SEARCHING THE CLOUDS

WHY LAW ENFORCEMENT OFFICIALS NEED TO GET THEIR HEADS OUT OF THE CLOUD AND OBTAIN A WARRANT BEFORE ACCESSING A CLOUD NETWORK ACCOUNT

Sara J. Kohls[*]

I. INTRODUCTION

Cloud computing is the newest big thing in remote computing technology. It allows a user to store his files and media on distant remote servers, the "cloud," in lieu of saving his materials to his local, personal hard drive.[1] The user can then access his data from any device with internet access.[2] The mobility of a user's personal files poses a problem for law enforcement agents who, armed with valid warrants, wish to search a suspect's computer. There is a high probability that a user has not saved his incriminating computer files on his personal computer's physical hard drive[3] if he uses the cloud to store his data.

---

* J.D. Candidate, 2013, Case Western Reserve University School of Law; B.A., 2008, *cum laude*, University of Massachusetts Amherst. I would like to thank Professor Michael Benza for his guidance and input. I would also like to thank my friends and family for their love and support, especially my husband, Jonathan Tobias.

1 *See* ANTHONY T. VELTE, TOBY J. VELTE & ROBERT ELSENPETER, CLOUD COMPUTING, A PRACTICAL APPROACH 3-22 (McGraw-Hill 2010) [hereinafter VELTE] (providing a general overview of cloud computing).

2. *Id.* at 135 ("If you store your data on the cloud, you can get at it from any location that has Internet access. . . . Workers don't need to use the same computer to access data nor do they have to carry around physical storage devices.").

3. *See* Dong Ngo, *Digital storage basics, Part 1: Internal storage vs. memory*, CNET (Nov. 7, 2012, 2:59 PM), [hereinafter Ngo] http://howto.cnet.com/8301-33088_39-57545421/digital-storage-basics-part-1-internal-storage-vs-memory/ (explaining that a hard drive is essentially a 'box containing a few magnetic disks,' which is connected to a computer or laptop via an interface); *see also* Dong Ngo, *Digital storage basics, part 2: External drive vs. NAS server*, CNET (Nov. 16, 2012, 8:50 PM), [hereinafter Ngo II] http://howto.cnet.com/8301-33088_39-57549884/digital-storage-basics-part-2-external-drive-vs-nas-server/ (describing portable external servers, which connect to the computer and "become a storage extension of the host.").

Guidance from existing physical computer search doctrine is limited, yet one thing is clear: a warrant for a physical computer hard drive does not include the right to search the cloud. In the simple yet highly realistic scenario described below, a law enforcement agent may not know what his next steps are when he encounters a computer during a lawful search and suspects that the user may have utilized the cloud network. This Note argues that the answer is simple: the Fourth Amendment protects the cloud, thus law enforcement officers must obtain a separate warrant to search a cloud network account. This protection is apparent when the *Katz v. United States* expectation of privacy test[4] is applied.

Recently, Justice Sotomayor stated in *United States v. Jones*:

> 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 law week, or month, or year. . . . 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.[5]

Justice Sotomayor's statement indicates that the expectation of privacy must evolve with technology. This Note argues that the traditional warrant exceptions, such as the third party doctrine and consent searches, have no place in cloud network searches in light of the evolving expectation of privacy in the technological era.

When a police officer enters a house with a valid search warrant and sees a computer, it is not always clear what his next steps should be. Does the warrant include the computer? What exactly can he access on that computer? How does the officer determine what files he can look for and where he can look for them? To make matters worse, these are questions that an officer faces *before* he finds evidence that the suspect's computing has gone beyond the confines of the physical hard drive.

Now, we add the cloud network to the confusion. Consider the following hypothetical:

After an in-depth investigation, the police establish probable cause supporting a search warrant to search the suspect's computer hard drive for data related to an alleged crime. To obtain the warrant, the officers present affidavits to a neutral and detached magistrate. Per the particularity requirement, the proposed warrant is limited to files saved on the suspect's physical computer. The magistrate specifically limits the scope of the warrant to the physical hard drive and grants it.

4. 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

5. 132 S.Ct. 945, 957 (2012).

Upon arriving at the suspect's residence, the police show the suspect the warrant and gain access to his computer. The police do not find any evidence on the computer's physical hard drive, but a computer specialist notes that there is evidence that the suspect has been using a cloud network account.[6] The police log into the suspect's cloud account without his consent and find hundreds of incriminating files. He is arrested.

After indictment, the defendant's attorney files a motion to suppress. The basis for the motion is that the seized data was beyond the scope of the warrant; therefore the search and seizure was unreasonable and violated the Fourth Amendment. The defendant argues the scope of the warrant limited the police to searching his physical hard drive, and that he did not grant the police authority to access his cloud storage account. Further, the police exceeded their authorization because the seized files were not stored on the defendant's computer, but on servers located hundreds of miles away. The defense attorney concludes the police should have obtained a separate warrant to search the cloud.

This Note argues that the Fourth Amendment does not permit an officer to access files that were never saved on a suspect's computer hard drive without a valid search warrant specific to cloud network storage account. The reasonable expectation of privacy test, established in *Katz*,[7] protects the files and media that a user stores on the cloud. The use of the cloud network can be compared to search regulations of the United States Postal Service (USPS): although a sender entrusts his mail to the third-party USPS, the government is required to obtain a warrant before searching the packages.[8] Similarly, law enforcement must obtain a warrant before accessing documents or files saved on the cloud. Further, a cloud network user does not lose his expectation of privacy the way a person does when he places his trash on the curbside for pickup. The important distinction is that a person leaves his trash out knowing that

6. This Note assumes that law enforcement wishes to search data saved only on the cloud. If there was a back-up copy saved on the computer, the warrant would cover the search.

7. 389 U.S. at 361 (Harlan, J., concurring) (noting that there is a twofold requirement, first that a person have exhibited an actual subjective expectation of privacy and, second that the expectation be one that society is prepared to recognize as "reasonable.").

8. *See infra* Section III(A)(1)(a) for a description of the law regulating search warrants and the mail.

somebody may go through it;[9] a cloud user does not have the same belief.[10]

This Note discusses the Fourth Amendment's protection of the cloud by first explaining exactly what the cloud is and how it differs from other technology, thus establishing why existing computer search methodologies do not apply to the cloud. Therefore, the law must adhere to three principles. First, pursuant to *Katz*, there is a reasonable expectation of privacy in the cloud. Second, executing a warrant to search a physical computer, pursuant to existing computer search doctrine, does not encompass the cloud. Third, law enforcement officers cannot apply an exception to circumvent the warrant requirement.

When police officers have a valid warrant to search a home computer, the search must start and end there. If the police find evidence that the user has a cloud account, the Fourth Amendment prohibits them from immediately accessing the cloud. The additional search warrant is necessary because there is a reasonable expectation of privacy in the cloud. Subsequently, a law enforcement agent has only one option when he wants to search a cloud network account: get a warrant.

II. WHAT IS THE CLOUD?

To understand why the Fourth Amendment protects the cloud, one must understand what the cloud is, why using the cloud is different than using a personal computer, and what sort of privacy implications are involved in cloud network usage.

A. Overview

Many people, even those with a technological background, struggle to understand the cloud's purpose and functions.[11] Put

9. California v. Greenwood, 486 U.S. 35, 40-41 (1988) (noting that thus, there would be no reasonable expectation of privacy in the items they discarded).

10. John B. Horrigan, Data Memo, *Use of Cloud Computing Applications and Services*, PEW INTERNET & AM. LIFE PROJECT (Sept. 12, 2008) *available at* http://www.pewinternet.org/Reports/2008/Use-of-Cloud-Computing-Applications-and-Services/Data-Memo.aspx [hereinafter Horrigan] (reporting high levels of concern from cloud network users when asked about how they would feel if the cloud network provider took various actions with their data).

11. In fact, as recently as 2008, when cloud computing was "new," even the high-profile players in the technological industry believed that the cloud was just "rebranding" current technology. *See* Dan Farber, *Oracle's Ellison nails cloud computing*, CNET NEWS (Sept. 26, 2008, 12:09 PM) http://news.cnet.com/8301-13953_3-10052188-80.html (reporting Ellison's disclosure of the "truth" about cloud computing: "[t]he

simply, cloud computing is a metaphor for the "newest" way to use the Internet.[12] Despite this initial confusion, nearly sixty-nine percent of Americans have used the cloud network in some fashion.[13] Both individuals and companies utilize the cloud in a similar manner. In lieu of a traditional internal server,[14] the cloud network allows the user to run services and programs on an external server,[15] which essentially allows the user to outsource these processes.[16] Thus, users are switching to cloud computing because it provides the same traditional type of networking and file storage capacities for a fraction of the price.[17] In fact, individuals and businesses alike are buying cheaper and less sophisticated machines because large hard drives are no longer necessary; users can stream programs, such as word processing or online gaming, directly from the cloud.[18]

Similarly, utilizing cloud storage involves exactly what the name suggests—storing files and media in a personal account on the cloud rather than on a local system.[19] Notable cloud storage providers include Dropbox,[20] Amazon,[21] Apple,[22] and Google,[23] but there are

---

interesting thing about cloud computing is that we've redefined cloud computing to include everything that that we already do.").

12. *See* VELTE, *supra* note 1, at 3 (describing the cloud network, how it works, the different uses for the cloud, and the various providers, among related things).

13. Horrigan, *supra* note 10 (showing users' different concerns regarding privacy of their data).

14. *See* Ngo II, *supra* note 3 (explaining that internal servers, or 'network attached storage' serves the purpose to "connect[] to a network and make its storage space available to all devices in the same local network.").

15. *See* VELTE, *supra* note 1, at 4, 7-8 ("[C]loud computing is a construct that allows you to access applications that actually reside at a location other than your computer or other Internet-connected device; most often, this will be a distant datacenter." At datacenter is a collection of servers that may be located anywhere, and not necessarily in the same location).

16. *See* Roger Cheng, *'Cloud Computing': What Exactly Is It, Anyway?*, WALL ST. J., Feb. 8, 2010, at R2 (detailing the numerous uses of cloud computing for businesses).

17. *See* VELTE, *supra* note 1, at 4 (explaining how business save money by using the cloud, not only by reducing the costs of buying and licensing programs, but also by reducing the cost of utilities and eliminating the need to buy some programs all together).

18. *Id.* at 7 (describing the concept of a "thin" client (computer) and why use of this type of machine is becoming increasingly popular).

19. *Id.* at 135 - 151 (providing a generalized overview of cloud storage).

20. DROPBOX, https://www.dropbox.com/ (last visited Mar. 26, 2012).

many others. Recently, these companies have brought the cloud into the public eye.[24] The services cloud service providers offer range from a simplistic on-stop "shopping" experience to more complicated systems, requiring multiple stops for a complete cloud-computing experience.[25]

Depending on which cloud network service provider a user chooses, his files or documents that are saved on the cloud are located on remote servers located all over the world.[26] This essentially allows the user to treat his cloud account as a portable hard drive to retrieve his documents and files from any computer with Internet access.[27] In some cases, the user does not have to download additional software to his computer to access the files he has stored on the cloud.[28] For example, Dropbox users simply log into their account via Dropbox's homepage in order to access their stored

21. AMAZON, https://www.amazon.com/clouddrive/learnmore/ref=sa_menu_acd_lrn 2 (last visited Mar. 26, 2012); *see, e.g.*, Rob Pegoraro, *Amazon Cloud Player puts your music on the Web*, WASH. POST (March 29, 2011, 5:58 AM) http://www.washingtonpost.com/blogs/faster-forward/post/amazon-cloud-player-puts-your-music-on-the-web/2011/03/29/AFBJ5jsB_blog.html; *see also, e.g.*, Stu Woo & Geoffrey A. Fowler, *Amazon Cloud Boosts Fire*, WALL ST. J. Sept. 30, 2011, at B2 (detailing the uses of Amazon's "cloud," which Amazon not only rents to companies such as Netflix, Inc., and Zynga, Inc., but also uses it to power searches on the Kindle Fire through the internet browser, Amazon Silk).

22. APPLE ICLOUD, http://www.apple.com/icloud/ (last visited Mar. 26, 2012); *see, e.g.*, David Goldman, *What to Expect from Apple's iCloud*, CNN (June 1, 2011, 3:16 PM), http://money.cnn.com/2011/06/01/technology/apple_icloud/index.htm (discussing the way the iCloud may be utilized to store and play music).

23. *E.g.*, GOOGLE: APPS FOR BUSINESS, http://www.google.com/apps/intl/en/business/officeconnect.html (last visited Mar. 26, 2012).

24. *See* Brian X. Chen, *From iCloud to Dropbox: 5 Cloud Computing Services Compared*, WIRED (June 20, 2011, 3:05 PM), http://www.wired.com/gadgetlab/2011/06/cloud-services-compared [hereinafter Chen] (comparing the five major cloud computing services).

25. *See id.* (comparing Amazon ("Amazon's Cloud Drive is as straightforward as a cloud service gets: It's just an online storage locker.") to Google ("Google's "cloud" suite can be confusing: There's no one-stop destination that hosts all your media.")).

26. *See* VELTE, *supra* note 1, at 8 ("Amazon has their cloud solution in servers all over the world.").

27. *See id.* at 137 (listing various cloud providers and the types of files they specialize in storing).

28. *See e.g.*, DROPBOX, https://www.dropbox.com.

documents.[29] Users do not need to install any additional programs on a computer to access their Dropbox account; rather, they can access their data on public computers with relative ease.

However, Dropbox operates differently from other cloud providers. Dropbox saves copies of a user's files or media to the user's "base" computer, the computer to which the user has installed the Dropbox software.[30] Other cloud network programs do not have this feature. Cloud providers such as Google Drive allow users to create, modify, and save entire document on the cloud.[31] Google Drive provides an entire word processing program to its users, and the user never has to save the document to his personal computer.[32]

B. Why People Use the Cloud Network

It is estimated that by 2020, "most" people will use the cloud network to access software applications online, as well as to store and access their data, in lieu of using traditional personal computers.[33] This is because of the cloud network's ease and convenience; when data is stored on the cloud, a user can access his materials "via an internet link" from whatever computer or device he wishes.[34] So long as the user has access to a "web-based interface," which essentially includes any device that is capable of internet access, such as a laptop, smartphone, tablet, or netbook, he may store or access data on the cloud.[35] Furthermore, the cloud provides a simple way for users to back up their data in another location. If, in an extreme scenario, a tornado ripped through a home and destroyed a user's

29. *Id.* (Log-In box).

30. *See* DROPBOX: FEATURES, https://www.dropbox.com/features (last visited Mar. 26, 2012) ("Any file you save to Dropbox also instantly saves to your computers, phones, and the Dropbox website.").

31. *See* GOOGLE DRIVE, http://www.google.com/drive/start/apps.html#product=docs (last visited Oct. 30, 2012).

32. *See id.* (describing the Google Docs feature of Google Drive, which allows the creation and editing of documents entirely on the cloud).

33. Janna Quitney Anderson & Lee Rainie, *The Future of Cloud Computing*, PEW INTERNET & AM. LIFE PROJECT (June 11, 2010) *available at* http://pewinternet.org/Reports/2010/The-future-of-cloud-computing/Overview.aspx. (basing this theory off an internet study).

34. *See* VELTE, *supra* note 1, at 135 ("As with other cloud services, you can access the data stored on the cloud via an internet link."); *see also* Chen, *supra* note 24 ("Have music on your PC that you want to listen to on your smartphone? Boom, stream it from the cloud. Want to access a document on another computer? Bam, grab it from your web-connected "cloud" drive.").

35. VELTE, *supra* note 1, at 136 (describing the use of cloud computing technology).

computer and local back-ups, a copy of his personal files would still be safe, stored on a remote server miles away.[36]

Moreover, users may have access to nearly unlimited space on the cloud. Users can sign up for the basic free package from the cloud provider, which allows them to store anywhere from one to five gigabytes[37] of material.[38] Alternatively, consumers with greater needs may choose to purchase as much as sixteen terabytes of storage from a cloud provider.[39] This means that a user could store *all* of his files and media on the cloud.

C. Can a Cloud Service Provider Access or Share Your Files?

When a cloud service provider accesses users' files, it is typically in order to comply with a court order or law enforcement.[40] However, it is important to note that nearly half of cloud network users would be "very" concerned if the cloud network provider immediately gave law enforcement their files when law enforcement asked the provider to do so.[41] Although the study was conducted several years ago, it showed that even when the cloud network use was not as prevalent, users expected that the files and media they save on the cloud would remain private.[42] Indeed, cloud users do not expect that a cloud network provider will hand their data to law enforcement without a second thought.

Cloud service providers explain when a user's stored files and media will be accessed in privacy policies and terms of service. For example, Dropbox's Terms of Service states that the provider will not share users' files with anyone, including law enforcement, except for "rare exceptions" or when the user provides permission.[43] Dropbox's

36. *See* Eric A. Taub, *Storing Your Files Inside the Cloud*, N.Y. TIMES, March 3, 2011, at B7 ("Backing up to an external hard drive doesn't help when your house burns or a tornado tears off the roof. If your computer is destroyed, your hard drive, stored 10 feet away in a closet, is probably gone too.").

37. *See* Ngo, *supra* note 3 (describing the units of data storage, such as gigabyte and terabyte, and how they relate to one another).

38. *See* Chen, *supra* note 24 (see chart for different types of cloud providers).

39. *Id.* (such as Windows Live and Dropbox).

40. *See, e.g.*, DROPBOX: PRIVACY POLICY, https://www.dropbox.com/security#privacy (last visited Mar. 26, 2012) (indicating when and how they comply with law enforcement).

41. Horrigan, *supra* note 10 (regarding attitudes about possible data policies of cloud services).

42. *Id.*

43. DROPBOX: TERMS OF SERVICE, https://www.dropbox.com/terms (last visited Mar. 26, 2012).

Security Terms state that the only information it will view about users' files is the file's metadata, which includes the file's name or location.[44] Google's privacy policy is much more complicated, but generally implies that it will not share personal information except in limited situations, including when requested by law enforcement.[45] It is important to note that this provision only refers to personal information, and does not specifically address documents stored on the cloud. Google also reserves the right to examine the content of anything the website hosts.[46] Amazon is notorious for granting the least amount of privacy protection on its cloud.[47] Amazon warns users that when they utilize Amazon's cloud service provider, the user grants Amazon unlimited access to the files.[48] However, Amazon's justifications include compliance with any applicable laws.[49] Some cloud providers take extra measures to protect user's data, which includes encryption of said data while it is in storage.[50] To the ultimate extreme, one provider takes a "zero knowledge" approach to their cloud storage offering.[51] SpiderOak encrypts all data, does not

44. DROPBOX: SEC. TERMS, https://www.dropbox.com/security (last visited Mar. 26, 2012).

45. GOOGLE PRIVACY CENTER, http://www.google.com/intl/en/privacy/privacy-policy.html (last visited Mar. 26, 2012) ("[W]e have a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or enforceable governmental request.").

46. GOOGLE TERMS OF SERVICE, https://www.google.com/intl/en/policies/terms/ (last visited Oct. 14, 2012)

> ("We may review content to determine whether it is illegal or violates our policies, and we may remove or refuse to display content that we reasonably believe violates our policies or the law. But that does not necessarily mean that we review content, so please don't assume that we do.").

47. *See* Steven J. Vaughan-Nichols, *No Privacy on Amazon's Cloud Drive*, ZDNET (Mar. 29, 2011, 9:02 AM) http://www.zdnet.com/blog/networking/no-privacy-on-amazons-cloud-drive/882?tag=nl.e539 ("Amazon can do pretty much anything they want with your files").

48. AMAZON TERMS OF USE, Section 5.2: *Our Right to Access Your Files*, http://www.amazon.com/gp/help/customer/display.html/ref=hp_200557340_tou?nodeId=200557360 (last visited Mar. 26, 2012).

49. *Id.*

50. CRASHPLAN, *Sec. Details*, http://www.crashplan.com/consumer/security.html (last visited Mar. 26, 2012) (detailing data security and protection).

51. SPIDEROAK, *Is SpiderOak really "zero knowledge"? Could you read a user's data if forced at gunpoint?*, https://spideroak.com/faq/

save user's passwords, and does not know the names of stored files or folders; the company advertises that "[y]our SpiderOak data is readable to you alone."[52]

The commonality existing among these examples is that service providers retain the means to comply with law enforcement requests. The implications this has on the cloud's Fourth Amendment protections are discussed below.

III. THE FOURTH AMENDMENT AND COMPUTERS

One of the central concepts of American privacy law is the freedom from governmental intrusion.[53] The Founders drafted this freedom directly into the Constitution as part of the Fourth Amendment, which prevents the government from conducting unreasonable searches or seizures and sets forth the warrant requirements.[54] The Fourth Amendment's protections encompass modern technology even though this technology did not exist at the time of the Amendment's ratification, for the Fourth Amendment protects against *all* unreasonable searches and seizures.

A. Issuing Warrants

The Fourth Amendment requires that a valid warrant only issue on "probable cause, supported by an oath or affirmation that particularly describes the place to be searched, and the persons or things to be seized."[55] These requirements prevent the issuance of generalized warrants, and protect the privacy of those whose homes, selves, and effects the police are searching.[56]

This Note focuses on probable cause and the particularity requirement. When the magistrate is reviewing the proposed search

---

questions/23/is_spideroak_really_zero_knowledge_could_you_read_a_users_data_if_forced_at_gunpoint/ (last visited Mar. 26, 2012) (giving an overview of its "zero knowledge" privacy policy).

52. SPIDEROAK, *Nuts & Bolts: True Privacy*, https://spideroak.com/engineering_matters (last visited Mar. 26, 2012). (showing the difference between SpiderOak and other cloud storage providers).

53. *See* DANIEL J. SOLOVE, NOTHING TO HIDE 4 (Yale University Press) (2011) [hereinafter SOLOVE].

54. U.S. CONST. amend. IV. ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures shall not be violated.").

55. *Id.*

56. *See* Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976) (noting that the police must take care when sorting through papers, whose evidentiary value is not immediately ascertainable, to "minimize[] unwarranted intrusions upon privacy.").

warrant, he may consider placing additional restrictions. Allowing the magistrate to impose these restrictions in order to enforce the warrant's particularity requirements ultimately helps prevent law enforcement agents from overreaching and protects privacy.

1. The Expectation of Privacy

The Fourth Amendment protects all people from unreasonable searches and seizures.[57] Unless the search falls into one of numerous exceptions, the Fourth Amendment requires that the police obtain a warrant, based on probable cause, before conducting a search.[58] The issue of whether a governmental intrusion constitutes a search has been, and continues to be, a hotly contested issue.

In 1967, the Supreme Court held in *Katz*, that the Fourth Amendment's protections against unreasonable searches and seizures "protect[] people, not places."[59] Justice Harlan set forth a two-part test in his concurrence, for whether the "area" is protected by the Fourth Amendment: first, the individual must have expressed an expectation of privacy in the place to be searched; and second, this expectation must be one that society is prepared to recognize as reasonable.[60] This test has been adopted as the predominant approach to evaluating the Fourth Amendment's protections. "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[61] If an officer invades this reasonable expectation of privacy absent a search warrant, he has conducted an illegal search.[62]

Since *Katz*, the Supreme Court has slowly enunciated where a person has a reasonable expectation of privacy. The Court refused to expand the Fourth Amendment's protections to areas such as open fields, due in part to the fact that "open fields are accessible to the public."[63] However, in *Kyllo v. United States*, the Court expressed that there is always a reasonable expectation of privacy in one's

57. U.S. CONST. amend. IV.

58. FED. R. CRIM. P. 41(d)(1).

59. 389 U.S. 347, 351 (1967).

60. *Id.* at 361 (Harlan, J., concurring).

61. *Id.* at 351-52.

62. *Id.* at 359 ("Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures.").

63. Oliver v. United States, 466 U.S. 170, 179 (1984) ("Open fields do not provide the setting for those intimate activities that the Amendment is intended to shelter from government interference or surveillance.").

home.[64] This reasonable expectation of privacy extends to the personal items contained within one's home, which, by default, include any computers that the resident may own.[65] However, once inside the home with a valid warrant, police may search for the items listed on the warrant in places where these items are reasonably expected to be.[66]

The following are examples of areas where the expectation of privacy has been evaluated to determine whether the Fourth Amendment's warrant requirement applies. These examples hold commonalities with the cloud network, and application of these principles gives insight into why the Fourth Amendment protects the cloud.

i. Mail

Americans enjoy an expectation of privacy in the mail; the government will not search their mail once the sender has relinquished it to a branch of the federal government, the USPS, for delivery. This expectation of privacy is historically well-established. In 1878, the Supreme Court in *Ex Parte Jackson* stated that, "[l]etters and sealed packages . . . in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles."[67] The Court established that obtaining a warrant, "as is required when papers are subjected to search in one's own household," is the only way an officer may open mail and examine its contents

64. 533 U.S. 27, 34 (2001) ("[I]n the case of the search of the interior of homes - the prototypical and hence most commonly litigated area of protected privacy - there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that exists, and that is acknowledged to be reasonable.").

65. *See* Payton v. New York, 445 U.S. 573, 589-90 (1980) (discussing how the Fourth Amendment draws a strict line when law enforcement enters a private home).

66. *See* United States v. Ross, 456 U.S. 798, 820-21 (1982) ("A lawful search of fixed premises generally extends to the entire area in which the object of the search may be found and is not limited by the possibility that separate acts of entry or opening may be required to complete the search. Thus, a warrant that authorizes an officer to search a home for illegal weapons also provides authority to open closets, chests, drawers, and containers in which the weapon might be found."); *see also* YALE KAMISAR ET AL., MODERN CRIMINAL PROCEDURE 317 (12th ed. 2008) ("[The police] may only look where the items described in the warrant might be concealed. For example, if a search warrant indicated that the items sought were stolen television sets, the officer would not be authorized to rummage through desk drawers.").

67. 96 U.S. 727, 733 (1878).

prior to it reaching its destination.[68] Officers must honor the warrant requirement even when the piece of mail is suspicious and likely contains something illegal.[69] An officer may detain the mail for the period of time that it takes him to obtain a warrant, but may not open and search the mail until a warrant has been obtained.[70]

ii. Trash

It has long been held that there is no expectation of privacy in garbage that has been relinquished on the side of the road.[71] In *California v. Greenwood*, the respondent challenged the admissibility of evidence that the police obtained by asking the garbage collector to keep his garbage separate, and then seizing it to conduct a search.[72] The Supreme Court found that the police's actions did not violate the Fourth Amendment's prohibition against unreasonable searches and seizures and noted that:

> [R]espondents placed their refuse at the curb for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through respondents' trash or permitted others, such as the police, to do so. Accordingly, having deposited their garbage "in an area particularly suited for public inspection and, in a manner of speaking, public consumption, for the express purpose of having strangers take it[.][73]

68. *Id.* ("No law of Congress can place in the hands of officials connected with the postal service any authority to invade the secrecy of letters and such sealed packages in the mail; and all regulations adopted as to mail matter of this kind must be in subordination to the great principle embodied in the fourth amendment of the Constitution.").

69. *See* United States v. Van Leeuwen, 397 U.S. 249, 252 (1970) ("[N]o law of Congress can place in the hands of officials connected with the postal service any authority to invade the secrecy of letters . . . and all regulations adopted as to mail matter must be in subordination to the great principle embodied in the fourth amendment of the Constitution.").

70. *Id.* at 253 ("The significant Fourth Amendment interest was in the privacy of this first-class mail; and that privacy was not disturbed or invaded until the approval of the magistrate was obtained.").

71. California v. Greenwood, 486 U.S. 35, 41-42 (1988) ("Our conclusion that society would not accept as reasonable respondents' claim to an expectation of privacy in trash left for collection in an area accessible to the public is reinforced by the unanimous rejection of similar claims by the Federal Courts of Appeals.").

72. *Id.* at 38.

73. *Id.* at 40-41(citation omitted).

Thus, when an object is knowingly relinquished to a third party, the expectation of privacy may be negated. However, the Supreme Court's holding in *Greenwood* was in part based on the contention that "[i]t is *common knowledge* that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public."[74]

2. Probable Cause

The Fourth Amendment provides that "no warrant shall issue, but upon probable cause."[75] Probable cause essentially means that there is a "fair probability" that the specific evidence sought will be at the place to be searched at the time that law enforcement wishes to search it.[76] Probable cause has been defined as a "fluid" concept, and is evaluated through a totality of the circumstances test, based on a practical, common-sense determination.[77] However, probable cause is not established if there is only minimal support that the evidence may be in that location.[78] Once the magistrate determined that probable cause exists, he may issue the warrant as long as the other warrant requirements are met.[79]

3. Particularity Requirement

To fulfill the Fourth Amendment's particularity requirement, a warrant must "particularly" describe the place to be searched and the persons or things to be seized.[80] The place to be searched prong requires that the officer conducting the search be able to identify the

74. *Id.* at 40 (emphasis added).

75. U.S. CONST. amend. IV. (regarding searches and seizures).

76. Illinois v. Gates, 462 U.S. 213, 238 (1983) ("The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the "veracity" and "basis of knowledge" of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place.").

77. *Id.* at 232 (probable cause turns on "the assessment of probabilities in particular factual contexts – not readily, or even usefully, reduced to a neat set of legal rules.").

78. *Id.* at 239 ("Sufficient information must be presented to the magistrate to allow that official to determine probable cause; his action cannot be a mere ratification of the bare conclusions of others.").

79. U.S. CONST. amend. IV; *see Gates*, 462 U.S. at 239-240 (explaining that the totality of the circumstances test will not lessen the magistrate's ability to make a determination as to whether probable cause exists to issue a warrant).

80. U.S. CONST. amend. IV.

location he is to search with "reasonable effort."[81] The "things to be seized" prong requires the description be sufficient enough so that an officer will be able to determine which items he may seize and which he may not.[82] This prong also requires that any item seized be within the scope of the probable cause.[83]

However, often one or both of these prongs are lacking. The Supreme Court recently outlined the warrant particularity requirements in *Groh v. Ramirez*, holding that a warrant that described with particularity the *place* to be searched was invalid because the warrant failed to identify any of the *items* that the petitioner intended to seize.[84] In *Groh*, the warrant's description of items to be seized was limited to one item: "[a] single dwelling residence . . . blue in color."[85] The Court held that the warrant did not contain a description of the items to be seized "at all," and although there was probable cause to issue the search warrant, the Court invalidated it due to the lack of particularity.[86]

Thus, because it is possible to establish probable cause to search a location for one item, but not another,[87] or that the warrant that may be so facially overbroad that it allows an agent to seize an entire house,[88] agents must exercise diligence when describing the place to be searched or the things to be seized. Law enforcement agents must also take care to not to be overly broad, because courts also refuse to

81. Steele v. United States, 267 U.S. 498, 503 (1925) (here, the description of the building as a garage and for business purposes at 611 W. 46th Street was a sufficient description).

82. Marron v. United States, 275 U.S. 192, 296 (1927) (noting that nothing can be left to the discretion of the officer executing the warrant as to what is to be taken).

83. *Cf.*, Groh v. Ramirez, 540 U.S. 551, 563 (2004) (noting that an officer executing a search warrant must ensure that the search is "lawfully authorized and lawfully conducted," and because there was no description of things to be seized, the "search was clearly 'unreasonable' under the Fourth Amendment.").

84. *Id.* at 554-555 (emphasis added).

85. *Id.* at 558.

86. *Id.* at 557("The warrant was plainly invalid . . . 'the warrant . . . was deficient in particularity because it provided no description of the type of evidence sought.'") (citation omitted).

87. *Cf.*, United States v. Carey, 172 F.3d 1268, 1276 (1999) (finding that the scope of the warrant had been exceeded because there was probable cause to search the computer for evidence of drug dealing, not the child pornography that the detective found).

88. *Groh*, 540 U.S. at 554.

uphold "blanket warrants," which are warrants that allow for broad scale search and seizures, absent proof of necessity.[89]

One of the main issues with computer warrants is that they often suffer from lack of particularity. Thus, police should diligently describe with particularity the specific files they seek in the warrant application,[90] and not simply provide a generalized description of the physical computer itself. It is also imperative that the police strictly abide by the particularity requirement, instead of merely requesting to search every file on the computer because of the large quantity of information that computers are capable of holding.[91] To make the description as particular as possible, it should include the type of file or media[92], where the files may be located, and/or a description of the crime itself and how the files or media sought may be related.[93]

4. Restrictions Imposed by Magistrates

Magistrates have begun to impose restrictions on the scope of computer warrants in an attempt to discourage law enforcement agents from exceeding the scope of what they have probable cause to search or seize.[94] These warrant limitations include the how and when the agent may conduct a computer search or seizure, among other things.[95] As it relates to computer searches, this means that a

89. *See, e.g.*, United States v. Hill, 459 F.3d 966, 976 (9th Cir. 2006) ("We do not approve of issuing warrants authorizing blanket removal of all computer storage media for later examination when there is no affidavit giving a reasonable explanation . . . as to why a wholesale seizure is necessary.").

90. *See e.g.*, *Carey*, at 1275 (noting that "the magistrate should then require officers to specify in a warrant which types of files are sought.").

91. *See e.g.*, United States v. Giberson, 527 F.3d 882, 887 (9th Cir. 2008) ("Computers, like briefcases and cassette tapes, can be repositories for documents and records.").

92. For example, a computer file may be a picture or drawing in .JPG format, or a Microsoft Word document (.doc).

93. *See e.g.*, United States v. Gawrysiak, 972 F.Supp. 853, 860-61 (D. N.J. 1997) *aff'd* 178 F.3d 1281 (3d Cir. 1999) (upholding the validity of a search warrant because it specifically limited what agents could search for, leaving little to their discretion).

94. *See* Orin Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241 (Oct. 2010) [hereinafter *Ex Ante Regulation*] (describing why magistrates should not impose restrictions on warrants); *see contra* Paul Ohm, Response, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 VA. L. REV. IN BRIEF 1 (Mar. 2011) [hereinafter Ohm] (responding to Kerr's article and describing why magistrates should be able to impose restriction).

95. *See Ex Ante Regulation*, *supra* note 94, at 1243-44 (describing four categories of how federal magistrate judges have limited computer searches and seizures).

magistrate may require that police only search for files or documents that have a .JPG or a .DOC extension, instead of allowing police to search any and all documents or folders on the system.[96]

Some scholars have criticized this approach,[97] yet others approve of the magistrates taking additional privacy safeguards.[98] The argument against magistrate-imposed restrictions is based on the contention that the subsequent adversarial proceedings will play the same role; thus, the restrictions are unnecessary.[99] The argument continues that if law enforcement has established probable cause, then the magistrate should not be allowed to limit the search because he is not in the position to know enough about the case to establish workable restrictions.[100]

On the other hand, those who argue in favor of allowing magistrates to place restrictions on warrants believe that these rules are "designed to cure the manifest lack of probable cause and particularity in almost every computer case."[101] It is important to note that magistrates rarely impose these types of restrictions outside of computer cases, and they must consider these types of searches in a different context; "computer search warrants are the closest things to general warrants we have confronted in the history of the Republic."[102] Allowing magistrates to place restrictions on computer search warrants provides two very important protections: first, it allows magistrates to limit searches to areas where probable cause exists and to protect against a lack of particularity; and second, it recognizes that the particularity requirement must be read differently in regards to computer searches to avoid general warrants.[103]

---

96. *See id.* at 1255-58 (giving examples of how magistrates have limited computer searches in the past).

97. *See id.* at 1247 (arguing that "ex parte" regulations are "unworkable and counterproductive" and that the same results can be achieved through legal challenges to the search).

98. *See* Ohm, *supra* note 94, at 12 (disagreeing with Kerr's argument against ex ante regulations, and noting that "[i]f the Fourth Amendment imposes new restrictions on what law enforcement agents can do, those agents will, as they have so many times before, find a way to continue to do their jobs efficiently and successfully while at the same time respecting the rights of the people.").

99. *See Ex Ante Regulation*, *supra* note 94, at 1293.

100. *See id.* at 1282 ("a magistrate judge cannot get a sense of the exigencies that will unfold at each stage of the search process.").

101. *See* Ohm, *supra* note 94, at 4.

102. *See id.* at 11.

103. *See id.* at 10.

B. Warrant Exceptions

The third party doctrine and consent searches deal with the same concept: a user forgoes his expectation of privacy when he purposely places something in the hands of another. These are arguably very persuasive reasons why the Fourth Amendment's warrant requirement is *already* negated in regards to the cloud network. However, distinctive differences exist in the way that the cloud works that renders these doctrines inapplicable and shows the Fourth Amendment's protections still apply to the cloud because a user maintains his expectation of privacy.

1. Third Party Doctrine

The basis of the third party doctrine is found in the 1966 Supreme Court decision *Hoffa v. United States*.[104] The Court held that:

What the Fourth Amendment protects is the security a man relies upon when he places himself or his property within a constitutionally protected area, be it his home or his office, his hotel room or his automobile. There he is protected from unwarranted governmental intrusion. And when he puts something in his filing cabinet, in his desk drawer, or in his pocket, he has the right to know it will be secure from an unreasonable search or an unreasonable seizure.[105]

However, *Hoffa* involved the admissibility of incriminating statements that the defendant, Hoffa, made to the third-party government agent who was in the hotel room.[106] The Court based its finding that Hoffa did not have a reasonable expectation of privacy in his incriminating statements because Hoffa voluntarily disclosed the information to the third party, who he had trusted.[107]

It was obvious that the petitioner was not relying on the security of his hotel suite when he made the incriminating statements to [the third party] or in [his] presence. [The third party] did not enter the suite by force or by stealth. He was not a surreptitious eavesdropper. [The third party] was in the suite by invitation, and every conversation which he heard was either directed to him or knowingly carried out in his presence.[108]

This reasoning became the basis of the third party doctrine, which holds that when an individual voluntarily places information in

104. 385 U.S. 293 (1966).

105. *Id.* at 301.

106. *Id.* at 302.

107. *Id.* ("the petitioner, in a word, was not relying on the security of the hotel room; he was relying upon his misplaced confidence that [the third party] would not reveal his wrongdoing.").

108. *Id.*

the hands of a third party, he loses his expectation of privacy in the information.[109] An actor assumes the risk that a third party, such as the person at the receiving end of the communication, will report the contents of the communication to the police.[110] At this point, the conversation no longer holds Fourth Amendment protections because the actor has foregone his reasonable expectation of privacy.[111]

The third party doctrine is problematic for the technological world.[112] Use of the cloud network potentially invokes this doctrine since users voluntarily place their files in the hands of a third-party service provider.[113] Therefore, the argument can be made that when a person voluntarily turns files over to a third-party cloud provider by utilizing their services, the government may obtain the files or media held by the third party without a warrant.[114] However, this argument is contingent upon the assumption that there is no expectation of privacy in the cloud, and that a cloud network provider is the type of third party that the *Hoffa* Court envisioned.

2. Consent Searches

When the police do not have a valid warrant, and may not be able to easily obtain one, they sometimes attempt to engage in a consent search.[115] Law enforcement engages in a consent search when they gain voluntary permission from either the person who has

109. *Id.* at 303 (holding that no Fourth Amendment rights were violated in the case).

110. *Id.* ("The risk of being overheard by an eavesdropper or betrayed by an informer or deceived as to the identity of one with whom one deals is probably inherent in the conditions of human society.").

111. *Id.*

112. SOLOVE, *supra* note 53, at 102-110 (describing how the third party doctrine has developed in regards to technology).

113. SOLOVE, *supra* note 53, at 105-106 (describing how the cloud potentially invokes the third party doctrine, which removes the Fourth Amendment's protections from the cloud).

114. *See* David A. Couillard, *Defogging the Cloud: Applying the Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2213-16 (June 2009) (explaining how the third party doctrine can be applied to cloud computing); *see also* SOLOVE, *supra* note 53, at 106 ("Since people's documents are no longer stored on their home computers but reside instead with third parties, the shift to cloud computing will effectively remove Fourth Amendment protection from their documents.").

115. *See e.g.*, Schneckloth v. Bustamonte, 412 U.S. 218, 227 (1973) ("In situations where the police have some evidence of illicit activity, but lack probable cause to arrest or search, a search authorized by a valid consent may be the only means of obtaining important and reliable evidence.").

authority,[116] or one who has "joint occupancy,"[117] in order to conduct the search. This determination is based on the surrounding circumstances.[118] Once consent is granted, the Fourth Amendment's warrant requirement is considered waived.[119]

As mentioned briefly above, third parties may grant consent when they have "joint access or authority" in a particular area that the police wish to search.[120] In *Illinois v. Rodriguez*, the Supreme Court held that consent to search was valid when given by somebody who the police reasonably believed had the authority to grant the consent.[121] For example, the police relied on the fact that the woman who gave consent to search an apartment had keys to the area, stored clothing and furniture there, and called it "our" apartment.[122] However, it is important to remember that when someone giving consent clearly does not have the authority to do so, consent is invalidated because the police should not have reasonably relied on the consent.[123]

C. Physical Computer Searches – Counteracting Overly Broad Warrants

Typically, so long as the warrant complies with Fourth Amendment requirements, no issues arise when the police obtain a warrant and conduct a search of a computer's physical hard drive.[124]

---

116. *Id.* at 248-49.

117. United States v. Matlock, 415 U.S. 164, 169 (1974) ("It has been assumed by the parties and the courts below that the voluntary consent of any joint occupant of a residence to search the premises jointly occupied is valid against the co-occupant[.]").

118. *Bustamonte*, 412 U.S. at 248-49 ("Voluntariness is a question of fact to be determined from all the circumstances[.]").

119. *Id.* at 221 (noting that the appellate court found that a consent search was "a waiver of a constitutional right," thus a showing of voluntariness needed to be established).

120. *Matlock*, 415 U.S. at 169.

121. 497 U.S. 177, 188-189 (1990) ("[D]etermination of consent to enter must 'be judged against an objective standard: would the facts available to the officer at the moment . . . [warrant a belief]' that the consenting party had authority over the premises... if so, then the search is valid.") (citation omitted).

122. *Id.* at 179.

123. *Id.* at 186 (describing how the officer's reliance on the consent to search must be reasonable).

124. *See* Groh v. Ramirez, 540 U.S. 551, 557 (2004) (explaining that a warrant needs to comply with the Fourth Amendment's four proscriptions: probable cause, supported by sworn affidavit, and particularly describing the place to be searched and the type of evidence

Challenges arise when a defendant later alleges that the police exceeded the scope of the warrant.[125] For example, police may purposely search for evidence outside the warrant's scope,[126] or when they purposely seize more files or data than they actually need.[127] However, it is clear that when the warrant is limited to the computer's physical hard drive, the search ends there; law enforcement may not use an otherwise valid warrant to access the user's cloud account.

Currently, police conduct searches of the files and documents contained on a computer in one of two ways. First, pursuant to the warrant, the police enter the location and seize the computer.[128] The police retain control of the computer while searching the hard drive in a controlled environment, a process that may take anywhere from days to months.[129] Alternatively, an agent makes an exact, read-only image of the hard drive as it is at the moment of the search.[130] The

---

sought, and that a warrant that fails to comply with these requirements is invalid).

125. *See* Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193, 197-216 (2005) [hereinafter Clancy] (explaining the various search methodologies and the issues with each of them).

126. *See* United States v. Carey, 172 F.3d 1268, 1270, 1273-74 (10th Cir. 1999) (explaining that a warrant to search the defendant's computer for "names, telephone numbers, ledger receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances," constrained the search to only those items listed and noting that the officer in question knew that he was exceeding the scope of the warrant. Thus, the subsequently seized evidence was inadmissible.).

127. *See* United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1173 (9th Cir. 2010) (en banc) (holding that when the government purposefully exceeded the scope of the warrant and seized more information than it was allowed, it needed to return the property it obtained through its intentional wrongdoing).

128. *See* United States v. Hill, 459 F.3d 966, 974-75 (9th Cir. 2006) (specifying reasons to seize the computer in its entirety in lieu of bringing a laptop to the scene to sort through the material, even though that meant non-seizable material would be taken as well. These included the risk that the police may damage the storage medium or compromise the evidence, and that the process of searching on-site might take a long time.).

129. *See, e.g.*, *id.* at 975-75 (explaining why the seizure of a computer and the subsequent search back at the police station was not unreasonable).

130. *See* Orin Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 540 (2005) [hereinafter *Searches and Seizures*] ("To ensure the evidentiary integrity of the original evidence, the computer forensics process always begins with the creation of perfect 'bitstream' copy or 'image' of the original storage device saved as a 'read only' file. All

agent takes the copy, rather than the actual physical computer, back to the lab where other officers search the read-only images at their leisure.[131] Because the copy is read-only, the subsequent search will not alter the copy.[132] The Federal Rules of Criminal Procedure allows for either approach.[133]

Courts have demonstrated they are unwilling to apply the "one warrant fits all" approach to electronic file seizure. In *United States v. Comprehensive Drug Testing*, when government agents seized all the drug testing records located at Comprehensive Drug Testing, Inc. because it was "too hard" to distinguish the ten accounts they sought from the hundreds that were intertwined on a single excel spreadsheet, the Ninth Circuit required the evidence be returned.[134] The Ninth Circuit, *en banc*, recognized that an officer must take extra steps to protect the privacy of those who are subjected to an overly-broad warrant,[135] and noted "[t]he pressing need of law enforcement for broad authorization to examine electronic records . . . creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant."[136]

These extra steps are required because the court specifically acknowledged that situations exist where broad-scale seizure may be the only feasible way to efficiently conduct the search.[137] The enforcement of these additional requirements addresses instances when it is especially apparent that it is "an obvious case of deliberate overreaching by the government in an effort to seize data as to which it lacked probable cause."[138]

To counter the issue of overbroad searches and lack of clear guidelines, the law has begun analogizing computer hard drive

---

analysis is performed on the bitstream copy instead of the original. The actual search occurs on the government's computer, not the defendant's.").

131. *See id.* at 540-41.

132. *Id.* at 541.

133. F. R. CRIM. P. 41(f)(1)(B) ("[I]n a case involving the seizure of electronic storage media *or* the seizure or copying of electronically stored information[.]") (emphasis added).

134. 621 F.3d 1162, 1169 (9th Cir. 2010) (en banc).

135. *Id.* at 1177 (explaining that judicial officers must be vigilant in "striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures").

136. *Id.* at 1176.

137. *Id.* at 1169.

138. *Id.* at 1172.

searches to different physical search methodologies. The government has recognized the need for limiting electronic searches, and has, in fact, codified that comparable searches must be limited.[139] For example, the procedure for interception of wire, oral, or electronic communications states "[e]very order and extension . . . shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective."[140] It is important to gain a basic understanding of these analogies in order to understand why none encompass the cloud, which explains why law enforcement needs a separate warrant to search the cloud network.

1. The "Container" Search Analogy

Likely due to the ease of comparison, hard drive searches are most commonly compared to "container" searches.[141] The container search analogy is based on the Supreme Court's holding that an officer's warrantless search of personal containers violates the owner's reasonable expectation of privacy.[142] However, when the police have a valid warrant, they are able to search any container that may contain the item described in the warrant.[143] Because the courts have analogized computers to be the "functional equivalent" of containers, the police may search a computer because items specified on the warrant might be contained therein.[144]

Scholars and courts alike have criticized applying the container analogy to computer searches because it is overly broad and essentially provides a "blank check" to the officer by giving him access to every file on the computer.[145] It is argued that police should

139. *See* 18 U.S.C. § 2518 (2006) (describing how "[n]o order entered under this section [of the law] may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization").

140. § 2518(5).

141. Office of Legal Educ. & Exec. Office for United States Attorneys, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 2-3 (2009), *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf ("To determine whether an individual has a reasonable expectation of privacy in information stored in a computer, it helps to treat the computer like a closed container such as a briefcase or file cabinet."); *see also Searches and Seizures*, *supra* note 130 at 550.

142. *See* United States v. Ross, 456 U.S. 798, 822-23 (1982).

143. *See* Clancy, *supra* note 125, at 198-99.

144. *Id.* at 199 ("computers have been said to be [like containers]").

145. *Id.* at 203-204; *see also* United States v. Carey, 172 F.3d 1268 (10th Cir. 1999).

be required to utilize restrictive measures in order to protect the privacy of the user.[146] The next two search methodologies are ways to limit the container search analogy.

2. The "Sub-Container" Search Analogy

Arguably, a warrant may constitute permission to search the entire computer container without limitations; thus it may be necessary to place further limitations on a computer container search.[147] Applying a "sub-container" analogy provides some added protections. Under this view, the computer is still viewed as one big container or "physical shell,"[148] but each directory or file is an even smaller unit, a "sub-container."[149] This view dictates that each sub-folder saved on the physical hard drive of the computer, e.g., a document, spreadsheet, or file, requires an individual search warrant.[150]

However, the sub-container theory has been criticized as an unworkable standard.[151] "Storage media do[es] not naturally divide into parts. Subdivisions must be invented, and every subdivision strategy comes with flaws."[152] This theory is difficult to apply.[153] Law enforcement has no consistent standard to determine what might be considered a "sub-container."[154] Some courts may view each individual file on a computer as a sub-container; however, other courts may find that the individuals lines within an excel spreadsheet, a single file, are sub-containers.[155] As "defining subcontainers defines

146. Clancy, *supra* note 125 at 203-204 (rejecting the container approach).

147. *See* Josh Goldfoot, *The Physical Computer and the Fourth Amendment*, 16 BERKELEY J. CRIM. L. 112, 112 [hereinafter Goldfoot] ("Computer storage media can reveal facts relevant to an investigation, but they can also reveal irrelevant facts that can be embarrassing or inform investigators for the first time about a new crime.").

148. *Id.* at 118.

149. *Id.* at 112-13, 119.

150. *Id.* at 119-120.

151. *Id.* at 131-32 (discussing the issues applying the sub-container view to computer searches).

152. *Id.* at 131.

153. *Id.* at 125-30 (describing a few of the many issues that the subcontainer view brings with it).

154. *Id.* at 125 ("From the subcontainer perspective, this question becomes: what are the subcontainers?").

155. *See* United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1181 (9th Cir. 2010) (en banc) (J., Kozinski, concurring) (implicitly applying the subcontainer view when noting law enforcement could have "could have selected the spreadsheet rows for the ten ballplayers for

what information is immune from seizure,"[156] the officers must be careful to specifically particularize the warrant to their search and to perhaps conduct a very narrow search to not miss a necessary sub-container. However, the ease of mobility of information on a computer dictates that this might not be the easiest thing to do.

3. The "Special" Approach Theory Analogy

As a third alternative, courts may utilize the "special" approach theory of computer searches, which is similar to the sub-container approach. For example, a magistrate utilizes the special approach in limiting the warrant by seeking a description or an example of the evidence sought by law enforcement before authorizing a broad search, and allowing the search to encompass only specific search terms that may relate to the items sought.[157] When utilizing this method, the court requires the warrant to "include measures to direct the subsequent search of the computer."[158]

Courts have considered the special approach.[159] For example, in *United States v. Carey*, the police seized two computers and obtained a search warrant to search for evidence related to drugs.[160] After conducting the search, the detective stumbled upon evidence of child pornography when he opened a file containing such pornography and continued to purposefully open subsequent files that he knew were not related to drugs.[161] The court rejected the government's attempted justification of the search through its proposed file cabinet argument,[162] and found that the detective had purposely exceeded the

whom he had a warrant, then copied and pasted those rows into a blank spreadsheet. If he had done so, he would have seen only those drug testing results for which he had a warrant.").

156. Goldfoot, *supra* note 147, at 125.

157. *See* Clancy, *supra* note 125, at 199-200 (criticizing the "special" approach as unworkable in light of the reality of the ease in which one may manipulate computer files); *but see* United States v. Carey, 172 F.3d 1268 (10th Cir. 1999) (utilizing the "special" approach and suppressing the evidence found when an officer opened .JPG files, which were not included in the warrant).

158. *See In re* Search of 3817 W. West End, 321 F. Supp. 2d 953, 955 (N.D. Ill. 2004) (expressing concern over the government's intention to review all files contained on a computer to determine their evidentiary nature, and requiring the government to provide a detailed protocol outlining the way the search would be limited).

159. *See, e.g.*, United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999) (acknowledging that computers often contain intermingled documents).

160. *Id.* at 1270.

161. *Id.* at 1271.

162. *Id.* at 1272 (rejecting the government's argument that because they had a warrant to search the computer, they could search the computer for

warrant's scope.[163] The court opined that the magistrate should require the officers to state the type of files they sought in the warrant, and that the search must be specifically limited to these types of files.[164]

The special approach, however, has also been criticized and generally deemed useless and inappropriate to govern computer searches.[165] This criticism resides in the ease that criminals may change a file's name or extension to unrelated or unsuspicious topics, and that those criminals who utilize computers are often sophisticated individuals with methods to cover their tracks.[166] For example, in *United States v. Hill*, the court noted that "[t]he ease with which child pornography images can be disguised – whether by renaming sexyteenyboppersxxx.jpg as sundayschoollesson.doc, or something more sophisticated – forecloses defendant's proposed search methodology."[167]

D. Networked Computer Searches

The law regulating the search of computer networks is more straightforward: the Fourth Amendment's protection of a user's data is very limited. This is due to the nature of computer networks, which usually function as a means of *purposefully* sharing data with other users.[168] Each device on the network is "attached" to the others and users use this connection to access shared data.[169] Although using

anything incriminating in nature, and that plain view justified the finding of pornography).

163. *Id.* at 1274-75 (finding the cabinet analogy inapplicable because the "files" were adequately labeled and the detective knew what each file contained and that he was exceeding the scope of the warrant).

164. *Id.* at 1275.

165. *See* Clancy, *supra* note 125, at 206-10.

166. *See id.*, at 208 ("'Computer records are extremely susceptible to tampering, hiding, or destruction, whether deliberate or inadvertent.' Images can be hidden in all manner of files, even word processing documents and spreadsheets. Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer.")(citation omitted).

167. 322 F. Supp. 2d 1081, 1090-91 (C.D. Cal. 2004).

168. *See* MICHAEL A. GALLO & WILLIAM M. HANCOCK, NETWORKING EXPLAINED 2 (2nd ed. 2002) [hereinafter GALLO] ("Specifically, the term 'networking' refers to the concept of connecting a group of systems for the expressed purpose of sharing information. The systems that are connected form a network.").

169. *See id.* at 3-4 (explaining that a computer network is a "collection" of devices, which extend beyond computers to printers, palm pilots, ect., that share resources by means of network "medium" and "protocol").

a network does not immediately negate a user's expectation of privacy, the knowledge that information transmitted on the network is not confidential and may be monitored reduces the expectation of privacy.[170] Even when a user takes steps towards ensuring that his files remain private, courts may find that the *objective* component of *Katz* still negates the expectation of privacy.[171] The loss of one's expectation of privacy usually occurs when the user has knowingly exposed his files to the public and placed them in a location where others can access them.[172]

Thus, law enforcement may theoretically negate the warrant requirement and search a computer network by obtaining consent or by the logic of the third party doctrine. Law enforcement may obtain consent to search a network, for example, from a network administrator, employer, or, arguably a co-worker—anyone who has "joint occupancy" and therefore access to the data.[173] Law enforcement may still choose to seek a warrant; however, when given the opportunity to surpass the burdensome requirement, he will likely choose not to. On the other hand, the third party doctrine applies to computer networks as well; the user has entrusted his data to a third party network host, much like Hoffa entrusted his secrets to a

170. *Cf.* City of Ontario, Cal. v. Quon, 130 S.Ct. 2619, 2632-33 (2010) (discussing that because Quon was explicitly informed that his employer-provided pager may be subject to audit, he may have no expectation of privacy, but finding that the search did not violate the Fourth Amendment on other grounds); *see, e.g.*, United States v. Heckenkamp, 482 F.3d 1142, 1146-47 (9th Cir. 2007) (holding that the defendant still had a reasonable expectation of privacy in his files on a network absent a policy outlining the active monitoring of the network).

171. *See, e.g.*, United States v. Ziegler, 474 F.3d 1184, 1189 (9th Cir. 2007) ("The government does not contest Ziegler's claim that he had a subjective expectation of privacy in his . . . computer . . . but Ziegler's expectation of privacy in his office and workplace computer must also be seen as objectively reasonable."); *see also* United States v. King, 509 F.3d 1338, 1342 (11th Cir. 2007) (holding that when a user utilized a computer network and knew that his documents were exposed to the public, although he took steps to keep his files private, he no longer retained a reasonable expectation of privacy).

172. Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."); *see also* United States v. King, 509 F.3d 1338, 1341-42 (11th Cir. 2007) (finding that society would not recognize the network user's expectation of privacy as reasonable because his files were shared with thousands of individuals who had access to the network).

173. United States v. Matlock, 415 U.S. 164, 170-71(1974) (dismissing the argument that the third party could not give consent, and holding that consent was valid because she was a "joint occupant").

government agent, and has misplaced his reliance that the third party will not share his data with law enforcement.[174]

A fundamental distinction exists between the cloud and computer networks. A computer network is *not* the Internet.[175] Typically, when a user is part of a computer network, he is aware that he allowing other network users access to his files and media, and therefore can plan what he saves and stores on the network accordingly.[176] In the alternative, although a user may create a personal "network" on the cloud by accessing his material from multiple computers, tablets, and smartphones, unless the user knowingly invites others to join his "network," his files and media remain private.[177] This difference makes it dangerous to compare the cloud to a computer network for the purposes of determining Fourth Amendment protections. For example, a Dropbox user has the ability to "share" a file or folder with others.[178] However, if the user chooses not to utilize this feature, his files remain private.[179] Even if the user has installed the Dropbox application on multiple devices, he is the only one who can access these files, provided that he has not shared his password with others.[180] Thus, because a user has not knowingly exposed his files and media to a public network when using the cloud, he has not foregone his expectation of privacy in the same way a computer network user has.

IV. SEARCHING THE CLOUD

The solution is simple. If a law enforcement agent wishes to search the cloud, he must obtain a warrant; anything less than this strict requirement violates the Fourth Amendment and is unconstitutional. A warrantless search and seizure of data from a cloud network account is unreasonable.

174. Hoffa v. United States, 385 U.S. 293, 302 (1966) ("[P]etitioner, in a word, was not relying on the security of the hotel room; he was relying upon his misplaced confidence that [the third party] would not reveal his wrongdoing.").

175. *See* GALLO, *supra* note 168, at 9.

176. *Id.* at 2 (describing the purpose of a network is to share information with others).

177. *See* DROPBOX: TERMS OF SERVICE, https://www.dropbox.com/terms (last visited Oct. 29, 2012) (explaining an optional feature that allows a user to share his files with others).

178. *Id.* ("The Services provide features that allow you to share your stuff with others or to make it public.").

179. *Id.*

180. *See id.*

Three points support the conclusion that a law enforcement agent must be required to obtain a separate warrant. First, pursuant to *Katz*, there is a reasonable expectation of privacy in the cloud. Second, a warrant search of a computer does not extend to and encompass the cloud. Third, any attempts to circumvent the warrant requirement are unsupported by law.

A. There Is an Expectation of Privacy in the Cloud

The Fourth Amendment protects cloud network accounts because a user has a reasonable expectation of privacy in the cloud. This protection is derived from the application of *Katz*'s two-part reasonable expectation of privacy test; that the person has exhibited an actual (subjective) expectation of privacy in the area to be searched, and that expectation is one that society is prepared to recognize as reasonable (the objective component).[181] A comparison of cloud computing to the protections afforded to, or stripped from, the mail and the garbage provide support for this conclusion.[182]

First, the subjective aspect of *Katz* is satisfied. Users maintain a reasonable expectation of privacy in files saved on the cloud. Primarily, this is because many cloud network users utilize it for private, personal means: to either back up data or to store documents in an easily accessible location.[183] Users do not assume that cloud network providers will snoop in or share their files, and are concerned when presented with a situation in which unauthorized or uninformed access may occur.[184]

Comparably, the Supreme Court has routinely held that law enforcement must seek a warrant before an agent is permitted to search the contents of a piece of mail that a person has voluntarily turned over to the third-party USPS.[185] In these types of situations, although the sender places his letters and packages into the hands of a third party, he has not foregone his expectation of privacy in the contents of his mail.[186] The same concept may be applied to the

181. United States v. Katz, 389 U.S. 347, 361 (1967).

182. *See supra* Section III(A)(1) for a discussion of the reasonable expectation of privacy in regards to the mail and the garbage.

183. Horrigan, *supra* note 10 (reporting the various ways users utilize the cloud, which include storing personal photos, files, and videos).

184. *Id.* (reporting when those surveyed were given ways providers may use their files, users "report[ed] high levels of concern when presented with scenarios in which companies may put their data to uses of which they may not be aware").

185. *Ex Parte* Jackson, 96 U.S. 727, 733 (1978); United States v. Van Leeuwen, 397 U.S. 249, 252 (1970).

186. *Ex Parte* Jackson, 96 U.S. at 733 ("Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, *except as to their outward form and weight.*") (emphasis added).

cloud. A cloud user has placed his files and media into the hands of the third-party cloud provider, and entrusts the third party will store and provide access to the files, but does not expect the provider to look at them.

Comparing the cloud network to the mail also provides another piece of support for the subjective expectation of privacy. The contents of the mail receive Fourth Amendment protection, not the physical envelope and address that have been exposed to the public eye.[187] The security notifications Dropbox provides state that the only information its employees have access to is the metadata, which is comprised of the file name and location.[188] This similarity provides direct support for the subjective expectation of privacy: users who accept these policies and choose to use the particular cloud network account based on these policies, have a reasonable subjective expectation of privacy.

Katz's objective aspect, that society recognizes the expectation of privacy as reasonable, is also satisfied through similar reasoning. Objectively, the cloud differs from searching garbage because no risk exists that once a user saves or "relinquishes" a file to a cloud account, that snoops and scavengers will ravage it. In fact, to further distinguish the cloud from the garbage, it is unlikely that anyone besides the user may view the file because he has not digitally left it out in the open the way the trash is left on the curb.[189] Thus, under *Greenwood*, simply placing data in the hands of a provider does not negate the expectation of privacy because others still may not obtain it.

Further, the government has acknowledged that there is an expectation of privacy in the contents of a physical hard drive, and law enforcement has begun to include a computer on warrant applications, obtain a second warrant when an unanticipated computer is located, or justify why the initial warrant covered searching the computer.[190] The cloud should be viewed in the same manner, because the cloud network is just another location, albeit an *off-site location*, where a user will store data. Moreover, if a user believed that the government could access data saved on the cloud at

187. *Id.*

188. DROPBOX: SEC. TERMS, https://www.dropbox.com/security (last visited Mar. 26, 2012) (Dropbox employees are prohibited from viewing the content of files you store in your Dropbox account, and are only permitted to view file metadata (e.g., file names and locations).").

189. *See* California v. Greenwood, 486 U.S. 35, 40-41 (1988) (describing one's lowered expectation of privacy when they take the trash out).

190. *See, e.g.*, United States v. Carey, 172 F.3d 1268, 1270-71 (1999) (explaining that law enforcement sought an additional warrant to search unanticipated computers).

any time, use of the cloud network would likely not be as prevalent. To compare the cloud to the mail again, patrons of the USPS would not surrender their mail as easily if they thought the government could open and search any letter or package. Part of the USPS' success is contingent upon the government understanding that privacy rights must be respected. The same reasoning must be applied to the cloud, and, in fact, already has been.

Therefore, because *Katz's* reasonable expectation of privacy test is satisfied, the answer to the initial hypothetical must be that law enforcement is required to obtain a separate warrant.[191]

B. Warrants to Search a Hard Drive Do Not Include Searching the Cloud

The Fourth Amendment protects a physical computer hard drive, and several methods of computer search doctrine have evolved with these protections in mind. However, these search methodologies are contingent upon the files or media being saved on the physical computer, and cannot be extended to files that are stored directly on the cloud.[192] Yet, each method offers some insight into why law enforcement needs a separate warrant for searching a cloud network account.

Arguably, the container view offers the most persuasive reason for why a separate warrant is necessary. The container view, in terms of computer searches, is contingent on the principle that the physical computer itself is the container; the law does not support defining the container as all of the user's computer data.[193] Thus, the warrant would cover the data the user saved within the container, and in the case of a computer, this data is saved on the computer's physical hard drive. Documents that are saved in a cloud network account are not located within the computer-container, and, furthermore, when a user chooses to save data on the cloud, he is purposely choosing *not* to place his data in a computer-container.

To provide further support, the law has already started to trend in this direction. For example, the Electronic Communications Privacy Act[194] and the Stored Wire and Electronic Communications

191. *See supra* Section I.

192. I acknowledge that some cloud programs, such as Dropbox, save an additional copy of document onto the user's hard drive. However, this changes the analysis regarding searching the cloud network. This Note assumes that the user is using the cloud service as the exclusive means to save their files and media, and there are no back-ups saved on the computer hard drive.

193. *See* discussion *supra* Section III(C)(1).

194. Electronic Communications Privacy Act, 18 U.S.C.A. §§ 2510–2522 (2002) (regulating the interception of transmitted electronic communications).

Act[195] inherently reject the view that a container encompasses communication the user has not saved in the computer-container, as these laws provide means of obtaining documents directly from a remote server or communications provider.[196] These laws show that Congress inherently recognizes that a user has the capability of using multiple electronic storage containers, and that one warrant does not cover all of them.

There is similar reasoning for why the sub-container method also does not allow an officer who is conducting a warrant search to access the cloud. If the sub-container view is applied to the computer, and the search is regulated to folders or portions of the hard drive, two things are evident.[197] First, the cloud is not a part of the hard drive, and cannot be classified a sub-container of the hard drive. Second, insofar as the cloud is considered a sub-container of the user's data storage, a separate warrant, which lists the cloud storage specifically, is necessary.

Similarly, "special" search restrictions also do not allow law enforcement to search the cloud. If the magistrate applies special restrictions to the search, such as limiting the search to only .JPG files, the officer cannot use that warrant to search the cloud for the .JPG files that may be located there.[198] The agent must continue to abide by the search parameters put forth in the particularity requirements in the warrant, and must obtain a second warrant if he feels the need to exceed the warrant's parameters.

Further support for the exclusion of the cloud under these methodologies is derived from searches of physical premises. For example, the law does not allow police to search for all physical papers related to drugs, and then access a storage container across town on the same warrant to search for more files related to drugs, simply because the police have a warrant to search for the type of document that may be stored there.[199] In this scenario, the police must seek two warrants because the police have established two separate sets of probable cause: first, probable cause to search the house for the papers, and second, probable cause to search the storage

195. Stored Wire and Electronic Communications Act, 18 U.S.C. §§ 2701–2725 (2002) (regulating the search of stored electronic communications).

196. 18 U.S.C. §§ 2703(b)(A), 2703(B)(i), 2703(B)(ii) (2002) (requiring a subpoena or warrant to obtain documents from a remote computing provider).

197. *See* discussion *supra* Section III(C)(2).

198. *See* discussion *supra* Section III(C)(3).

199. *Cf.* Groh v. Ramirez, 540 U.S. 551, 563 (2004) (describing the particularity requirements of a warrant, and noting that the warrant must describe, with particularity, the place to be searched or the items to be seized).

unit for papers. If the initial warrant specifically limits the search to the house, the police cannot use the commonality between the two sets of probable cause to enter the second location. This scenario is exactly what law enforcement faces when searching the cloud. If the storage locker is a physical computer, none of the search methodologies justify the search across town. Thus, the Fourth Amendment requires that a separate warrant be obtained to search a separate container.

Overall, because none of the existing computer search methods allows law enforcement to search the cloud, and the methods actually hold the commonality that they exclude the police from the cloud, the answer to the hypothetical remains the same. Law enforcement must obtain a separate warrant.

C. The Fourth Amendment's Warrant Requirement is Not Negated by an Exception

The final reason that law enforcement must obtain a warrant before searching the cloud is that the two warrant exceptions, which are arguably the most applicable, the third party doctrine and consent searches, do not negate the warrant requirement. The law has been trending in this direction for quite some time.

Recently, Justice Sotomayor criticized the third party doctrine in *United States v. Jones*.[200] She wrote:

> [T]his 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. . . . [W]hatever the societal expectation, 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.[201]

This passage from Justice Sotomayor's concurrence indicates two things. First, she believes that *Katz*'s existing expectation of privacy test can still be applied to emerging technologies.[202] However, this concept is contingent upon the idea that complete secrecy, especially in the digital world, should not be a prerequisite for Fourth Amendment protections.[203]

200. 132 S.Ct. 945, 957 (2012).

201. *Id.*

202. *See id.* (as indicated by the passage above).

203. *Id.*

As *Katz's* reasonable expectation of privacy test is satisfied,[204] the Fourth Amendment protects the cloud, and a warrant exception does not negate these protections. Thus, when a cloud network user saves his data to his personal cloud account, for the limited purposes of storing, protecting, and accessing his documents, he does not lose the Fourth Amendment's protections because he has entrusted his documents to a third party. Moreover, the privacy policies of cloud providers like Dropbox, which advertise that the company may look at documents for limited purposes,[205] does not implicate the third-party doctrine.

The law does not support stretching the third party doctrine to negate the Fourth Amendment's protections of the cloud just to allow law enforcement easier access to a user's stored data. The third party doctrine was meant to apply to situations where a user purposely puts information into the public sphere, foregoing his expectation of privacy; for example, when a defendant knowingly speaks about his criminal activities to a third party.[206] In *Hoffa*, the Court specified that the defendant had taken the risk in choosing in whom to place his trust, and had not been relying on the security of his hotel room, which was a constitutionally protected area.[207] However, a cloud network user is not taking the same type of risk; he is instead relying on the security of the "room." The user has not disclosed the contents of his files to the provider the way Hoffa told the informant his secrets. Nor has the user, in most cases, disclosed the files by creating a public network with others who may play a role analogous to that of the government informant. Instead, the user relies on Fourth Amendment protection via his expectation of privacy: he is in a constitutionally protected area, and no law enforcement agent can gain access to his room, or his cloud account, without a warrant.

Furthermore, returning to the mail analogy, a cloud network provider acts similarly to the USPS, transporting data (mail) from

204. *See supra* Section IV(A).

205. DROPBOX: SEC. TERMS, https://www.dropbox.com/security (last visited Mar. 26, 2012) ("Like most online services, we have a small number of employees who must be able to access user data for the reasons stated in our privacy policy (e.g., when legally required to do so). But that's the rare exception, not the rule. We have strict policy and technical access controls that prohibit employee access except in these rare circumstances.").

206. Hoffa v. United States, 385 U.S. 293, 301 (1966).

207. *Id.* at 302 ("[P]etitioner, in a word, was not relying on the security of the hotel room; he was relying upon his misplaced confidence that [the third party] would not reveal his wrongdoing.").

one location to another and holding it in the meantime.[208] If the USPS is suspicious of a package and brings it to a law enforcement agent's attention, and the agent wishes to look at the contents, he must obtain a warrant.[209] In *Van Leeuwen*, the Supreme Court clearly demonstrated that a third party's transportation or storage of somebody's materials does not automatically negate the expectation of privacy.[210] Accordingly, the third party doctrine does not negate the expectation of privacy, and therefore does not negate the warrant requirement.

Moreover, a cloud network provider is not the type of entity that may grant consent for law enforcement to search its user's account. For a third party to grant law enforcement access to the files, one characteristic must be present: joint ownership or control over the area to be searched.[211] In the case of an internal computer network, typically, a second factor is also involved: the person whose area is being searched has knowingly placed something, whether it is a physical file or computer data, into the public eye.[212] Consequently, law enforcement often can surpass the warrant requirement when searching a computer network because a user has knowingly placed his data into the public eye, where other users can view it, and the user also knows that there is joint ownership or control over the network, as a network administrator often runs and polices network use.[213]

In the case of the cloud, neither of these factors is present. First, cloud network users and providers do not have joint ownership and control over a cloud network user's *data*; in fact, the user regains control over his materials.[214] The cloud network provider is merely a

208. *See Ex Parte* Jackson, 96 U.S. 727, 733 (1878) (describing how the federal mail service carries mail and the constitutional implications of their temporary possession).

209. United States v. Van Leeuwen, 397 U.S. 249, 253 (1970) (upholding law enforcement's detention of the package for the time reasonable to gain a warrant).

210. *Cf. id.* (not negating reasonableness factor of the timing issue because of a warrant exception).

211. *See* Illinois v. Rodriguez, 497 U.S. 177, 181 (1990) (noting that the Fourth Amendment's general prohibition of warrantless entry of a person's home does not apply where voluntary consent has been obtained).

212. *See supra* note 172 and accompanying text.

213. *See id.*; *see also supra* Section III(B)(2).

214. *See, e.g.,* DROPBOX: TERMS OF SERVICE, https://www.dropbox.com/terms (last visited Mar. 26, 2012) ("You retain full ownership to your stuff. We don't claim any ownership to any of it.").

holding box, and typically does not access or look at a user's data without permission, nor does the provider police what the user places in the account by examining every file.[215] This is not the same type of joint ownership and control that occurs in consent cases, where two people are living together and sharing the space.[216] The cloud provider merely provides the space and that is all. Therefore, the second factor closely ties into the first. A cloud network user has not knowingly exposed his data to the public the way that somebody who is using a business computer network has. Unless the cloud network user chooses to knowingly share his files with other users, the user is engaged in personal and private use of the cloud. In a computer network or consent search case, the user knowingly places his files where others can access them. This is not the case with the cloud.

Thus, because a warrant exception does not negate the warrant requirement, the answer to the hypothetical remains the same.

V. CONCLUSION: GET A WARRANT

The Ninth Circuit in *Comprehensive Drug Testing* noted, in dicta, that "[w]here computers are not near each other, but are connected electronically, the original search might justify examining files in computers many miles away, on a theory that incriminating electronic data could have been shuttled and concealed there. The advent of fast, cheap networking has made it possible to store information at remote third-party locations[.]" [217] The Ninth Circuit then recognized that requesting that people not utilize current technology to store their files and media was "no answer," as it "is no longer a peculiarity or luxury of the very rich; it's a way of life."[218]

The Fourth Amendment protects, and must continue to protect, the cloud network. In the hypothetical discussed at the beginning of this Note, the law enforcement agent's next step would be to obtain a second warrant to search the suspect's cloud account. Through his

215. *See, e.g., id.* ("You are solely responsible for your conduct, the content of your files and folders, and your communications with others while using the Services.").

216. *But see Rodriguez*, at 188-189 (1990) ("the surrounding circumstances [of the search] could conceivably be such that a reasonable person would doubt its truth and not act upon it without further inquiry. As with other factual determinations bearing upon search and seizure, determination of consent to enter must "be judged against an objective standard: would the facts available to the officer at the moment. . . 'warrant a man of reasonable caution in the belief' "that the consenting party had authority over the premises?").

217. United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc).

218. *Id.* at 1177.

search pursuant to the first warrant, the agent has established probable cause to support a warrant application to search the suspect's cloud account. Thus, after his warrant is reviewed and possibly granted, he may either show the warrant to the suspect and request, politely, that he be given access to the cloud account, or he may bring the warrant to the cloud network provider and obtain the data, or means to access the data, directly from them.

These simple steps provide law enforcement with a clear-cut rule regarding cloud network searches and seizures. Courts then must make known to law enforcement that the Fourth Amendment protects the cloud by refusing to grant overly broad warrants and by suppressing evidence that law enforcement obtains from the cloud when it is a result of an unreasonable search or seizure.

Society already recognizes that the Fourth Amendment protects the cloud, and the law must respect this protection. For example, many people believe that their materials in the cloud are protected, and would be outraged if their cloud network service provider simply turned their documents over without informing them.[219] Even major companies are calling for an overhaul of online privacy law.[220] Therefore, the current legislation and departmental policies that have trended towards requiring additional warrants for cloud network searches, instead of unconstitutionally negating the requirement all together, must continue to evolve. Law enforcement agencies must adopt guidelines like those described in the Department of Justice's guide, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*,[221] which urges local agencies to adopt an operational policy that requires agents to obtain a second warrant when the data they seek is stored elsewhere in the country.[222] Further, the legislation must recognize the Fourth Amendment's protections of the cloud by refusing to codify the procedure for searches of a cloud network account pursuant to anything less than a warrant based on probable cause.

---

219. Horrigan, *supra* note 10 (reporting high levels of concern from cloud network users when asked about how they would feel if the cloud network provider took various actions with their data).

220. *See, e.g.,* DIGITAL DUE PROCESS, http://digitaldueprocess.org (last visited Oct. 30, 2012) (for information about the organization, its goals, and a list of its current members).

221. Office of Legal Educ. & Exec. Office for United States Attorneys, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, vii (2009), *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf (noting that the guide is not binding, and is simply meant to be used as guidelines).

222. *Id.* at 90 ("If the agent comes across evidence of a crime that is not identified by the warrant, it may be safe practice to obtain a second warrant.").

Until law enforcement routinely recognizes the Fourth Amendment protects the cloud network, an additional added protection is to continue to allow magistrates to impose restrictions on computer warrants. Magistrates can do this by strictly enforcing the particularity requirement and by placing strict parameters on computer warrants. If a magistrate grants a warrant for a computer hard drive, he should specifically note that the search cannot expand onto the cloud. Then, if the agent oversteps his bounds, the defense may use the warrant's imposed limitations to suppress any data seized unlawfully from the cloud. Restrictions such as limiting the search parameters to the physical hard drive, requiring searches to be conducted on copies of the hard drive instead of the actual computer, or requiring that search of the computer takes place off-line[223] will prevent law enforcement from even "accidently" exceeding the bounds of the warrant. If magistrates clearly and consistently apply restrictions to computer search warrants and suppress unlawfully seized evidence from the cloud, law enforcement will get the message: if they want to go beyond the physical hard drive, they *must* obtain a separate warrant.

These additional steps will not interfere with law enforcement's ability to continue to perform effective searches and seizures. Users of the cloud network have not given up their expectation of privacy simply because they choose to use the best means of data storage available. When the user has not shared the documents through a network beyond one he has created for himself, he has not exposed the documents to the public and maintains his reasonable expectation of privacy. The law must recognize this and must be willing to develop criteria for the expectation of privacy to meet the demands of the evolving technological world.

223. In some cases, data saved in a cloud network account is not accessible from a device that is off-line.