NACDL White Paper:

Electronic Surveillance & Government Access to Third Party Records

NACDL Fourth Amendment Committee

(Approved by the NACDL Board of Directors

February 19, 2012)

Introduction[*]

The past twenty-five years have brought dramatic advances in information and communication technologies, from the birth of the World Wide Web and the widespread use of personal computers, cell phones, personal satellite navigation systems, and other "smart" handheld and tablet electronic communication devices. Such developments have fundamentally altered the way people work, communicate, and socialize, providing a level of convenience, efficiency, and access to information that was previously unimaginable. At the same time, the amount of private information amassed by third parties like Internet service providers (ISPs),[1] email providers,[2] cloud computing services,[3] and cell phone carriers has grown exponentially, creating a culture where this new technology has the potential to invade personal privacy through the creation, collection, and aggregation of such information. Unfortunately, changes in technology have outpaced the law and much of this information is accessible to law enforcement and other government agencies without a warrant based on probable cause.

Federal law governing the privacy of electronic communications has not been meaningfully updated in over twenty-five years and many federal courts have struggled to adapt Fourth Amendment jurisprudence to the realities of the digital age. Even the Supreme Court has acknowledged that "[i]t is not so clear that courts at present are on so sure a ground" and cautioned jurists to "proceed with care when considering the whole concept of privacy expectations in" electronic communication devices.[4]

Since the 1870's, a warrant has been required to read postal mail,[5] and since the Supreme Court's decision in *Katz v. United States*, a warrant has generally been required to wiretap

[*] NACDL would like to thank the Members of NACDL's Fourth Amendment Committee, former National Security Coordinator Michael Price, and 2011 summer intern Melissa Weeden for their contributions to this report.

telephone conversations.[6] However, under current law, email, text messages, and other electronic communication content do not receive this same level of protection. Until January 2012, GPS-tracking information was subject to review by law enforcement without any judicial supervision, even though such information may easily reveal associations, affiliations, practices, and preferences – ranging from the intimately personal to the political. [*]

In August 2011, the Executive Committee of the Board of Directors of the National Association of Criminal Defense Lawyers (NACDL) passed a resolution adopting the principle that law enforcement access to the content of private electronic communications and geolocation information should require a warrant supported by probable cause.[7] The Fourth Amendment is the appropriate starting point for assessing the limits on government access to these records, and its guarantees should not turn on the mode of communication, nor can they favor one medium over another. The Fourth Amendment protects private data, regardless of how it is stored or transmitted, provided an individual has a reasonable expectation of privacy in the use of that data. It is uncertainty over whether users have a reasonable expectation of privacy in electronic communications that is the biggest challenge in determining whether Fourth Amendment protections apply to the communications.

I. The Fourth Amendment and Third Party Records

The Fourth Amendment guarantees "the right of the people to be secure in their persons houses, papers, and effects, against unreasonable searches and seizure, shall not be violated, and no warrants shall issue, but upon probable cause. . . ."[8] The Fourth Amendment generally guides analysis of government acquisition of private information about a person. A search under the Fourth Amendment occurs when the government infringes on "an expectation of privacy that

[*] The impact of the Supreme Court's decision in *United States v. Jones* and its analysis of third party records are discussed more fully *infra* at page 17.

society is prepared to consider reasonable,"[9] which leads courts to a two part analysis, first determining if a person has manifested a "subjective expectation of privacy" in the object of the search and then determining if that expectation is "one that society is prepared to recognize as reasonable."[10] Again, uncertainty regarding a person's reasonable expectation of privacy in electronic communications—and the third party records generated by way of such communications—is an issue currently being considered by U.S. courts.

Third party records are records that are created and stored by private companies in the ordinary course of business. Banking information and telephone call information are two traditional examples of third party records. In *Miller v. United States* and *Smith v. Maryland*, the Supreme Court held that individuals have no reasonable expectation of privacy in such records due to the fact that they are maintained by and accessible to a third party such as the bank or telephone company.[11] The Court found that people waive their "reasonable expectation of privacy" when they provide information to a third party, and consequently, law enforcement access to these records is not a violation of the Fourth Amendment's warrant requirement.[12] By revealing one's affairs to another, reasoned the Court, a person "assume[s] the risk" that the company would reveal that information to the government.[13] Known as the "third party doctrine," this rule holds true even when individuals reveal information on the assumption that the third party will not betray their confidence.[14] As discussed later in this memorandum, the viability of the "third party doctrine" may be in question in light of the Supreme Court's recent decision in *United States v. Jones*.

Today, however, third party records include far more than banking information or a list of telephone numbers dialed. They include copies of all email messages, whether the user deleted them or not, geolocation information, and a record of every website one visits and the search

terms used to find those sites. These kinds of third party records—Facebook entries, SMS text messages, device locator records, keystrokes, etcetera—often generated without the user's knowledge—can reveal highly personal information. The types of third party records routinely created today were non-existent when the Court decided *Miller* and *Smith* and Congress drafted the Electronic Communications Privacy Act.

Law enforcement can often gain access to such information without a warrant, permitting agents to track one's physical location over time, learn his habits, monitor his political and religious activity, and stitch together an intimate portrait of his daily life based on information that one would reasonably expect to remain private.[15]

II. Statutes Governing Law Enforcement Access to Third Party Records

The Electronic Communications Privacy Act (ECPA), combined with a patchwork of statutes with differing legal standards—probable cause, reasonable suspicion, or a lesser standard—including the Stored Communications Act (SCA), sections of the USA Patriot Act and the Foreign Intelligence Surveillance Act (FISA), allows law enforcement access to a trove of personal information that individuals generate, often unwittingly, on a daily basis. Law enforcement may also rely on the Pen Trap Statute, and the Wiretap Act, to access third party records. These outdated statutes essentially allow law enforcement officials to undercut Fourth Amendment rights in the digital age.

a. The Electronic Communications Privacy Act and The Stored Communications Act

In 1986, Congress passed the Electronic Communications Privacy Act (ECPA) to prevent the "unauthorized interception of electronic communications" and "update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies."[16] ECPA was ahead of its time in many respects. Cell phone

and email use were in their infancy and commercial Internet traffic was six years away from congressional approval;[17] the first web browser would not be introduced until 1993.[18] It is an understatement to say that a lot has changed since 1986. Regrettably, ECPA has not changed. For all of its foresight, ECPA continues to afford greater protection to documents in a file cabinet than to emails stored on a server.[19] Also, ECPA does not provide for an exclusionary rule to prevent the admission of improperly gained evidence in a criminal trial.[20]

Title III of ECPA, known as the Stored Communications Act (SCA), provides a mechanism in Section 2703 through which law enforcement may obtain the contents of stored electronic communications, like email, from a third party service provider, such as America Online (AOL) or Comcast. When individuals use the Internet, they use these providers' computers to contact other computers, transmitting their private information to these third-party service providers. In other words, these providers allow an individual's private computer to contact other computers, and transmit the communications data to and from the parties.[21] The SCA also permits law enforcement to compel the production of detailed records and other information pertaining to those communications, aside from their contents. The SCA makes distinctions between types of information that can be collected—content vs. non-content—and how that information is stored—electronic communications service (ECS) vs. remote commuting service (RCS)).

The distinction between content information and non-content information is crucial to understanding the SCA, as the statute ascribes different privacy protections to each. Non-content information is defined as "a record or other information pertaining to a subscriber or customer of such service (not including the contents of communications)."[22] Non-content information is often referred to as "transactional information."[23] It includes records of a person's electronic

communication usage, such as the time of, parties to, and duration of the electronic communication.[24] It may also include email sender/address information, logs of account usage, mail header information, records of a person's visits to online locations, the length of time of those visits, and actions taken while on those sites.[25]

According to Title I of ECPA, the Wiretap Act, content information "includes any information concerning the substance, purport, or meaning" of a wire, oral or electronic communication.[26] The content of an email, for example, includes the subject line and any text contained in the body of the message. By contrast, logs of account usage, mail header information[27] (without the subject line) and lists of outgoing e-mail addresses sent from an account are traditionally considered non-content information.[28] In other words, content information is the substantive information that a person intends to communicate, while non-content information is the information about when and how the person communicates.[29]

The distinction between content and non-content information is logical, but as a consequence of technological advances over the last twenty-five years, it is often difficult to neatly separate the two. "Non-content" information can often reveal as much information about a person as can the contents of a particular communication.[30] For example, a search query string reveals the contents of communications because the search terms that a user inputs are part of the URL.[31] A subpoena for transactional records will reveal the words that a person searches for online, which most certainly will reveal "…information concerning the substance or meaning of that communication." [32] "The 'substance' and 'meaning' of the communication is that the user is conducting a search for information on a particular topic."[33]

Not only did Congress distinguish between content and non-content information, it also distinguished between computer functions by creating the categories of "electronic

communication service" (ECS) and "remote computing service" (RCS), responsible for storing and remotely processing data.[34] Congress established different rules in the SCA for each category. According to the 1986 statute, a company provides a customer with ECS when it temporarily stores an electronic communication when it sends and receives communications, such as an email.[35] For instance, ". . . when an email sits unopened on an ISP's server, [such as Comcast,] the ISP is acting as a provider of ECS with respect to that email."[36] On the other hand, a company provides a customer with RCS when the customer outsources a computing task, like the creation of a spreadsheet or paying a remote computer to store extra files.[37] For instance, if the author of a document sends that document to a ". . . commercial long-term storage site for safekeeping, that storage site is acting as an RCS with respect to that file."[38] Of course, today, however, home computers are well equipped to process their own spreadsheets and other data and the proliferation of "cloud"-based providers, such as Google Docs, both convey and store electronic communications. Consequently, the difference between an ECS and an RCS has become obsolete. Unfortunately, the SCA has not been meaningfully amended since 1986, and so the ECS and RCS categories remain frozen in law.

In order to understand the application of Section 2703 to electronic communications, one must first know if the government is seeking content or non-content information from an ECS or RCS provider. If the information sought by the government is not covered by an RCS or ECS, in other words, the information is stored on an individual's home computer, then the SCA does not apply and only the Fourth Amendment, and therefore all of its exceptions, applies.[39] The SCA requires a warrant based on probable cause for the government to require an ECS provider to disclose the contents of an electronic communication that it has held in electronic storage for 180 days or less.[40] However, the government has three different options it may use to require an ECS

provider to disclose the contents of an electronic communication it has held in electronic storage for more than 180 days *or* an RCS provider to disclose the contents of an electronic communication it has stored—without regard to the number of days it has stored such communication.[41] First, the government may use a warrant based on probable cause.[42] Second, the government can provide notice to the subscriber and use an administrative subpoena.[43] Third, the government may provide notice to the subscriber and obtain a court order, known as a 2703(d) order, based on "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication . . . are relevant and material to an ongoing criminal investigation."[44]

With respect to non-content information—"record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)"—the government has four options it can use to require an ECS or an RCS to disclose such records.[45] It may use a warrant based on probable cause, a 2703(d) order, consent of the subscriber or customer, or a formal written request relevant to an investigation concerning telemarking fraud for limited information.[46] Finally, the government may use an administrative subpoena, without prior notice to a subscriber, to access the name, address, local and long distance telephone connection records, length and types of service, telephone number, and means and source of payment for such service.[47]

Courts have held that a person has no expectation of privacy in subscriber information and, therefore, a lesser showing is required of law enforcement to obtain the information.[48] With an administrative subpoena, therefore, only the recipient of the subpoena, meaning the third party company, has cause to challenge the subpoena. Recently, Twitter challenged a government

subpoena served to obtain the record information of people suspected to be members of WikiLeaks.[49]

The distinction between emails 180 days old and 181 days old reflects Congress' understanding of email as it existed in 1986. Congress assumed that people would check their email by downloading it to their computers, thereby removing it from the company's server. If a message remained on the server for 180 days, Congress assumed it was abandoned.[50] Consequently, Congress allowed the government to access the contents of the message under a lesser legal standard. This is completely inconsistent with the way email is used today, as it is often checked multiple times per day but is stored on a provider's server indefinitely. Today, the vast amount of inexpensive (or free) digital storage space has eliminated the need for computer users to clean out their email boxes.[51]

1. SCA jurisprudence regarding email

Forced to contend with a 1986 model of electronic communications, judges have had to stretch the meaning of the SCA to apply to the types of electronic communications we use today, applying it to communications and situations it was never meant to govern. For example, in *United States v. Weaver,*[52] the court undertakes a complicated analysis to decide if an email that was already opened in a Hotmail account, yet continued to be stored on the Hotmail server for less than 181 days, could be accessed by only a subpoena.[53] The court reasoned that the ISP acted as both an electronic communication service and a provider of remote computing services—as an ECS when it held the emails in intermediate storage before they were opened and as an RCS by storing the emails after they were opened.[54] Therefore, the court found that the opened emails could be obtained by a subpoena under section 2702(a)(2).[55]

However, compare *Weaver* to the Sixth Circuit's ruling in *United States v. Warshak*, holding that "a subscriber enjoys a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial ISP'" regardless of their age.[56] The court further held that "[t]he government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause."[57] To the extent that the SCA says otherwise, the Sixth Circuit declared it is unconstitutional.[58] The court reasoned that email and other traditional forms of communication, like tangible mail, are so similar that it would "defy common sense to afford emails lesser Fourth Amendment protection," comparing an ISP to a post office.[59]

Nonetheless, in other circuits around the country, information that should receive the same Fourth Amendment protection is available to law enforcement without a warrant or any judicial oversight due to the outdated SCA. Indeed, a great deal of the information stored or conveyed by third party providers does not receive the degree of protection that users expect. The fact that electronic communications utilize a third party's network or must be transmitted with the aid of a service provider should not eliminate an individual's reasonable expectation of privacy in their contents, nor should it give the government free reign to demand detailed logs of the location information required to send and receive such data.

2. SCA's application beyond email

Electronic communication in the form of email is the main mode of electronic communication that Congress had in mind when it created the SCA, but over time, the SCA has been interpreted to cover other types of electronic communication as well. Now, there are many forms of electronic communication, including posts on electronic bulletin boards, which include public and semi-public messages on social networking websites such as Facebook and MySpace.

A completely public bulletin board, like a public blog, is not protected under the SCA.[60] However, a semi-private or completely private bulletin board like Facebook or MySpace provides an electronic communication service.[61] Public messages on Facebook and MySpace have been interpreted by courts to be in electronic storage because the user chose not to delete it, causing the website to store it. Therefore, posts on sites like Facebook and MySpace are governed by the same rules as emails, which are also in electronic storage.[62]

Although it seems logical to protect Facebook and MySpace communications in the same way that email is protected, there is some dispute about the reasonable expectation of privacy in these posts. One court has held that there is no expectation of privacy in materials posted on Facebook and MySpace because the user chose to share the information with other people.[63] However, it has also been argued that a person who uses a website's password protection option on these semi-public sites *does* have a reasonable expectation of privacy in the contents of the website because the user was allowed to choose his privacy settings and choose who could see his private page.[64] Following this theory, the user has an expectation of privacy that no one other than designated persons will be able to see the information posted on these websites. Recent news reports indicate that law enforcement officials have been using warrants to obtain content information from a person's private Facebook profile.[65]

b. Section 215 of the Patriot Act

The issue of data collection by third parties has become even more relevant with the creation and reauthorization of Section 215 of the Patriot Act—the "Business Records" provision.[66] Section 215 authorizes law enforcement to seek orders from the Foreign Intelligence Surveillance Court (FISC) for business records and other "tangible things," such as books, Internet history, driver's license records, and hotel records.[67] The legal standard for this

court order is far less than probable cause, requiring only a showing that there are "reasonable grounds to believe" that the records being sought are relevant to "an authorized investigation . . . to protect against international terrorism or clandestine intelligence activities."[68] Section 215 orders fall under the "third-party doctrine." Although lacking a warrant requirement, several courts have held that Section 215 does not violate the Fourth Amendment.[69]

Emails, opened and unopened, new or old, are all treated the same when collected as part of a foreign intelligence investigation. The Patriot Act allows the collection of all business records, and the Foreign Intelligence Surveillance Act does not expressly address communications in storage. Therefore, any email, whether stored or not, if it is found to be a business record, is available to the government with a court order upon a showing that law enforcement officials have reason to believe that the information in the email is relevant to foreign intelligence operations.[70]

A Justice Department decision, which is not available to the public, is rumored to give the government authority to obtain these records in a way that is broader than the text of the bill.[71] In 2009, a Justice Department Official, while testifying before Congress regarding reauthorization of Section 215, stated that Section 215 "supports an important sensitive collection program."[72] The details of this program are publicly unknown because how the executive branch interprets Section 215 and other sections of the Patriot Act is classified. Since 2009, U.S. Senators have been pushing the Obama administration to declassify its interpretation of Section 215.[73] However, the administration has failed to release a statement regarding what information is being collected and how it is being used. During floor debate in 2011 on reauthorization of the Patriot Act, Senator Ron Wyden stated "when the American people find

out how their government has secretly interpreted the Patriot Act, they will be stunned and they will be angry."[74] This information remains classified.

c. National Security Letters

National Security Letters (NSLs) have become the most controversial of all of the Patriot Act provisions. The Patriot Act expanded NSL authorities under the Right to Financial Privacy Act,[75] which is used to compel production of records from "financial institutions," and ECPA,[76] which is used to compel telephone and Internet records.[77] NSLs have become a broad and compulsory tool similar to administrative subpoenas that law enforcement can use to gather information about Americans from third-parties.[78] "In their current form, NSLs need only certify that the records sought are relevant to an authorized investigation."[79] NSLs allow law enforcement to obtain from communications companies "financial records, consumer credit reports and telecommunications transactional records without judicial authorization."[80] Communications companies include traditional communications companies such as phone and Internet providers, but they also include any company that provides online services that give people "the ability to send messages or communications to third parties."[81] This includes companies such as Facebook, Gmail, or AOL, which provide instant messaging services.[82]

"Once information is obtained in response to a national security letter, it is indefinitely retained and retrievable by the many authorized personnel who have access to various FBI databases,"[83] whether or not the information obtained is used against an individual in a criminal prosecution.

d. Wiretap Act and Pen Register/Trap Trace Statute

In addition to the Stored Communications Act, the Electronic Communications Privacy Act also amended the Wiretap Act and the Pen Register/Trap Trace statute. Title I of ECPA is

the Wiretap Act and governs the interception of electronic communications.[84] It allows law enforcement to collect content material of communications and obtain permission to intercept wire, oral or electronic communications through a court order based on probable cause.[85] In order to obtain a wiretap order, the government must demonstrate that there is probable cause to believe that a crime was or is being committed, that the communication is relevant to that crime, that normal investigative procedures have been tried but have failed, and the location from which the communication is made is connected to the crime.[86] Some have called this the "super-warrant" requirement.[87]

Title II of ECPA is the Pen Register/Trap Trace statute. It governs the collection of phone numbers dialed and numbers of incoming calls.[88] The legal standard for obtaining an order to use a pen register or trap and trace device is less than probable cause and less than reasonable suspicion, requiring the government to certify only "that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."[89] However, the statute expressly prohibits the use of either tool "in a manner so as to constitute a 'tracking device.'"[90] In order to use these instruments as tracking devices, the government must show probable cause.[91]

Each of the foregoing statutes was designed to address the collection of a type of data in existence at the time of its passage. The evolution of data types and storage technology has rendered the statues largely obsolete.

III. Geolocation Information

Recently, the collection of location information by law enforcement has become the most heavily publicized of the categories of electronic communication collected by third parties. In 2011, the Supreme Court granted certiorari and heard oral argument regarding the

constitutionality of GPS tracking by law enforcement officials in *United States v. Jones*, a case involving the placement of a GPS locator on a suspect's car by police officers without a valid warrant.[92] The Court issued its ruling in January 2012, holding that the use of the GPS locator in *Jones* constitutes a search in violation of the Fourth Amendment.[93]

In the private sector, Apple and Google both exposed themselves to controversy in 2011 when it was discovered that the companies' smartphones were gathering information about user location and sending it back to Apple and Google.[94] Cell phones and mobile Internet devices like smartphones and tablets constantly generate location data that can be intercepted in real time.[95]

There are conflicting decisions about what is needed to obtain location information from cell phone providers and the use of GPS tracking devices.

a. Cell-phone surveillance

The SCA, discussed supra, does not clearly specify a standard for government access to cell phone location information and excludes from its provisions "any communication from a tracking device,"[96] which is defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object."[97] A majority of jurisdictions have held that a cell phone is a "tracking device," rendering the SCA inapplicable to cell phone location information.[98] To collect real time or prospective cell site data, a majority of published decisions require the government to show probable cause.[99]

b. GPS surveillance

Prior to the Supreme Court's ruling in *Jones*, Circuit courts were split over the question of whether law enforcement could attach a GPS tracker on a suspect's car without a warrant or judicial approval.[100] Most courts held that such GPS surveillance did not require a warrant

because a person has no expectation of privacy in their public movements—that is, it was not a "search."[101] However, in *United States v. Jones*, a unanimous Supreme Court applied the warrant requirement, reasoning that

> The Fourth Amendment provides in relevant part that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." It is beyond dispute that a vehicle is an 'effect' as that term is used in the Amendment. We hold that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.' It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a "search" within the meaning of the Fourth Amendment when it was adopted.[102]

The majority opinion did not apply the *Katz* reasonable expectation of privacy test, noting that *Katz* did not supersede the Court's trespass jurisprudence, but instead added to it.[103] However, five Justices, while ultimately agreeing with the majority's holding, felt that the majority could have gone further and applied the *Katz* reasonable expectation of privacy test in addition to the trespass analysis.[104] In fact, Justice Alito would have applied the privacy test instead of the trespass analysis stating that "the Court's reliance on the law of trespass will present particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact with the item to be tracked."[105]

In her concurrence, Justice Sotomayor discussed the reasonable expectation of privacy standard, but determined that "[r]esolution of these difficult questions in this case is unnecessary, however, because the Government's physical intrusion on Jones' Jeep supplies a narrower basis for decision."[106] She did raise concerns, however, about surveillance that does not require a trespass and law enforcement access to third party records.[107]

> [A]s Justice Alito notes, physical intrusion is now unnecessary to many forms of surveillance. With increasing regularity, the Government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-

> installed vehicle tracking devices or GPS-enabled smartphones. In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance. But '[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis.'[108]

Further, Justice Sotomayor questioned the use of the third party doctrine in the digital age and suggested that it may be time to reconsider *Smith* and *Miller*.[109]

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. E.g., *Smith*, 442 U.S., at 742, *United States v. Miller*, 425 U.S. 435, 443 (1976). This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as Justice Alito notes, some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable," and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[110]

NACDL filed an *amicus* brief in *Jones*, arguing that warrantless GPS surveillance imposes an unacceptable burden on First Amendment associational rights, as well as Fourth Amendment privacy rights. NACDL further argued that the warrant requirement is minimally burdensome, and, therefore, a warrant based on probable cause should be required for law enforcement to use a GPS tracking device.[111]

IV. Execution of Warrants for Content of Communications

Even in cases where a warrant based on probable cause is issued, and the requirements of specificity and particularity in the application for the warrant and the particularity clause of the

warrant are met, there may be instances where law enforcement seeks more data than that for which it has probable cause. For example, in *United States v. Comprehensive Drug Testing, Inc.*, the government did just this, citing the "hazards" of retrieving data stored electronically, including the ability to disguise files with misleading names, the ability to hide data, and the ability to "booby trap" data, causing it to be deleted upon its discovery.[112] In these instances, it is important that the warrant specify how the data is to be handled, and establish procedures that must be followed in executing the warrant to ensure that information for which law enforcement does not have probable cause is not viewed by investigating case agents and is returned to the party on which the warrant has been served.[113] A warrant based on probable cause should not be interpreted as a gateway to access all electronic data within the system subject to the warrant. The "plain view exception" to the Fourth Amendment does not apply to overly broad requests for data for which the government does not have probable cause.

V. Policy Recommendations to Protect the Privacy of Electronic Communications

1. The content of any electronic communication that is sought by a law enforcement official should only be obtained through a warrant based on probable cause, adhering to the requirements for specificity and particularity in the application for the warrant, the particularity clause of the warrant, as well as the execution of the warrant.

2. The definition of "content" information should be amended to cover any information that will demonstrate the substance of an electronic communication, to include private emails, instant messages, text messages, word processing documents and spreadsheets, photos, Internet search queries and private posts made over social networks. This would include any information found in any third party records, including information stored within a cloud system, and transactional information that can reveal the content of an electronic communication, including a search query string, a URL, browser history and email subject lines.

3. Congress should amend the Electronic Communications Privacy Act (ECPA) and eliminate the RCS and ECS distinctions, and the 180 day "rule."

4. Law enforcement must be required to obtain a warrant based on probable cause to obtain prospective or retrospective geolocation information—whether by way of a third-party service provider, or by direct use of a GPS device to track a suspect's movements.

5. Opened email, even though found on a third-party service provider's server, should only be obtainable by way of a warrant based on probable cause.

6. Congress should statutorily extend the exclusionary rule to apply to searches that do not comply with these warrant requirements.

Conclusion

The protection of the Fourth Amendment should be extended to adequately protect the privacy of electronic communications. When the privacy statutes that govern the collection and acquisition of electronic communications were passed, the quantity and type of information gathered by third party companies was nowhere near as revealing of personal information as the records kept by third party companies are today. Given these developments, the third party doctrine is no longer consistent with reasonable expectation of privacy.

Currently, with merely a subpoena, a law enforcement official can learn countless details of a person's private life through the examination of Internet searches, email, and, until recently, geolocation information. The Fourth Amendment is meant to protect the government from gaining this type of detail without a warrant, regardless of the technology used to gather the information.

Requiring a warrant for location and content information strikes the proper balance between the needs of law enforcement while giving private information the protection it deserves. A simple rule requiring a warrant for this information also gives guidance to companies about when they must disclose subscribers' information.

[1] ISPs are companies that provide access to the Internet, such as Comcast and Verizon.

[2] Email providers include AOL Mail, Gmail, and Yahoo! Mail.

[3] Cloud computer services include Google Docs, Flickr, and Dropbox.

[4] City of Ontario v. Quon, 130 S.Ct. 2619, 2629 (2010).

[5] Ex parte Jackson, 96 U.S. 727, 733 (1877).

[6] Katz v. United States, 389 U.S. 347 (1967).

[7] NACDL Board Resolution of August 5, 2011 (http://www.nacdl.org/About.aspx?id=21156).

[8] U.S. Const. amend. IV.

[9] United States v. Jacobsen, 466 U.S. 109, 113 (1984).

[10] Smith v. Maryland, 442 U.S. 735, 740 (1979) (quoting *Katz*, 389 U.S. at 361).

[11] United States v. Miller, 425 U.S. 435, 443 (1976) ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."); *Smith*, 442 U.S. at 744-45).

[12] *Miller*, 425 U.S. at 443.

[13] *Smith*, 442 U.S. at 744.

[14] *Miller*, 425 U.S. at 443; *Smith*, 442 U.S. at 744.

[15] *See* United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) *aff'd sub nom*. United States v. Jones, 2012 WL 171117.

[16] S.Rept. 99-541, at 1 (1986).

[17] Miguel Helft and Claire Cain Miller, *1986 Privacy Law Is Outrun by the Web,* N.Y. Times, Jan. 9, 2011, *available at* http://www.nytimes.com/2011/01/10/technology/10privacy.html.; J. Beckwith Burr, *The Electronic Communications Privacy Act of 1986: Principles for Reform*, Digital Due Process 8, *available at* http://www.digitaldueprocess.org/files/DDP_Burr_Memo.pdf.

[18] Burr, *supra* note 17, at 8.

[19] Helft, *supra* note 17.

[20] Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 Md. L. Rev. 681, 681 (2011).

[21] Orin Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1209-1210 (2004).

[22] 18 U.S.C. § 2703(c)(1).

[23] Brian D. Kasier, Note, *Government Access to Transactional Information and Lack of Subscriber Notice*, 8 B.U. J. Sci. & Tech. L. 648, 650 (2002)

[24] *Id*.

[25] Kerr, 72 Geo. Wash. L. Rev at 1228.

[26] 18 U.S.C § 2510(8).

[27] Email header information is the information that travels with emails, including who sent the email, when the email was sent, from where it was sent and how it arrived and who is the receiver and how it was received. See Email Productivity Software, http://emailaddressmanager.com/tips/header.html (last visited Feb. 2, 2012).

[28] Kerr, 72 Geo. Wash. L. Rev. at 1228.

[29] *Id*.

[30] Lillian R. BeVier, Symposium: *The Communications Assistance for Law Enforcement Act of 1994: A surprising Sequel to the Break Up of AT&T*, 51 Stan. L. Rev. 1049, 1055 (1999).

[31] *In re* United States for an Order Authorizing the Use of a Pen Register and Trap on [xxx] Internet Service Account/User Name [xxxxxxx@xxx.com], 396 F.Supp.2d 45, 49 (D. Mass 2005).

[32] *Id*. (citing 18 U.S.C. § 2510(8)).

[33] *Id.*

[34] *See* 18 U.S.C. § 2703.

[35] 18 U.S.C. §2510(15).

[36] Kerr, 72 Geo. Wash. L. Rev. at 1216.

[37] *Id*. at 1213-14.

[38] *Id*. at 1216.

[39] *Id.* at 1213.

There is a lack of consensus regarding "cookies." "Cookies are small chunks of information that websites can put on your computer when you visit them. Among other things, cookies enable websites to link all of your visits and activities at the site. Since cookies are stored on your computer, they can let sites track you even when you are using different Internet connections in different locations. But when you use a different computer, your cookies don't come with you." (https://www.eff.org/wp/six-tips-protect-your-search-privacy). Some district courts have configured the SCA to regulate the placement of cookies on home computers by saying that home computers are a provider of electronic communication services. (*In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001); *In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272 (C.D. Cal. 2001)). However, one academic has argued that the information that is gathered from cookies is information that is on a home computer, which is already protected by the Fourth Amendment and its requirement of a warrant based on probable cause and is not within the purpose of the SCA. (*Compare,* Kerr, 72 Geo. Wash. L. Rev at 1214-15, *with DoubleClick*, 154 F.Supp.2d at 508 (Court assumes without deciding that information stored and gathered through cookies is in electronic storage)).

[40] 18 U.S.C. § 2703(a). "Electronic storage" is defined as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof, and any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17)(A) and (B).

[41] 18 U.S.C. § 2703(a)-(b).

[42] 18 U.S.C. § 2703(b)(1)(A).

[43] 18 U.S.C. § 2703(b)(1)(B)(i).

[44] 18 U.S.C. § 2703(d).

[45] 18 U.S.C. § 2703(c).

[46] 18 U.S.C. § 2703(c)(1)(A)-(D).

[47] 18 U.S.C. § 2703(c)(2).

[48] *See* United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010), United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008); Guest v. Leis, 255 F.3d 325, 335-336 (6th Cir. 2001), United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000).

[49] *In re* Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(d), No. GJ3793, 2011 WL 5508991 (E.D.Va. Nov. 10, 2011).

[50] Kerr, 72 Geo. Wash. L. Rev. at 1234.

[51] Joshua Gruenspecht, *"Reasonable" Grand Jury Subpoenas; Asking for Information in the Age of Big Data*, 24 Harv. J.L. & Tech. 543, 544-45 (2011).

[52] 636 F. Supp. 2d 769 (C.D. Ill. 2009).

[53] *Id*. at 770.

[54] *Id*. at 771-772.

[55] *Id.* at 773

[56] United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010).

[57] *Id*. at 288.

[58] *Id.*

[59] *Id.* at 285-86.

[60] Crispin v. Christian Audigier, Inc., 717 F.Supp.2d 965, 989 (C.D. Cal. 2010).

[61] *Id*.

[62] *Crispin,*717 F.Supp.2d at 989; *but see* Snow v. DirecTV, Inc. 2005 WL 1226158, at *3 (M.D. Fla. May 9, 2005) adopted by 2005 WL 1266435 (M.D. Fla. May 27, 2005), *aff'd on other grounds*, 450 F.3d 1314 (11th Cir 2006) (This information is not in electronic storage because the website on which they are posted is the final destination for the information).

[63] *See* Romano v. Steelcase Inc., 30 Misc.3d 426, 434, 907 N.Y.S.2d 650 (N.Y. Sup. Ct. 2010).

[64] 1 LaFave, Search and Seizure § 2.6 at 721 (4th ed. 2006).

[65] Reuters, *U.S. Law Enforcement Obtaining Warrants to Search Facebook Profiles*, FoxNews.com (July 12, 2011), *available at* http://www.foxnews.com/scitech/2011/07/12/us-law-enforcement-obtain-warrants-to-search-facebook-profiles/.

[66] 50 U.S.C. § 1861.

[67] 50 U.S.C. § 1861 (a)(1). *See also* https://www.eff.org/deeplinks/2011/10/ten-years-later-look-three-scariest-provisions-usa-patriot-act.

[68]50 U.S.C. § 1861(b)(2(a).

[69] United States v. Abu-Jihaad, 531 F.Supp.2d 299, 309 (D. Conn. 2008), *aff'd*, 630 F3d 102 (2d Cir. 2010); *In re Sealed Case*, 310 F.3d 717, 746 (2002)("[W]e think the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close. We, therefore, believe firmly, applying the balancing test drawn from *Keith,* that FISA as amended is constitutional because the surveillances it authorizes are reasonable."); United States v. Mubayyid, 521 F.Supp.2d 125, 137 (D. Mass. 2007).

[70] Julian Sanchez, *Leashing the Surveillance State: How to Reform the Patriot Act Surveillance Authorities*, Policy Analysis, May 16, 2011, 12-13 (2011), *available at* http://www.cato.org/pub_display.php?pub_id=13099.

[71]Mark Benjamin, *New Patriot Act Controversy: Is Washington Collecting Your Cell Phone Data?*, Time Magazine, June 24, 2011, *available at* http://www.time.com/time/nation/article/0,8599,207966,00.html?xid=fbshare.

[72] *Hearing on the USA PATRIOT Act*: *Before the Subcomm on the Const, Civ. Rights, and Civ. Liberties of the H. Comm. On the Judiciary*, 111th Cong. 9 (2009) (statement of Todd Hinnen, Deputy Assistant Attorney General, National Security Division, U.S. Department of Justice), *available at* http://judiciary.house.gov/hearingshear_090922.html.

[73] Press Release, Senator Ron Wyden, Senators Press Holder to Declassify Key Facts about Patriot Act (Nov. 17, 2009), *available at* http://wyden.senate.gov/newsroom/press/release/?id=dee00e95-6825-442a-bafe-ef66a84b2a86.

[74] Press Release, Senator Ron Wyden, In Speech, Wyden Says Official Interpretations of Patriot Act Must be Made Public (May 26, 2011), *available at* http://wyden.senate.gov/newsroom/press/release/?id=34eddcdb-2541-42f5-8f1d-19234030d91e.

[75] 12 U.S.C. § 3414.

[76] 18 U.S.C. § 2709.

[77] Sanchez, *supra* note 70 at 15.

[78] *Id*.

[79] *Id*. at 16.

[80] *Id*. at 15.

[81] *Id.* (citing U.S. Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence (2009) §3(B), available at http://www.cybercrime.gov/ssmanual/03ssma.html#B.1.).

[82] *Id*.

[83] U.S. Department of Justice, Office of the Inspector General, "A Review of the Federal Bureau of Investigation's Use of National Security Letters," 110, March 2007.

[84] 18 U.S.C. §§ 2510-2520.

[85] 18 U.S.C. § 2518.

[86] *Id*.

[87] Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 Nw. U. L. Rev. 607, 630 (2003).

[88] 18 U.S.C. § 3127 (3)-(4).

[89]18 U.S.C. § 3123(a)(1).

[90] 47 U.S.C. § 1002(a)(2)(B) ("except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of title 18), such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)").

[91] *See In re* Applications of the United States of America for Orders Pursuant to Title 18, United States Code, Section 2703(d) to Disclose Subscriber Information and Historical Cell Site Information for Mobile Identification Numbers: (XXX) XXX-AAAA, (XXX) XXX-BBBB, and (XXX) XXX-CCCC, 509 F. Supp. 2d 64, 68 (D. Mass. 2007) (citing 47 U.S.C. § 1002 (a)(2)(B) (2006)).

[92] United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010) *aff'd sub nom*. United States v. Jones, 2012 WL 171117.

[93] United States v. Jones, No. 10-1259, 2012 WL 171117, at *3 (U.S. Jan. 23, 2012).

[94] Julia Angwin and Jennifer Valentino-Devries, *Apple, Google Collect User Data,* Wall Street Journal (Apr. 22, 2011), *available at* http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html.

[95] *The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age*, *Before the S. Comm. On the Judiciary*, 111th Cong. 5 (2010) (statement of James X. Dempsey, Vice President of Public Policy Center for Democracy and Technology).

[96] 18 U.S.C. § 2711 (cross-referencing 18 U.S.C. § 2510 for definitions (18 U.S.C. § 2510 (12)(C))).

[97] 18 U.S.C. § 3117.

[98] *See In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747, 759 (S.D. Tex. 2005); *In re* Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Phone, 2006 U.S. Dist. LEXIS 11747, *2 (S.D.N.Y. 2006); *In re* Application of the United States of America for an Order Authorizing the Disclosure of Prospective Cell Site Information, 412 F. Supp. 2d 947 (E.D. Wis. 2006); *In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 294 (E.D.N.Y. 2005); *In re* Application of the United States of American for an Order (1) Authorizing the Use of a Pen Register and Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information, 384 f. Supp. 2d 562 (E.D.N.Y. 2005).

[99] *See In re* Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone, 2006 U.S. Dist. LEXIS 11747, *2 (S.D.N.Y. 2006); *In re* Application of the United States of America for an Order Authorizing Disclosure of Prospective Cell Site Information, 412 F. Supp. 2d 947 (E.D. Wis. 2006); *In re* Application for Pen Register and Trap/Trace Device With Cell Site Location Authority, 396 F. Supp. 2d 294 (E.D.N.Y. 2005); *In re* Application of the United States of American for an Order (1) Authorizing the Use of Pen Register and Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information, 384 F. Supp. 2d 562 (E.D.N.Y. 2005).

Some courts have adopted a hybrid theory advanced by the Department of Justice, holding that location information is accessible to the government in real time if it meets the standard for stored transaction information under § 2703(d). The hybrid theory uses both the Pen Register Statute and the SCA. A detailed discussion of this theory is beyond the scope of this white paper, especially because most jurisdictions have rejected it. *See, In re* Application of the United States for an Order (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; and (2) Authorizing Release of Subscriber Information and/or Cell-Site Information, 411 F. Supp. 2d 678, 680 (W.D. La. 2006); *In re* Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone, 460 F. Supp. 2d 448 (S.D.N.Y. 2006); Lisa M. Lindemenn, Note, *From Cell to Slammer: Flaws in the Hybrid Theory*, 53 Ariz. L. Rev. 663, 672 (2011).

[100] *Compare* United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010) (holding that a law enforcement agent must get a warrant based on probable cause before installing a GPS on a suspect's car because a person has a reasonable expectation that his constant movements are not exposed to the public), *with* Untied States v. Garcia, 474 F.3d 994 (7th Cir. 2007) (holding that law enforcement attaching a GPS to a suspect's car is not a search because a person has no reasonable expectation of privacy on a public street)

[101] *See Garcia*, 474 F.3d at 996; United States v. Marquez, 605 F.3d 604, 609-10 (8th Cir. 2010); United States v. Pineda-Moreno, 591 F.3d 1212, 1216 (9th Cir. 2010).

[102] *Jones*, 2012 WL 171117 at *3 (citation omitted).

[103] *Id*. at *5.

[104] *Id*. at *8 (Sotomayor, J., concurring) ("Of course, the Fourth Amendment is not concerned only with trespassory intrusions on property. Rather, even in the absence of a trespass, 'a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.'); *Id*. at *11 (Alito, J., concurring) ("I would analyze the question presented in this case by asking whether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove.")

[105] *Id*. at *15.

[106] *Id*. at *10.

[107] *Id*. at *9-10.

[108] *Id*. at *8 (citations omitted).

[109] *Id*. at *10.

[110] *Id*.

[111] Brief of The National Association of Criminal Defense Lawyers, et al. as Amici Curiae Supporting Respondent, United States v. Jones, No. 10-1259 (2010), *available at* http://www.nacdl.org/Advocacy.aspx?id=19557.

[112] United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1168 (9th Cir. 2010).

[113] *Id*. 1168-69.