442-443. As a result, Miller could not complain when government agents did not first obtain a warrant based on probable cause before they compelled the bank to turn over records of Miller's banking transactions. *Id.* at 444-45. It was not the Bank's mere ability to produce the records that precluded Miller's Fourth Amendment claim, but rather the nature of the records themselves and Miller's relationship to them that defeated his privacy expectations. *Id.* at 442 ("We must examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents.").[11]

Unlike banking records, CSLI provides detailed information about people's communications as well as their movements and activities. Because CSLI will often disclose extensive personal information, it much more closely

[10] *See* Susan Freiwald, *First Principles of Communications Privacy*, Stanford J. Law & Tech. 2007 (criticizing courts' tendency to rely on analytic shortcuts like a "third party" rule and a "content/non-content" distinction rather than analyzing reasonable expectations of privacy).

[11] The Court called the information sought "business records." *Miller*, 425 at 440. That likely explains the Government's attempt to characterize CSLI the same way. *See e.g.*, Gov. Br. At 2, 4, 26, 27, 35. In Section IIIA, infra, I argue that CSLI does not constitute a routine business record.

resembles the private communications the *Miller* Court found subject to a reasonable expectation of privacy than the banking records it did not. *See Miller*, 425 U.S. at 442 ("The checks are not confidential communications but negotiable instruments to be used in commercial transactions.").

Even if CSLI were like the bank records in *Miller*, that case's shaky foundation makes it a poor case to extend to the CSLI context. The Supreme Court's finding that Miller "voluntarily" shared his banking information with the bank and thereby waived his reasonable expectation of privacy in it is hard to justify in an age when banking is a necessity rather than a choice.[12] In addition, the *Mille*r Court treated the bank as a party to the transactions with Miller and found Miller's banking activities analogous to confiding in one's friends. *See Miller*, 425 U.S. at 443. Miller relied on two cases that concerned disclosures of conversations by actual parties to them. *See United States v. White*, 401 U.S. 745, 752 (1971) (finding the law to permit "authorities to use the testimony of those associates who for one reason or another have determined to turn to the police" and to permit those associates to record or transmit their conversations with the wrongdoer); *Hoffa v. United States*, 385 U.S. 293, 302 (1966) (finding no Fourth Amendment interest in incriminating statements voluntarily revealed

[12] Amici provide an excellent analysis of why cell phone subscribers should not be seen to assume the risk that their service providers will disclose their CSLI without a warrant. *See* EFF/ACLU/CDT Brief at 19-22. Because we agree with their analysis, we do not repeat it here.

to a confidant). It would make more sense to treat the bank as a third party intermediary between the customer and those with whom he transacted instead of as a party to those transactions (second party) as to whom Miller assumed the risk of disclosure. Because *White* and *Hoffa* addressed second party disclosures, and because the *Miller* Court treated the bank as a second party when it relied on those cases, *Miller* does not establish the broad third party rule that the Government seeks to invoke. *See* Patricia L. Bellia and Susan Freiwald, *Fourth Amendment Protection for Stored E-mail*, 2008 U. Chi. L. Forum 121, 145-58 (critiquing *Miller* and the claim that it establishes a broad "third party" rule).

As to true third parties intermediaries like cell phone service providers, their mere access to their customers' data cannot defeat those customers' reasonable expectations of privacy in that data. If so, that would contradict *Katz*, which established that users maintain a reasonable expectation of privacy in their telephone calls despite telephone employees' technical ability to monitor those communications. *Katz*, 389 U.S. at 353. Just last year, the Ninth Circuit held that a wireless company's ability to access its users' text "messages for its own purpose" did not detract from its users' reasonable expectations of privacy. *See Quon v. Arch Wireless*, 529 F.3d 892, 905 (9th Cir. 2008)("Appellants did not expect that Arch Wireless would monitor their text messages, much less turn over the messages to third parties without Appellants' consent"); *see also United*

*States v. Long*, 64 M.J. 57, 63 (C.A.A.F. 2006) (consent to monitoring did not imply consent to "engage in law enforcement intrusions . . . in a manner unrelated to the maintenance of the e-mail system").

### B. Smith v. Maryland Does Not Change the Analysis

The government relies on *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979), to further support its claim that one cannot expect privacy in information voluntarily turned over to third parties. *Smith* relied on *Miller*, see *Smith*, 442 U.S. at 744, and as just discussed, *Miller* does not establish a broad third party rule. In addition, the telephone numbers at issue in *Smith* vary considerably from CSLI, as do the risks users voluntarily assume about each.[13] *See* EFF/ACLU/CDT Brief at 19-22.

## III. CSLI IS NOT TOO IMPRECISE FOR FOURTH AMENDMENT PROTECTION

The Government argues that it may acquire CSLI without first obtaining a warrant based on probable clause because the CSLI it seeks is insufficiently precise to indicate information that implicates a reasonable expectation of privacy. However, whatever information the Government requested, we do not know what it would have obtained. The question of whether 18 U.S.C. § 2703(d) is constitutional depends on the nature of all the CSLI that service

[13] Exactly what service providers collect and retain as CSLI can not be common knowledge, as it is an issue in this case.

providers store, not the subset that may be requested in a particular case. Providers have no statutory obligation to filter the information they disclose, and, under foundational Fourth Amendment principles, courts may not trust the Government to filter the information themselves.

### A. The Government Seeks More Than "Routine Business Records"

Although the Government strongly implies that it seeks limited data, its actual application is not part of the public record.[14] Instead, the Government states that its Application seeks "the *type of records* shown in the record exemplar." Gov. Br. at 32-33 n.17 (emphasis added). The exemplar itself lists only the date and time of incoming and outgoing calls to the target, the telephone numbers involved (redacted), cell towers (including sectors) used at the beginning and end of each call, and the duration of calls. The Government does not claim that the exemplar matches the actual records it sought, but merely that "the exemplar is from the same wireless carrier from which the government seeks to obtain records in this proceeding." Gov. Br. at 8 n.6. In other words, the Government establishes that the targeted provider collects at least this type of information but not that it collects or would provide no more.

The exemplar is listed as the first of fifty-four pages and looks nothing

[14] In fact, the information sought in the redacted application that was filed under seal but made available solely to the Court and counsel for amici does not match that found in the exemplar. We invite this Court to compare the two.

like a customer bill. In fact, it apparently lists the date and time the report was created, rather than the subscriber's address or other account information. Although we cannot know for sure, the exemplar seems to be a report the provider drew from a set of raw data. The underlying data could actually be much more extensive. In fact, the Government implies that the exemplar includes but does not exhaust the information that may be found in the targeted provider's records. The Government indicates that it did not request triangulation or Global Position System ("GPS") data from the provider but it does not affirmatively state that such information would not have been available. Gov. Br. 9, 32-33 n.17.

So while the Government claims to request "Routine Business Records", Gov. Br. At 4, 35, it seems instead to be demanding that customized reports be drawn from data service providers retain. That fact further undermines the Government's weak third party claim, *See Azrack Opinion*, 515 F. Supp. 2d at 337 (rejecting an extension of the *Miller* "logic" because the information sought was not kept by service providers in the ordinary course of their businesses). It also weakens the Government's claim that CSLI is necessarily imprecise.

### B. Nothing in the Statute Limits the Content of CSLI

That the Government could likely obtain more extensive and intrusive information than that shown in the exemplar from the targeted provider or others

would be less worrisome if the applicable statutory provision limited the information it could obtain. It does not. As the Government recognizes in its brief, the language in 18 U.S.C. § 2703(c)(1) is a "catch-all category" designed to include any information that a service provider stores that is "pertaining to" a subscriber of an electronic communication service. Gov. Br. at 12.

Though the Government claims that service providers do not retain "a history" of "tower registration," which would indicate the location of the nearest cell site even when the cell phone is not making or receiving a call, it has provided no support for its prior claim that service providers always delete such data. *See* Gov. Request for Review at 3 n.2 (8/29/2008) (claiming that the exemplar demonstrates that carriers never store "call handoff" data). The Government could not possibly vouch for the business practices of all the different service providers.[15] As both the Magistrate Judge and Amici discuss at length, providers may record CSLI that includes much more extensive data than that contained in the exemplar. *See Lenihan Order*, 534 F. Supp. 2d at 589-91, 602; EFF/ACLU/CDT Brief at 11-13, 22-23.

Because law enforcement has and will have limited control over the content of CSLI, courts must take the inevitable growth of the technology into

[15] *See* Gidari, Jr., *Keynote Address*, 41 U.S.F. L. Rev. at 550 (reporting that in 2007 there were "at least 3500 registered carriers in this country" and "another 1300 wireless companies.")

account now. *See United States v. Kyllo*, 533 U.S. 27, 36 (2001) ("While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development."); *see also* i*d.* at 40 (rejecting the idea that the constitutionality of the surveillance should be judged on the basis of what occurred in the case at bar, and instead requiring courts to "take the long view" and give "clear specification of those methods of surveillance that require a warrant").

### C. Providers Lack a Statutory Obligation to Filter the CSLI They Disclose

Whatever the Government in fact requested in its Application, there is no way to know what it actually would have received in response.[16] To the extent service providers retain more than the limited subset of CSLI the government purports to seek, there would be neither reason nor way for providers to filter CSLI so as to make what they deliver comply with that request for limited data. In a related context, for example, the Communications Assistance for Law Enforcement Act ("CALEA") requires that law enforcement agents do more than obtain a pen register order to acquire CSLI in real-time. 47 U.S.C. § 1002(a)(2)(B). Despite the clear prohibition against it, providers presented only with pen register orders apparently fail to filter out location data because it is

[16] Even assuming that the provider kept limited data at the time of the Application a year ago, it may now keep much extensive (and precise) CSLI that it could provide to the Government even if the Government requested less.

just too costly to do so. *See* Gidari, Jr., *Keynote Address*, 41 U.S.F. L. Rev. at 549 ("[u]nder every pen register order implement, the government gets location. . . . The location information is just flowing as part of the solution."); *see also id*. at 550 (Service providers "are paying a fortune for the CALEA hardware and software, and they are not paying to filter it further.").[17] Even without seeking it, then, law enforcement agents will likely receive CSLI that intrudes upon users' constitutionally protected privacy interests.

### D. The Government's Self-Restraint Cannot Guarantee Fourth Amendment Protections

The Government's argument that its limited request for information insulates that request from Fourth Amendment scrutiny boils down to a claim that its agents in the field may be trusted to protect Fourth Amendment rights through self-restraint. Law enforcement agents may not avoid the application of the Fourth Amendment by asserting that they themselves will limit their review of CSLI and that they may do so without meaningful judicial oversight.

Whether or not this Court credits the Government's claim that it seeks CSLI that is more limited than what it could acquire from the provider, nothing

[17] *See also* 47 U.S.C. § 1002 (b)(1) (clarifying that law enforcement may not compel or prohibit service providers from using any particular equipment or technology to comply with CALEA); *see also In Re Matter of Grand Jury Subpoenas to Southwestern Bell Mobile Sys.*, 894 F.Supp. 355, 359 (W.D. Mo. 1995) (describing how in using "toll records" in the SCA, Congress intended to "make certain that the providers of electronic communication services were not required to create records not kept in the ordinary course of business").

in the statute requires that self-restraint or ensures that agents seeking CSLI in the future will be so circumspect. Failure to require a probable cause warrant before agents may compel disclosure of CSLI, therefore, opens the floodgates to constitutional violations.[18]

To trust the government to curb its own appetite for increasingly intrusive CSLI would run counter not only to constitutional principles but also to experience. For example, as pen registers evolved from devices that recorded telephone numbers into devices capable of recording ever richer data, law enforcement agents demanded the ability to use them without satisfying more than the minimally demanding requirements Congress established in 1986. *See* Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act,* 69 So. Cal. L. Rev. 949, 982-89 (1996) ("The Evolution of the Pen Register from Mechanical Device to Computer System."). In the latest installment of this story, law enforcement agents have even advocated the right to obtain post-cut-through-dialed-digits with a pen register order, despite the fact that those digits often contain content, on the ground that service providers are unable to filter out the non-content data. *See Azrack Opinion*, 515 F. Supp.2d at 328, 332 n.5. "Post-cut-through dialed digits" generally refers to digits dialed

[18] Oversight under 18 U.S.C. § 2703(d) includes neither probable cause justification, meaningful remedies for misuse, nor judicial oversight of the monitoring, once begun.

after the first ten (phone number digits) and may include bank account numbers, social security numbers, and prescription numbers. *See id.* at 328. Courts have quite properly found that to allow law enforcement agents to segregate the data themselves would violate the Fourth Amendment. *See, e.g., id* at 339.

By urging this Court to sidestep the constitutional inquiry and credit its representation that agents will not seek data that implicates the Fourth Amendment, the Government asks that executive agents be permitted to take on for themselves the oversight role the Constitution entrusts solely to the members of the judiciary.[19] The Supreme Court soundly rejected a similar request more than forty years ago:

> The Government urges that, because its agents . . . did no more here than they might properly have done with prior judicial sanction, we should retroactively validate their conduct. That we cannot do. It is apparent in this case that the agents acted with restraint. Yet the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer. They were not required, before commencing the search, to present their estimate of probable cause for detached scrutiny by a neutral magistrate. They were not compelled, during the conduct of the search itself, to observe precise limits established in advance by a specific court order. Nor were they directed, after the search had been completed, to notify the authorizing magistrate in detail of all that had been seized.

*Katz v. United States*, 389 U.S. 347, 356 (1967).

[19] According to one court, agents limit their requests specifically to avoid constitutional confrontations. See *In Re United States Application for an Order Authorizing Installation and Use of Pen Register*, 415 F. Supp.2d 211. 218 n.5 (W.D.N.Y. 2006)

## CONCLUSION

Just as with wiretapping, video surveillance, and searches of the home, acquisition of historical CSLI intrudes upon users' reasonable expectations of privacy and must be subject to Fourth Amendment safeguards. In particular, agents must first convince a neutral and detached magistrate that they have probable cause to believe that such acquisition will yield evidence of a crime before they may compel service providers to disclose CSLI, whether prospective or historical. Any purported imprecision of CSLI does not change that constitutional mandate. Law enforcement may certainly acquire CSLI, but not in ways that flout the Fourth Amendment. I urge this Court to affirm the District Court's decision.

Respectfully submitted

Date March 16, 2009 s/ Susan Freiwald

Susan Freiwald
Professor of Law
University of San Francisco
School of Law
2130 Fulton Street
San Francisco, CA 94117
NY2557627
Phone: (415) 422-6467
E-mail: freiwald@usfca.edu

## CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 5925 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2003 version 11 in Times New Roman, 14-point font.

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

4. A virus check was performed on this brief using Sophos Anti-Virus Version 7.7.5.

Dated: March 16, 2009 s/ Susan Freiwald

Susan Freiwald
Professor of Law
University of San Francisco
School of Law
2130 Fulton Street
San Francisco, CA 94117
NY2557627
Phone: (415) 422-6467
E-mail: freiwald@usfca.edu

## CERTIFICATE OF SERVICE

I certify that on this 16th day of March, 2009, the BRIEF OF AMICUS CURAIE SUSAN FREIWALD IN SUPPORT OF AFFIRMANCE OF THE DISTRICT COURT was served on all parties via electronic filing and that pursuant to Third Circuit Rule of Appellate Procedure 25.1 ten (10) paper copies will be delivered to a third party commercial carrier for delivery to the Clerk of the Court within three calendar days.

Dated: March 16, 2009 s/ Susan Freiwald

Susan Freiwald
Professor of Law
University of San Francisco
School of Law
2130 Fulton Street
San Francisco, CA 94117
NY2557627
Phone: (415) 422-6467
E-mail: freiwald@usfca.edu