IN THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF PENNSYLVANIA

In the Matter of the Application of the UNITED STATES of America FOR AN ORDER DIRECTING A PROVIDER OF ELECTRONIC COMMUNICATIONS SERVICE TO DISCLOSE RECORDS TO THE GOVERNMENT,	)	**Magistrate's No. 07-524M**

BRIEF OF AMICUS CURIAE SUSAN FREIWALD IN FAVOR OF AFFIRMANCE

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

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 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, even when the government requests only the type of data at issue in this case. There is no reason to deny Fourth Amendment protection to CSLI, and, in fact, reason to require that government agents satisfy the more demanding hurdles imposed on government wiretappers before they acquire CSLI. Because the government claims the ability to acquire CSLI without first procuring a probable cause warrant, the Court should deny the government's request to review, and should affirm Magistrate Judge Lenihan's order.

ARGUMENT

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

Because government agents intrude upon a mobile 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 mobile phone technology support a subjective expectation of privacy in CSLI and applicable precedents support an objective expectation, whether the CSLI comprises prospective or historical data. Users have a reasonable expectation of privacy in CSLI that reveals activities in their homes as well as activities outside their homes. Law enforcement agents may not avoid the application of the Fourth Amendment by asserting that they themselves will limit their review of CSLI without meaningful judicial oversight.

A. The Government's Self-Restraint and the Imprecision of the CSLI Should Not Impact the Constitutional Analysis

The thrust of the government's argument is that it should be entitled to acquire CSLI without first obtaining a warrant based on probable clause because the CSLI it acquires is insufficiently precise to indicate information that implicates a reasonable expectation of privacy. In particular, the government claims that the CSLI it has requested does not provide information about the inside of a home. The government's claim lacks merit. CSLI, even if imprecise, will almost always indicate constitutionally-protected information about the inside of a home, and may well implicate the Fourth Amendment even without revealing in-home information. Moreover, it would be improper to rely on the government's self-restraint, both as a matter of constitutional principles and practical reality. The government likely has little control over what information the service providers divulge, and may well acquire quite precise information, no matter what it requests. And CSLI will grow only more precise over time. If, on the other hand, law enforcement agents dictate the content of the CSLI they acquire, then service providers may serve as agents of the government, and their own actions

in acquiring CSLI could constitute a Fourth Amendment search.

1. Even If CSLI Is Limited As the Government Claims, Its Acquisition Implicates the Fourth Amendment Right of Privacy in the Home

The government claims that the data it seeks is not sufficiently precise to intrude on users' constitutional privacy rights. The government claims in it brief to have requested information of the type it provides in Exhibit C, which reveals the telephone numbers dialed, the identification number ("PTN") of the caller/called party, the duration of a call, whether it was international, forwarded, inbound or outbound and the physical location of the caller at the outset and end of the call as indicated by information about the nearest cell site, including which face of the cell tower received the signal. *See Government's Brief*, Exhibit C Document 11-4.[1] The government characterizes this information as "much too imprecise to tell whether calls have been made or received from a constitutionally protected space, let alone to reveal facts about the interiors of private homes or other protected spaces." Government Brief at 26.

The government focuses on the interiors of private homes because clear Supreme Court precedents establish a privacy interest there. Over twenty years ago, in *United States v. Karo*, 468 U.S. 705 (1984), the Supreme Court recognized that acquisition of location data that reveals information about what takes place inside a home constitutes a Fourth Amendment search. *See id*. at 714 (recognizing the "basic Fourth Amendment principle" that people have a reasonable expectation of privacy in their homes); *see also Kyllo v. United States*, 553 U.S. 27, 31 (2001) (describing the right to privacy in the home as at the "very

[1] The government's application indicates that it has sought some additional information that may well divulge more about the target's movements and activities. Because the Judge's order permits viewing only by the attorneys in this case, I do not feel at liberty to further discuss that information.

core" of the Fourth Amendment).

The government errs, however, when it implies that the only way for the acquisition of CSLI to implicate the Fourth Amendment is for it to pinpoint a target's location in a space that exactly matches an area previously identified as his home. There are other possible ways for CSLI to reveal facts about the interior of a home. For example, the target will likely use his cell phone regularly from his home in the morning, evening and weekend hours.[2] Law enforcement agents should be able to infer, from data covering a fairly short time frame and of the type sought in this case, when the target is making and receiving calls from home and from there to identify the cell tower and face closest to his home.[3] Once agents identify that tower/face combination, then whenever it is the tower/face identified on a call, the target is likely in his home. In addition to the timing of the target's calls, law enforcement agents could use the telephone numbers of those called and calling and the duration of calls to identify similar patterns in CSLI that establish when the target was in his home using his cell phone.

With simple inferences, then, law enforcement agents may use supposedly "imprecise" CSLI to reveal that a target is in his home, awake, and using the telephone. That would suffice to implicate the Fourth Amendment under *Karo* and necessitate a probable cause warrant. *See Karo*, 468 U.S. at 714; *see also id*. at 708-11 (when beeper indicated that the monitored drum remained in the house, it conveyed information about "a private

[2] In fact, many users have replaced their land-line phones with cell phones, which they use to make and receive all calls. *See* The Harris Poll #36: "Cell Phone Usage Continues to Increase" (April 4, 2008) (available at http://www.harrisinteractive.com/harris_poll/index.asp?PID=890) (finding that 32% of Americans aged 18-29 and 14% of all adults used a cell phone only).

[3] In addition to divulging information about actual calls, if CSLI was recorded whenever the telephone was powered on, then the information would quickly divulge when a target was home because it would show the telephone on in the same place for long periods (*e.g*., sleeping hours) that would correspond to the time the target was home.

residence, not open to visual surveillance."). That agents need to make inferences about CSLI to obtain from it information about the interior of the home does nothing to negate the Fourth Amendment implications. *See Kyllo*, 553 U.S. at 36 (rejecting "dissent's extraordinary assertion that anything learned through 'an inference' cannot be a search").

Information that the target is on the phone and awake sufficiently implicates the target's right to privacy. In *Kyllo*, the Supreme Court rejected the idea that the search has to reveal "intimate details" to intrude upon reasonable expectations of privacy. *See Kyllo*, 533 U.S. at 39-40. According to the *Kyllo* Court, because the line of privacy at the home has to be both "firm and bright," government investigations that rely on a device "not in general public use" [4] to divulge details about the home that would not otherwise be available without a physical intrusion constitute Fourth Amendment searches. Id.

The government implies that it need not get a warrant before acquiring CSLI because agents will not be able to tell in advance whether the target has used the cell phone in his home. But that putative lack of knowledge is the reason to get a warrant rather than to be excused from getting one. *See 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 n. 75 (W.D. Pa. 2008) ("*Lenihan Order*") ("The argument that a warrant requirement would oblige the Government to obtain warrants in a large number of cases is hardly a compelling argument against the requirement.") (quoting *Karo*, 468 U.S. at 718). Just as the Supreme Court did in *Karo*, when it recognized that "[r]equiring a warrant will have the salutary effect of ensuring that the use

[4] The relevant device for obtaining CSLI would not be the cell phone itself but rather the cell phone company hardware and software that records CSLI. Such hardware and software presumably are not in general public use.

of beepers is not abused, by imposing upon the agents the requirement that they demonstrate in advance their justification for the desired search," *Karo*, 468 U.S. at 717, modern courts should impose a warrant requirement on government acquisition of CSLI.

2. Acquisition of CSLI About Information Outside the Home Also Implicates the Fourth Amendment

While government acquisition of CSLI that reveals information about activities taking place within a private home most clearly implicates the Fourth Amendment, that is not the only way for acquisition of CSLI, even of the limited type the government purports to seek, to do so. The government's claim that information about public activities cannot constitute a Fourth Amendment search overstates a rule that, in any case, has only limited applicability to CSLI.

The Government cites *United States v. Knotts*, 460 U.S. 276, 282 (1983), for the proposition that "there is no reasonable expectation of privacy in cell-site information." Government Brief at 22. But *Knotts* had nothing to do with CSLI. It concerned the government's monitoring of a radio beeper attached to a large container of chemicals stored in an automobile that government agents followed "on public streets and highways." *Knotts*, 460 U.S. at 281. Several meaningful differences between CSLI and the data divulged by the beeper in *Knotts* undermine the Government's claim about a lack of privacy in CSLI.

First, agents affixed the beeper in *Knotts* to a five gallon drum of ether and monitored the drum rather than the individual suspects. If those surveillance targets had been separated from the drum for any reason, the monitoring would have ceased being effective. Cell phones, on the other hand, travel with and often on the users themselves. Modern cell phones include so many features in addition to calling, that users have reason to have them at hand all the time. *See United States v. Park*, 2007 WL 1521573, at *8 (N.D. Cal.) (listing features of

"modern cell phones" such as "address books, calendars, voice and text messages, email, video and pictures"). Thus the beeper monitoring the Supreme Court considered in *Knotts* was considerably less intrusive, by virtue of being considerably less reliable, than that afforded by acquisition of CSLI.[5] *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*") (finding use of pen registers to divulge content to violate the Fourth Amendment and observing that "the evolution of technology and the potential degree of intrusion changes the analysis").

Second, because government agents exclusively monitored a car, the *Knotts* Court relied on the "diminished expectation of privacy in an automobile." *Knotts*, 460 U.S. at 281; *see also United States v. Forest*, 355 U.S. 942, 951-52 (6th Cir. 2004) (because the CSLI in the case divulged only the movements of a car along public highways, on facts "nearly identical to the facts in *Knotts*," its acquisition did not implicate the Fourth Amendment). CSLI, by contrast, reveals the movements and activities of cell phone users in many places besides their cars; modern cell phones accompany their users on walks, into buildings, as well as into their homes. *See* James X. Dempsey, *Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology*, PLI Order No. 14648, 572 (June-July 2008) ("A cell phone clearly goes places where an individual has a reasonable expectation of privacy."). Because the *Knotts* Court focused on the lack of privacy in cars on public roads, its reasoning does not apply to CSLI.

That CSLI is the product of substantially enhanced technology also has constitutional significance. In *Knotts*, the Supreme Court announced that "[n]othing in the Fourth

[5] In addition, because agents often obtained a warrant before installing the type of beeper used in the mid-1980's, that initial hurdle limited the use and therefore possible abuse of beepers. *See Karo*, 468 U.S. at 713, n.3 (discussing advisability of getting a warrant before installing a beeper).

Amendment prohibited the police from augmenting the sensory facilities bestowed on them at birth with such enhancement as science and technology afforded them in this case." *Knotts*, 460 U.S. at 282. Years later, however, the Supreme Court disavowed the notion that use of sense enhancement technology does not implicate the Fourth Amendment. *See Kyllo*, 533 U.S. at 32 ("The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy"). In *Kyllo*, the Court rejected the notion that use of the thermal imaging device was not a search because, had snow been present on the roof, its melting patterns could have revealed (without technology) the same information about heat in the house. *See Kyllo*, 533 U.S. at 35 n.2 ("The fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment.").

Moreover, even if "public information" were not subject to a reasonable expectation of privacy, cell phones often travel in pockets or pocketbooks and therefore are "withdrawn from public view." *See Karo*, 468 U.S. at 716. If, as the Supreme Court explained in *Karo*, agents need to "obtain warrants prior to monitoring a beeper when it has been withdrawn from public view," *Id* at 718, they need to obtain a warrant before acquiring CSLI when the cell phone that produces it is removed from public view. *See id*. at 735 (Stevens, J., concurring in part and dissenting in part) ("The concealment of such [electronic devices] on personal property significantly compromises the owner's interest in privacy, by making it impossible to conceal that item's possession and location from the Government, despite the fact that the Fourth Amendment protects the privacy interest in the location of personal property not exposed to public view.")

Finally, acquisition of CSLI about those for whom there is no individualized suspicion

of wrongdoing implicates the Fourth Amendment as well. *See City of Indianapolis v. Edmund*, 531 U.S. 32, 37 (2000) ("A search or seizure is ordinarily unreasonable in the absence of individualized suspicion of wrongdoing."). For example, in the case at bar the government seeks CSLI for a user upon whom apparently no individualized suspicion has focused. *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, or connecting the Criminal Suspect to [the subscriber's] cell phone."). 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). As the Electronic Frontier Foundation, *et. al.*, persuasively argues in their amicus brief in this case, the "dragnet type" surveillance that the Supreme Court assured was not occurring in *Knotts* may well be just what acquisition of CSLI affords. See Electronic Frontier Foundation Brief, at V(C)(2); *see also Knotts*, 460 U.S. at 284. In theory, the more than two hundred and fifty million Americans who use cell phones as their primary or significant means of communication are vulnerable to government surveillance when law enforcement agents have access to their CSLI.[6] That risk necessitates judicial oversight of the acquisition of CSLI.

[6] 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").

3. Law Enforcement Agents' Relationships with Service Providers Raise Constitutional Questions

Even if the government successfully demonstrated that the CSLI it seeks does not implicate the Fourth Amendment, the CSLI the government seeks may well not be the CSLI it obtains. There are several possible scenarios, each with different implications for the Fourth Amendment. Under one, law enforcement agents obtain all the records the service providers store in the ordinary course of their businesses. In that case, it is probable that agents will receive, in the near future if not already, even more detailed CSLI than that which they purport to seek. In the second scenario, service providers will retain the CSLI law enforcement asks them to retain. In that case, the providers themselves may be agents of the government and their own acquisition of CSLI would need to be evaluated under the Fourth Amendment.

Throughout its brief, the Government argues that it seeks only the business records of the service providers, nothing more and nothing less.[7] If so, then law enforcement agents have no effective control over what information is included in CSLI. 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 provides no support for its implied claim that service providers always delete such data. *See* Government Brief at 22-23. The Government could not possibly vouch for the business practices of all the different service providers.[8] In fact, in some cases, government agents have apparently asked for extensive historical data. *See, e.g., In re:*

[7] I reject the argument that CSLI falls into a "business records" type exception to the Fourth Amendment *infra* pages 21-25.

[8] *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.")

Applications of the United States for Orders, 509 F. Supp. 64, 74 n.6 (D. MA. 2007) (describing "cell site information," in the context of an application for historic data as "the physical address/location of the cell site, the call origination, call termination, as well as the strength, angle and timing of the caller's signal.") ("*Alexander Opinion*"). Even a good faith attempt to acquire the limited data that the government purports to seek, therefore, may be thwarted by business practices over which the government has no control. If government agents receive CSLI for an extended period, it would be nearly impossible for that not to constitute a Fourth Amendment search.[9]

Current trends suggest that production of ever more precise location data is on the rise, particularly as service providers comply with the statutory mandate to hone their location tracking.[10] Consumers' demand for services that require precise location data will encourage production of ever finer CSLI. For example, one provider permits parents to track their children's movements on a street map.[11] Others inform cell phone users which restaurant, gas station, or even friend is closest to their exact location.[12] The increasing availability of these services illustrates the inevitability of CSLI becoming increasingly detailed, if it is not already. Even if these services are designed only for real-time use, cell phone companies could obtain value by selling historical CSLI for use in developing and testing these and related applications. Thus providers are bound to retain historical CSLI for some time.[13] *See*

[9] *See* footnote 3.

[10] *See Lenihan Order*, 534 F. Supp. at 598 (discussing enhanced 911 rules).

[11] See Family Locator, available at https://sfl.sprintpcs.com/finder-sprint-family/moreInfo.htm.

[12] See Michelle Higgins, *A Guide to Anywhere, Right in Your Hand*, New York Times, June 17, 2007, 56; Ryan Kim, *Find Friends by Cell Phone,* San Francisco Chronicle, November 14, 2006, at C-1.

[13] In researching this brief, several service providers rebuffed inquiries about their current practices regarding the content and storage of CSLI, claiming that the information is

Lenihan Order, 534 F. Supp. 2d at 589-91, 602 (describing how service providers are developing and retaining increasingly precise CSLI).

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 it delivers less intrusive, particularly since the intrusiveness of the data would not be easy to determine without analysis. In the context of prospective CSLI, 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 acquiring CSLI solely with a pen register order, providers presented only with pen register orders apparently fail to filter out location data because it is 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.")[14] Even without seeking it, then, law enforcement agents will likely receive CSLI that intrudes upon users' constitutionally protected privacy interests.

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

---

proprietary. That further supports the idea that companies see a market for the data.

[14] *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").

already in use or in development."); *see also Kyllo*, 533 U.S. 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").

On the other hand, if instead of passively receiving whatever CSLI providers maintain, law enforcement agents successfully dictate to service providers what to include in the CSLI they produce, then providers may be acting as agents for the government. *See, e.g.*, *McClelland v. McGrath*, 31 F. Supp. 2d 616, 619 (N.D. Ill. 1998) (noting that when telephone company employees act "at the request or direction of police officers," they act as government agents and the Fourth Amendment applies). That practice would only heighten the need for meaningful judicial review, because the service providers' own acquisition of detailed CSLI would itself constitute a Fourth Amendment search if done for law enforcement purposes. It seems, in fact, that companies are currently retaining CSLI for a law enforcement purpose. *See Lenihan Order*, 534 F. Supp. 2d at 615 (suggesting that providers retain CSLI "principally, if not exclusively, in response to Government directive" instead of "any business purpose for the customer or for the provider in serving the customer").

4. Law Enforcement Self-Restraint Cannot Protect Fourth Amendment Rights

The prior discussion assumed that law enforcement agents either acquired service providers' CSLI in whatever form the providers retained their business records, or engaged service providers as government agents to acquire CSLI. The more likely scenario falls in between those two: law enforcement agents encourage service providers to retain the information the agents find most valuable, but service provider retention does not constitute state action. The problem is that, under this scenario, law enforcement agents ask the courts

to trust them to limit their inquiries to those that do not implicate the Fourth Amendment and to do so without effective judicial oversight.[15]

By urging the court to sidestep the constitutional inquiry and credit their representations that they will not seek data that implicates the Fourth Amendment, law enforcement agents are asking to assume themselves the oversight role the Constitution entrusts solely to the members of the judiciary. 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.

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

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

[15] 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. For that reason, it neither sufficiently deters abuse nor meets the Fourth Amendment requirements.

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. 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. Similarly, courts should find that the Constitution prohibits trusting law enforcement agents themselves to segregate CSLI as they currently request.

B. Users have a Reasonable Expectation of Privacy in their CSLI

When the "government violates a subjective expectation of privacy that society recognizes as reasonable," it conducts a Fourth Amendment search. Kyllo, 533 U.S. at 33. Because law enforcement agents conduct a Fourth Amendment search when they acquire CSLI, they may not do so without first acquiring a probable cause warrant from a neutral magistrate.[16]

1. Subjective Expectations of Privacy in CSLI

Most mobile phone users would be unpleasantly surprised, if not outraged, to learn that a law enforcement agent could gain access to their CSLI without first obtaining a warrant based on a showing of probable cause. A recent study found that 73% 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."[17]

[16] In Part III, *infra*, I argue that law enforcement agents may in fact need to satisfy the heightened procedural requirements imposed on government wiretappers.

[17] Jennifer King and Chris Jay Hoofnagle, Research Report*: A Supermajority of Californians Supports Limits on Law Enforcement Access to Cell Phone Location Information*

72% also supported a law requiring the police to give notice to the user whose CSLI they seek before obtaining historical CSLI.[18] Both findings demonstrate that most users view their CSLI as private information and expect it to remain private absent a compelling need for access.[19]

CSLI may disclose to law enforcement agents that a cell phone user has attended an Alcoholics Anonymous meeting, or sought AIDS treatment, or visited an abortion clinic.[20] It 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.

People surely entertain a subjective expectation or privacy in their CSLI, and would not approve of their cell phones being turned into tracking devices monitored largely at the discretion of law enforcement agents. *See Karo*, 468 U.S. at 735 (Stevens, J., concurring in part and dissenting in part) ("As a general matter, the private citizen is entitled to assume, and in fact does assume, that his possessions are not infected with concealed electronic devices."). While that privacy interest grows as the specificity and comprehensive nature of the CSLI grows, even limited CSLI should provide a sufficient view into a user's personal activities and movements to intrude upon his subjective expectation of privacy.

(April 18, 2008) (available at SSRN http://ssrn.com/abstract=1137988) ("*King and Hoofnagle report*").

[18] *Id.*

[19] 83% of respondents agreed that police should be able to track them in an emergency, which accords with the current statutory provisions that allow for warrantless searching and wiretapping for limited periods in cases of emergency. *See, e.g.*, 18 U.S.C. § 2518(7) (providing a 48 hour period during which agents may wiretap without a warrant in an emergency).

[20] *See* Matthew Mickle Werdegar, *Lost? The Government Knows Where You Are: Cellular Telephone Call Location Technology and the Expectation of Privacy*, 10 Stan. L. Policy Rev. 103, 111 (1998).

2. Objective Expectations of Privacy in CSLI

The objective prong of the reasonable expectation of privacy test ultimately requires a court to make a normative finding about whether users should be entitled to view the object of the search as private. *See* Susan Freiwald, *First Principles of Communications Privacy*, Stanford J. Law & Tech. 2007 (describing the difficulties courts have in analyzing reasonable expectations of privacy and in making the requisite normative judgments). Just as citizens in a democracy would not want to live in a society where the police may listen in on their telephone conversations without the protections afforded by the Fourth Amendment, surely they would not want to live in a society in which the increasingly common use of mobile phone technology operates as a window through which law enforcement agents may view our movements and activities.[21]

Users have a reasonable expectation of privacy in their CSLI because it reveals information about the inside of a home. In *Karo*, the Supreme Court made clear that "private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable." *Karo*, 468 U.S. at 714. As discussed, even CSLI that conveys information about activities outside of the home may very well intrude upon users' reasonable expectations of privacy.

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*, 389 U.S. at 353, so warrantless access to CSLI would violate the privacy on which cell phone users justifiably rely while using their cell phones. By analogy, the expectation of

[21] Again, citizens would likely approve of location monitoring in an emergency, but in non-emergency contexts a judge should monitor the monitoring.

privacy users have in their CSLI must be objectively reasonable. 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," *Katz*, 389 U.S. 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.

Accordingly, several of the courts to have considered the question have found or strongly implied a reasonable expectation of privacy in CSLI. *See, e.g., Alexander Opinion*, 509 F. Supp. 2d at 74 n.6 ("[A] cell phone user maintains a reasonable expectation of privacy about his location."); *In re Application for Pen Register and Trap/Trace Device With Cell Site Location Authority*, 396 F. Supp. 2d 747, 757 (S.D. TX. 2005) ("[A] cell phone user may very well have an objectively reasonable expectation of privacy in his call location information.").

While Congressional enactment cannot trump constitutional analysis, it can shed light on society's views at the time the law was passed. As mentioned, Congress viewed acquisition of prospective CSLI as more intrusive than acquisition of the telephone numbers and other information available with a pen register when it passed CALEA in 1994. 47 U.S.C. § 1002(a)(2)(B). *See generally*, Freiwald, *Uncertain Privacy* (describing the debates that culminated in CALEA). Because, as I next argue, there is no reason to protect historical CSLI less than prospective CSLI, Congress' judgment in CALEA further supports an objective expectation of privacy in CSLI. Moreover, because CSLI has become more comprehensive, it has become only more intrusive over time.

C. Historical CSLI Should Enjoy the Same Fourth Amendment Protection as Prospective CSLI

Law enforcement acquisition of records of CSLI, or historical data, should receive the same Fourth Amendment protection as acquisition of CSLI in real-time or prospectively. *See Alexander Opinion*, 509 F. Supp. 2d at 74 ("[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."). Arguments to the contrary are based either on outdated notions of the limited nature of stored information[22] or incorrect applications of constitutional precedents.

Ultimately, how the Fourth Amendment regulates a particular investigative method must turn on the method's intrusiveness and the likelihood that law enforcement agents will abuse it.[23] In fact, law enforcement acquisition of historical CSLI can intrude into personal privacy even more than acquisition of prospective CSLI. A law enforcement agent interested in prospective CSLI could get an order on August 1st to track the target's movements for three months, and on October 31st the agent would have 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. The length of time the target's cell phone generated records and the service provider stored 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 valuable and informative to law enforcement agents as prospective CSLI. Historical data may indicate with whom targets

[22] In fact, because law enforcement agents may wait mere seconds before real-time CSLI becomes historical, the distinction between the two types of data can be entirely arbitrary.

[23] I further discuss the factors relevant to Fourth Amendment regulation of government surveillance *infra* pages 25 to 30.

have met, where, and for how long. It may put targets at the scene of a crime at the time the crime was committed, and thereby refute the target's alibi that he was somewhere else. CSLI may also reveal patterns that themselves could be informative.[24] 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."). Because bad-faith actors can easily abuse CSLI to intrude into people's constitutionally protected private lives, the judicial oversight under the Fourth Amendment provides an essential safeguard.

Because law enforcement agents have been able to access electronic records of people's movements and conversations only relatively recently, the landmark Supreme Court cases have not meaningfully addressed stored data. *See, e.g.*, *Karo*, 468 U.S. at 707-10 (describing real-time monitoring of beeper's radio transmissions). The argument that historical CSLI is constitutionally unprotected boils down to the claim that it is an unprotected "third party record." *See* Government Brief at 20. I address that claim in the next part.

Meanwhile, some have looked to the greater protection Congress has afforded to communications in transmission as opposed to in electronic storage as evidence that stored CSLI lacks Fourth Amendment protection. *See, e.g.,* Government Brief at 11. That argument is unpersuasive. First and most importantly, whether acquisition of CSLI implicates the Fourth Amendment must be decided in the first instance by courts, and not by Congress. While Congress' judgment may be informative in some cases, it should be least helpful when Congress has not meaningfully updated the pertinent statutory scheme since 1986. *See*18

[24] Even imprecise CSLI could indicate where a target lives or at least spends her evenings, and where she works or at least spends her days.

U.S.C. §§ 2701-2709, 2711-2712, Stored Communications Act ("SCA"). Moreover, the SCA concerns itself largely with communications rather than with CSLI. Federal legislators failed to address historical CSLI clearly in 1986, likely because, at that time, there were only about 1,500 cell sites in operation for about 680 thousand American subscribers. Today, the issue is much more pressing as there are more than 213,000 cell sites used by over 255 million subscribers.[25] Though Congress has yet to address acquisition of historical CSLI explicitly, it has not cast doubt on its protection under the Fourth Amendment.

II. THE GOVERNMENT DOES NOT ADVANCE A COMPELLING REASON TO VIEW ACQUISITION OF CSLI AS NOT A SEARCH

A. The "Third Party Rule" Does not Govern Acquisition of CSLI

The Court should decline the Government's invitation to extend the holding in *United States v. Miller*, 425 U.S. 435 (1976), that bank customers had no reasonable expectation of privacy in their bank records stored with the bank, to CSLI. The Government over reads *Miller* to posit a broad "third party rule" under which users forfeit constitutional protection of those things they voluntarily share with third parties.

Most importantly, and as discussed, a thorough analysis reveals that users have a reasonable expectation of privacy in their CSLI, which contradicts a simplistic application of a third party rule.[26] In addition, if the third party rule were as broad as the government claimed, then any "third party" provider access to users' data would defeat those users' reasonable expectations of privacy. That version of the third-party rule would run headlong into *Katz* which established that users maintain a reasonable expectation of privacy in their

[25] CTIA Survey at 2.

[26] *See* Freiwald, *First Principles* at ¶¶36-49 (criticizing courts' tendency to adopt shortcuts like "a third party rule" rather than conduct a reasonable expectations of privacy analysis).

telephone calls, despite telephone employees' technical ability to monitor those communications. *Katz*, 389 U.S. at 353. Just last month, the 9th 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").

The *Miller* court did not announce a rule that any time a customer uses an intermediary in his communications or his activities, he forfeits an expectation of privacy. If it had, there would be no expectation of privacy in internet communications, which take place entirely through "third party" intermediaries. *See, e.g., Long*, 64 M.J. 57; *United States v. Maxwell*, 45 M.J. 406 (C.A.A.F. 1996); *see also Karo*, 486 U.S. at 716 n.4 ("There would be nothing left of the Fourth Amendment right to privacy if anything that a hypothetical government informant might review is stripped of constitutional protection.")

The Supreme Court did find that Miller had voluntarily shared his banking information with the bank, and thereby waived his reasonable expectation of privacy in it. That aspect of *Miller's* reasoning has been the subject of much criticism. *See, e.g.*, Patricia L. Bellia and Susan Freiwald, *Fourth Amendment Protection for Stored E-mail* (Forthcoming, University of Chicago Legal Forum) (available at http://ssrn.com/abstract=1143038). By using the precedents it did, the *Miller* Court analogized the bank to the intended recipient of the bank customer's communication, or the second party to it, when the bank actually acted as

a third party intermediary between the customer and those with whom he transacted. *See Miller*, 425 U.S. at 443. If the bank is a third party, then it does not make sense to apply the second party rule and to view the depositor as having voluntarily confided in the bank in the same way one voluntarily confides in one's friends. *See Hoffa v. United States*, 385 U.S. 293, 302 (1966) (reasoning that "no interest legitimately protected by the Fourth Amendment [was] involved" because the Fourth Amendment does not protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it"). *Miller's* shaky foundation makes it a poor case to extend to the CSLI context.

While it seems unlikely that Miller voluntarily assumed the risk that the bank would disclose information about his banking transactions, it is even less likely that cell phone users voluntarily assume the risk that their cell phone companies will disclose CSLI, when, as the government admits, cell phone users do not even know the information the cell phone company is recording and have never had possession of it. *See* Government Brief at 20. The government relies on *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979*),* to support its claim that one cannot expect privacy in information voluntarily turned over to third parties. Again, there is no third party rule as broad as the government implies. *See* Bellia and Freiwald, *Fourth Amendment Protection*, at 27-38 (demonstrating that the case law refutes a broad third party rule). In addition, in finding that telephone users voluntarily conveyed the telephone numbers they dialed and assumed the risk of their disclosure, the *Smith* Court went to great lengths to establish that telephone users were aware the telephone companies had and retained a listing of all telephone numbers dialed. *Smith*, 442 U.S. at 742-43 ("Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company

does in fact record this information for a variety of legitimate business purposes."). The government's claim that "it makes no difference if some users have never thought about how their cell phones work," Government Brief at 21, does not square with its claim that users assume the risk their CSLI will be disclosed, because one cannot voluntarily convey information one is not aware one is conveying.

B. CSLI Is Much Richer than Telephone Numbers or Bank Records

Acquisition of CSLI differs markedly from those investigative techniques, such as acquiring dialed telephone numbers and bank records, which the Supreme Court found not to constitute Fourth Amendment searches in the 1970's. Users have a reasonable expectation of privacy in CSLI, whether it has been generated before the government's request as historical data or afterwards as prospective data.

As discussed, to the extent the government acquires CSLI that differs from the records service providers would keep in the ordinary course of their businesses, *Miller* would not apply. *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).[27]

Even if CSLI does show up in provider records, it more closely resembles the private communications that the *Miller* Court found subject to a reasonable expectation of privacy then the "business records" of the cell phone company. *See Miller*, 425 U.S. at 442 ("The checks are not confidential communications but negotiable instruments to be used in

[27] To the extent cell phone providers retain CSLI in response to law enforcement desires rather than for their own business purposes, CSLI should not be considered "business records" used in the ordinary course. *See Miller*, 425 U.S. at 442 ("All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the bank and exposed to their employees in the ordinary course of business.").

commercial transactions."). While not the content of communications, CSLI nevertheless indicates significant information about users' private lives. Information that reveals where users go and how long they spend there, and which includes information about what they do at home, differs significantly from the bank documents at issue in *Miller*.

Similarly, the information that a pen register revealed at the time of *Smith v. Maryland* was much more limited and therefore less revealing than CSLI. *United States v. New York Telephone*, 434 U.S. 159, 167 (1977) (explaining that pen registers did not indicate "the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed"). Here, CSLI provides intrusive information about the whereabouts of a user which directly implicates his right of privacy. Beyond its "limited capabilities," the pen register at issue in *Smith* could acquire information only after the government installed it, i.e., prospectively or in real time. *See Smith*, 442 U.S. at 742 (describing "search" question as "resting on claim" of a reasonable expectation of privacy "regarding the numbers he dialed on his phone"). As mentioned, historical CSLI includes information about past travels and activities for whatever period of time the provider retains it. Only the particularity and probable cause requirements of the Fourth Amendment can prevent the government from fishing through potential vast amounts of location data, in clear violation of constitutional principles.

III. ACQUISITION OF CSLI REQUIRES THE SAME EXTENSIVE JUDICIAL OVERSIGHT AS WIRETAPPING

The Supreme Court has established that some investigative practices, such as wiretapping and eavesdropping, create such a significant risk of executive branch overreaching at the expense of constitutionally protected privacy rights that law enforcement agents may not use them without even greater judicial involvement than that provided by the

warrant requirement. Several Courts of Appeal have recognized that government use of silent video surveillance requires, as a matter of constitutional law, the same heightened oversight. Because government acquisition of CSLI shares those same features of wiretapping, eavesdropping, and video surveillance that call for greater judicial oversight, it too should be subject to the same heightened procedural protections as those more established practices.

A. Electronic Surveillance that is Hidden, Intrusive, Indiscriminate and Continuous must be Subject to More Demanding Procedural Hurdles

In *Berger*, the Supreme Court explained that electronic surveillance techniques, such as the electronic eavesdropping at issue in that case, required higher levels of judicial involvement than that associated with traditional search warrants. *See Berger v. New York*, 388 U.S. 41, 60 (1967) (discussing how eavesdropping, with its "inherent dangers," required more "judicial supervision" and "protective procedures" than "conventional" searches). In imposing those same enhanced procedural requirements on the government's use of silent video surveillance, several federal Courts of Appeal elaborated on what features of electronic surveillance necessitated heightened judicial involvement to meet Fourth Amendment requirements. Judge Posner, in a decision for the 7th Circuit whose reasoning was widely followed, explained that the hidden, intrusive, indiscriminate, and continuous 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 Surveillance: Remembering the Lessons of the Wiretap Act*, 56 Ala. L. Rev. 9, 789-80 (2004) (discussing cases and requirements). As a result, before engaging in wiretapping, bugging, or video surveillance,

law enforcement agents must overcome the rigorous procedural hurdles codified in the Wiretap Act, 18 U.S.C. §§ 2510-22. Those include the particular description, minimization, limited duration, and use only as last resort requirements. See *Torres*, 751 F.2d at 883-84 (finding core provisions of the Wiretap Act to be required by the Fourth Amendment).

B. Acquiring CSLI is Hidden, Intrusive, Indiscriminate and Continuous Just Like Wiretapping

Executive branch acquisition of cell-site location data also constitutes the type of electronic surveillance that requires the most rigorous judicial oversight. When law enforcement agents acquire CSLI, whether the data is historical or prospective, they conduct electronic surveillance that is hidden, intrusive, indiscriminate and continuous.

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 is acquiring or has acquired his CSLI. As in the wiretapping and video surveillance contexts, it could compromise the investigation to give notice beforehand. Failure to give notice at any time, however, significantly raises the risk that agents will exceed the scope of a proper investigation with impunity. Under the Wiretap Act, the judge who granted the wiretapping order must provide an inventory to the target and may even provide transcripts and other records of the investigation. *See* 18 U.S.C. § 2518(8). After-the-fact notice provides a mechanism for targets to raise claims of improper surveillance. Because it may take place without the target ever finding out, government acquisition of CSLI should be subject to the same protective requirements.

As already discussed, law enforcement acquisition of CSLI has the potential to be extremely intrusive in that it may disclose a detailed record of the target's movements and

activities. Uninvited and virtually constant government observation of one's movements implicates constitutional privacy rights, the right to travel, and First Amendment rights of association and expression. Acquisition of the rich information available from CSLI, though different from that available from wiretapping and video surveillance, shares the intrusive character of those other surveillance methods. Because of that, it must be subject to heightened requirements so that the government does not needlessly intrude on valuable privacy rights.

Acquisition of CSLI is inherently indiscriminate in that much of the CSLI acquired will not be incriminating. Just as the wiretapping of traditional telephone calls acquires non-incriminating conversations and video surveillance footage includes numerous innocent scenes, CSLI may reveal many movements and activities that are entirely unrelated to criminal actions. The risk of acquiring information about non-incriminating activities justifies substantial judicial oversight of wiretapping, bugging, and video surveillance to reduce unwarranted invasions of privacy and to ensure that searches not become government fishing expeditions. Because CSLI also contains significant non-incriminating information, acquisition of it should be subject to those same heightened constraints.[28]

Finally, 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. To address that risk, the Supreme Court required that electronic surveillance orders issue for a limited period of time, and cease as soon as the constitutional justification ceases. To apply for a renewal, agents must satisfy the same requirements as those imposed

[28] *See also supra* pages 6 to 10 (discussing current practice of acquiring CSLI pertaining to mere associates of suspects).

on initial requests. *See Berger*, 388 U.S. at 59. Because CSLI also covers a period of time, its acquisition should be subject to the same limits.

As the preceding discussion shows, acquisition of CSLI shares the same features of wiretapping, bugging and video surveillance that make those investigative methods particularly invasive and particularly subject to abuse. In recognition of that and as a matter of constitutional law, courts must impose on those agents who seek CSLI the same requirements as those imposed on agents seeking to wiretap or conduct video surveillance. Adherence to those requirements must be checked in a hearing granted to the target of the surveillance to ensure that agents do not acquire CSLI in violation of constitutional safeguards.

C. Properly Circumscribed Surveillance of Historical CSLI Could Proceed Upon a Probable Cause Warrant Instead of a Wiretap-Type Warrant

A properly limited request for historical rather than prospective CSLI may reduce the need for judicial oversight from the level attendant to wiretapping to a standard search warrant. That is not because historical CSLI does not implicate the Fourth Amendment, but rather because a properly constructed request could minimize the extent to which acquisition of historical CSLI is hidden, intrusive, indiscriminate, and continuous.

First, because historical data would not be compromised by notice given after the records are created but before they are disclosed to law enforcement agents, law enforcement agents could give prior notice to targets that would make the investigation less hidden. At a prior hearing, to which the target is given notice, a judge may also require, subject to later review, that agents acquire records pertaining to a narrowly defined area and as to a particular subject, for which and as to whom they have probable cause. If the order is so narrowed, then

it will be significantly less intrusive and indiscriminate than an order to acquire all CSLI going forward. Similarly, a request for CSLI that is limited to a particular moment in time, or a short period, would be less continuous than unrestricted data acquisition. Subject to these limits, acquisition of historical CSLI could well proceed pursuant to a search warrant. When access to historical CSLI is not subject to these limits, however, it should proceed only after law enforcement agents satisfy the procedural hurdles imposed in conventional wiretap investigations. As discussed, because it is easy to gather CSLI for a long period, it may be even more intrusive and indiscriminate than prospective CSLI.

IV. CONGRESS COULD NOT ELIMINATE THE NEED FOR A WARRANT TO ACCESS CSLI

Although the proper construction of several potentially applicable statutes has most occupied the judges reviewing government access to CSLI, this brief has focused on the constitutional analysis. For if the Fourth Amendment does regulate access to prospective and historical CSLI, the statutory analysis may proceed quite simply. Either courts may construe the SCA to meet Fourth Amendment requirements, or its offending provisions must be struck down.

To meet Fourth Amendment standards, the SCA would have to require, at the least, a probable cause warrant before law enforcement may access historical CSLI. As discussed, targets must be given notice, an opportunity to contest, and a real remedy for improper investigations to satisfy the constitutional requirements. Construing the SCA in that manner would mean affirming the denial of the government's application in this case, because the government did not establish probable cause that the information it sought would reveal evidence of a crime. Law enforcement agents should have to establish at least that much before they obtain information that reveals where a target has been and how long she has

spent there.

If the SCA necessarily permits access to CSLI upon less than what the Fourth Amendment requires, then the Court must find it to be unconstitutional. Not only is it up to the courts, and not Congress, to ensure that executive branch investigations meet Fourth Amendment requirements, but the Fourth Amendment itself was passed in part to ensure that Congress not grant government agents excessively intrusive powers of investigation. *See* Tom Y. Davies, *Recovering the Original Fourth Amendment*, 98 Mich. L. Rev. 547, 619-68 (1999); *see also Berger*, 388 U.S. at 64 (striking down a New York statute that did not impose adequate Fourth Amendment safeguards on law enforcement eavesdropping and thereby amounted to an unconstitutional general warrant).

While the government will surely complain about the loss of warrantless access to information it believes it is entitled to have, that is no reason to uphold the practice. As the Supreme Court has recognized, it "could not forgive the requirements of the Fourth Amendment in the name of law enforcement." *Berger*, 388 U.S. at 62.

CONCLUSION

CSLI may provide an essential tool to government agents engaged in law enforcement. Just as with wiretapping, video surveillance, and conventional searches, however, acquisition of CSLI must be subject to Fourth Amendment safeguards, because users have a reasonable expectation of privacy in their CSLI, whether the data is prospective or historical. When government agents acquire CSLI, they so do in a manner that is hidden, intrusive, indiscriminate and continuous and therefore must be subject to the core protections of the Wiretap Act that impose greater procedural hurdles than a probable cause warrant. To the extent agents reduce those problematic features by requesting a severely circumscribed

investigation of historical CSLI for a particular subject, over a limited time period and with prior notice to the target, a traditional search warrant may suffice. Law enforcement may certainly acquire CSLI, but not in ways that flout the Fourth Amendment.

Respectfully submitted

Date July 31, 2008 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 hereby certify that on July 31, 2008, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification to the appropriate parties.

s/ Susan Freiwald