William & Mary Law Review

Volume 56 (2014-2015)
Issue 6

Article 8

5-22-2015

Obscured by Clouds: The Fourth Amendment and Searching Cloud Storage Accounts Through Locally Installed Software

Aaron J. Gold

OBSCURED BY CLOUDS: THE FOURTH AMENDMENT AND SEARCHING CLOUD STORAGE ACCOUNTS THROUGH LOCALLY INSTALLED SOFTWARE

TABLE OF CONTENTS

INTRODUCTION

Suppose the police suspect Winston of possessing child pornography on his computer. Acting on that suspicion, authorities secure a warrant to seize and search Winston's computer and all other digital storage mediums at his residence. However, when combing through the files stored on Winston's devices, the police find no trace of the illicit images.

To ensure that the search is thorough, law enforcement officers begin to open separate programs installed on the machine, searching for documents hidden within the applications. One program they open is Microsoft's OneDrive,[1] which provides a list of files that are stored in Winston's cloud storage account. The files, however, are not actually present on his computer's hard drive, or on any other storage medium he possesses. The police do this despite the fact that their warrant specifies only their right to search the contents of Winston's physical drive. Regardless, they can see the files available for download and they seize them anyway. Later, when checking the downloaded data, the police do not find any evidence of child pornography, but they do find documents incriminating Winston of another crime. As it turns out, Winston does not traffic child porn, but he was in fact committing bank fraud.

This seemingly small exploration might appear innocuous on its face, but it carries broad implications for search and seizure law in a digital environment. The warrant gave the police license to search files on Winston's computer and the storage media he owned, but in this instance they did not find incriminating data there. Instead, the police discovered evidence on a remote platform that Winston's computer could access, but the evidence was not stored on his actual computer.

The Fourth Amendment to the Constitution protects citizens against warrantless searches and seizures of their "homes, papers, and effects."[2] Nevertheless, this guarantee is not unconditional; the

1. For the purpose of this example, assume that this is the version of the OneDrive application that comes preinstalled on the Windows 8 operating system.

2. *See* U.S. CONST. amend. IV.

Supreme Court has recognized several exceptions.[3] Courts face the challenge of applying these standards as society and technology evolve beyond the immediate foresight of the Fourth Amendment's drafters. Winston's predicament highlights not only the general Fourth Amendment difficulties intrinsic to searching computers, but also the added complications of privacy and the Internet.

The aforementioned hypothetical dealt specifically with issues surrounding cloud computing. Cloud computing is a colloquial term for computer services provided remotely over the Internet, rather than by direct local access.[4] Cloud computing has both a private and a public form. A private cloud hosts services to a limited number of people,[5] whereas a public cloud is one offered through a third-party service to general consumers.[6] In particular, cloud storage is a term for storing data and files on remote drives.[7] A user essentially sends their files to another location where the files are redundantly preserved.[8]

Companies providing public cloud storage maintain user data on clusters of networked servers at off-site locations.[9] Users can upload data to cloud servers in various ways, including placing files in a folder that synchronizes with the storage service,[10] accessing the account directly from an Internet browser, or doing so through cloud-linked software installed on a computer.[11] Generally, cloud accounts permit users to access their data from any Internet-capable

---

3. *See infra* Part III.

4. Margaret Rouse, *Cloud Computing*, TECH TARGET, http://searchcloudcomputing.techtarget.com/definition/cloud-computing [http://perma.cc/HCV3-R6FU] (last visited Apr. 11, 2015).

5. *Id.*

6. *Id.*

7. Mickey Meece, *A User's Guide to Finding Storage Space in the Cloud*, N.Y. TIMES, May 17, 2012, at B6; Walter S. Mossberg, *Learning About Everything Under the "Cloud,"* WALL ST. J., May 6, 2010, at D1.

8. *See* Meece, *supra* note 7.

9. Jonathan Strickland, *How Cloud Computing Works*, HOWSTUFFWORKS, http://computer.howstuffworks.com/cloud-computing/cloud-computing.htm [http://perma.cc/V3VW-8T86] (last visited Apr. 11, 2015).

10. Ian Paul, *Top 15 Cloud Storage Tips and Tasks*, PCWORLD (May 6, 2012, 6:00 PM), http://www.pcworld.com/article/255072/top_15_cloud_storage_tips_and_tasks.html [http://perma.cc/P485-GHG5].

11. *See* Rouse, *supra* note 4. Linking software to cloud services creates a direct connection between a user and his or her storage account, without requiring the user to access the site independently from the Internet. *Id.*

device that has a web browser or cloud-linked software.[12] Winston's computer hosted cloud-linked software. The files the police collected via that program were *not* on his hard drive, and the warrant only specified files that were actually on his machine. The question becomes whether the existence of software on the hard drive with direct access to outside files permits the police to broaden their search.

The backbone of Fourth Amendment jurisprudence developed prior to the advent of personal computers, and its modern application can be fraught with difficulty. Even applying these principles to storage mediums that police have *actually seized* proves troublesome,[13] particularly in the context of the plain view exception to the warrant requirement.[14] Those uncertainties only get murkier when physical computers and the Internet collide. Recently, courts have begun to address these issues in a modern digital context,[15] but scholarship on the subject is limited.[16]

The number of people storing data though cloud services is increasing.[17] Soon, if not already, Winston's plight will cease being hypothetical. There must be clarity as to whether law enforcement can use locally installed software to access data stored on cloud

---

12. Mossberg, *supra* note 7.

13. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 537 (2005).

14. *See* United States v. Galpin, 720 F.3d 436, 447-48 (2d Cir. 2013); Kerr, *supra* note 13, at 576; *infra* Part III.A (providing a more in-depth description of the plain view doctrine).

15. *See, e.g.*, United States v. Cotterman, 709 F.3d 952, 965 (9th Cir. 2013) (discussing cloud storage and the Fourth Amendment within the scope of the distinct border search doctrine); United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (discussing the Fourth Amendment and e-mail).

16. Professor Orin Kerr, a leading authority on the Fourth Amendment in the digital context, specifically notes that such scholarly inquiry is sparse. Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1006 (2010). Much of the scholarly analysis of the Fourth Amendment and cloud storage has come in the form of other student notes. *See, e.g.*, Derek Constantine, Note, *Cloud Computing: The Next Great Technological Innovation, the Death of Online Privacy, or Both?*, 28 GA. ST. U. L. REV. 499, 514-15 (2012); David A. Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2205-06 (2009); William Jeremy Robison, Note, *Free at What Cost?: Cloud Computing Under the Stored Communications Act,* 98 GEO. L.J. 1195, 1209 (2010).

17. Karen A. Frenkel, *Demand for Cloud Storage: No End in Sight*, CIO INSIGHT (Sept. 6, 2013), http://www.cioinsight.com/it-strategy/cloud-virtualization/slideshows/demand-for-cloud-storage-no-end-in-sight.html [http://perma.cc/ZV7T-XNDL].

servers—but not on the local machine—because they can see and access the files when searching a suspect's computer. Winston could argue that he had a separate expectation of privacy, and that the police had no right to comb through his cloud storage. The police could then counter that such an expectation is not reasonable, and that the Fourth Amendment does not protect information stored on the Internet. Alternatively, authorities may argue that even if such a protection exists, they were justified in bypassing the warrant requirement because the files were in plain view of their lawful search, or because of the risk that Winston could destroy the data via remote access.

Others have discussed expectations of privacy in cloud storage in different contexts, and some have grappled with issues similar to those discussed in this Note.[18] This Note, however, will focus on the relationship between cloud storage and locally installed software on a home computer. It will argue that a proper reading of the Fourth Amendment and the surrounding circumstances vindicates Winston and constrains the police. Under the Fourth Amendment, the police do not have an automatic right to rifle through cloud storage via software installed on computers they search. Part I of this Note will discuss the general Fourth Amendment problems associated with searching physical hard drives that the police have under their control. Part II will argue that consumers have a reasonable expectation of privacy in data they keep in cloud storage. Part III will demonstrate why cloud data that is accessible through local software does not come under the umbrella of the plain view doctrine or the exigency exception to the warrant requirement. Finally, Part IV will offer a solution that courts may employ to properly preserve Fourth Amendment protections, as well as to enable the police to carry out their mission to enforce the law.

---

18. *See, e.g.*, Constantine, *supra* note 16, at 525-28 (discussing the third-party doctrine with regard to different cloud storage providers); Nicolette Lotrionte, Note, *The Sky's the Limit: The Border Search Doctrine and Cloud Computing*, 78 BROOK. L. REV. 663, 664-65 (2013) (examining how cloud computing and storage intersect with the expanded powers of the border search doctrine); Robison, *supra* note 16, at 1209-18 (discussing cloud storage providers and the Stored Communications Act); Mark Wilson, Comment, *Castle in the Cloud: Modernizing Constitutional Protections for Cloud-Stored Data on Mobile Devices*, 43 GOLDEN GATE U. L. REV. 261, 263-64 (2013) (discussing cloud computing in the mobile context).

I. BACKGROUND

The Fourth Amendment preserves the right of people to "be secure in their persons, houses, papers, and effects[ ] against unreasonable searches and seizures;" and warrants, supported by probable cause, must "particularly describ[e] the place to be searched, and the persons or things to be seized."[19] The Amendment's central concern is protecting individual liberty and providing security from government intrusion.[20]

A. A Reasonable Expectation of Privacy

The Fourth Amendment is not absolute. Its protections shield individuals only in a realm in which they can maintain a reasonable expectation of privacy.[21] With the 1967 watershed opinion *Katz v. United States*, the Court recognized for the first time that a reasonable expectation of privacy is critical to Fourth Amendment search and seizure analysis.[22] In that case, the police eavesdropped on Katz without a warrant as he made a phone call from a telephone booth.[23] The Court struck down his conviction, ruling that such action constituted a search under the Fourth Amendment, and therefore required judicial approval.[24]

Rejecting a prior approach, which indicated that there needed to be some physical trespass to offend the Fourth Amendment,[25] the Court concluded that Katz justifiably relied on an expectation of privacy, and that warrantlessly violating that expectation breached his rights.[26] This is because the Fourth Amendment, as the Court decreed, protects people, and is not limited to particular places.[27]

---

19. U.S. CONST. amend. IV.
20. *See* Boyd v. United States, 116 U.S. 616, 630 (1886).
21. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
22. *Id.*
23. *Id.* at 349 (majority opinion).
24. *See id.* at 359.
25. *Id.* at 353.
26. *Id.* at 359.
27. *Id.* at 351. That is not to say that "places" are not important concerns. This provision protects people in part by specifically limiting the places that law enforcement may permissibly search. *Id.*

For an expectation of privacy to be reasonable, not only must the individual have a subjective expectation of privacy, but also society as a whole must objectively believe that such an expectation is sensible.[28] Moreover, to be reasonable, that objective expectation must be justifiable given the facts of the surrounding circumstances.[29]

Part of the Court's implicit reasoning in *Katz* was that the "vital role that the public telephone has come to play in private communication" established the reasonable expectation of privacy in Katz's telephone conversation.[30] This indicates that what makes privacy expectations reasonable is far from a static determination. Rather, expectations shift as technology advances.[31] The Court has already addressed related matters, including issues involving aerial surveillance[32] and infrared scanning of homes.[33] Most recently, the Court recognized the role that cell phones have come to play in modern society and the associated privacy interests that citizens have in these devices.[34]

B. General Fourth Amendment Challenges with Computers

Courts now consistently recognize that people possess a reasonable expectation of privacy in their computers.[35] Thus, searching one

---

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

29. *See* Smith v. Maryland, 442 U.S. 735, 740 (1979).

30. *See* Katz, 389 U.S. at 352.

31. United States v. Jones, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring) ("[T]he Katz test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes.").

32. Florida v. Riley, 488 U.S. 445, 451 (1989) (holding that observing a citizen's property from a legal altitude did not constitute a search).

33. Kyllo v. United States, 533 U.S. 27, 40-41 (2001) (holding that using an infrared heat scanner on a home was a search, and was impermissible without a warrant).

34. Riley v. California, 134 S. Ct. 2473, 2485 (2014) (requiring that police generally obtain a warrant before they can search a cell phone). That is not to say the Court was not cognizant of the privacy interest in cell phones prior to *Riley*. *See* City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010) ("Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy.").

35. *See, e.g.*, United States v. Heckenkamp, 482 F.3d 1142, 1146 (9th Cir. 2007) ("Individuals generally possess a reasonable expectation of privacy in their home computers." (quoting United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004)); Trulock v. Freeh, 275

without its owner's consent requires a warrant or a valid exception to the warrant requirement.

Professor Orin Kerr likens the computer hard drive to any other variety of sealed container in which individuals would retain a privacy right.[36] Yet, he acknowledges inherent Fourth Amendment problems that arise when searching a computer hard drive. It is difficult to describe with particularity the place to search given the vast size of a hard drive and the innumerable places the owner might hide data.[37] Furthermore, courts struggle with the fact that there is currently no way to know with certainty the type of data a file contains without examining the contents closely.[38]

One tempting approach is to limit a computer search to certain types of files—files specifically designed to contain data that might be used as evidence of the pertinent crime.[39] That method would indeed accord with the spirit of the Fourth Amendment's command of particularity for its warrants,[40] and some courts have tried to take this approach when issuing warrants.[41]

F.3d 391, 403 (4th Cir. 2001); Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001); *see also* United States v. Ziegler, 474 F.3d 1184, 1190 (9th Cir. 2007) (recognizing a reasonable expectation of privacy in an office computer); Leventhal v. Knapek, 266 F.3d 64, 73 (2d Cir. 2001) (same).

36. Kerr, *supra* note 13, at 549.

37. *Id.* at 566.

38. United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc). Authorities can perform computer searches through specialized forensic software, or by simply opening a file and viewing the contents for themselves.

39. For example, if the police are looking for evidence of child pornography, they could limit their search to file types that support images or video. By contrast, if the police are investigating bank fraud, they could reserve their inquiry for files that support text editing. *See* THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION 579-80 (2008).

40. Much motivation for the Fourth Amendment's warrant requirement grew from anger toward general warrants and writs of assistance in colonial America. THOMAS N. MCINNIS, THE EVOLUTION OF THE FOURTH AMENDMENT 15-20 (2009). Those measures afforded British customs officers the ability to search colonial homes and buildings for any suspected contraband, imposing no limitations on what authorities might seek. WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING 307, 320-21, 537-38 (2009).

41. United States v. Gleich, 397 F.3d 608, 611 (8th Cir. 2005) (upholding a warrant limiting the search of a suspect's computer to files that could "contain photographs, pictures, visual representations or videos in any form that include sexual conduct by a minor") (internal quotation marks omitted); State v. Maxwell, 825 A.2d 1224, 1234 (N.J. Super. Ct. Law Div. 2001) (authorizing a warrant to specifically search "computer address books" in investigating a suspect's phone calls to minor sexual assault victims).

Ultimately, however, such limitations might not be feasible given the realities of digital storage. Users often employ file types including ".jpeg" for images,[42] ".avi" for video,[43] ".docx" for text documents in Microsoft Word,[44] and countless other types for countless other purposes. It would be quite simple to segregate a search by file type depending on the focus of the search, but that more than likely would be a fruitless exercise. By changing a few letters in a file's name, one can make one form of data appear to be another.[45] Such a change would make a directed search for specific file types ineffective and require a much more thorough examination in order to determine what a computer file stores.[46] Furthermore, users can compress data to make files appear much smaller than their normal size,[47] which, like data encryption,[48] could confound authorities.

Additionally, there is nothing stopping someone engaged in bank fraud from taking pictures of their documents and storing them as *actual* images, as opposed to changing a file type. The same is true for someone seeking to hide illicit images in a word processing document.

The difficulty in searching computer files leads to tricky applications of the plain view doctrine, a recognized exception to the warrant requirement.[49] In order to apply that exception, the incriminating character of a piece of evidence must be readily apparent,

---

42. *.Jpeg*, PC.NET, http://pc.net/extensions/file/jpeg [http://perma.cc/VZ8P-ES52] (last updated June 2, 2009).

43. *.Avi*, PC.NET, http://pc.net/extensions/file/avi [http://perma.cc/X3TQ-8G7D] (last updated May 20, 2009).

44. *.Docx*, PC.NET, http://pc.net/extensions/file/docx [http://perma.cc/LY5B-YKGE] (last updated Oct. 17, 2009).

45. *See* Kerr, *supra* note 13, at 545-47; *How to Change a File Extension in Windows*, MEDIACOLLEGE.COM, http://www.mediacollege.com/microsoft/windows/extension-change.html [http://perma.cc/5HZ5-HJX4] (last visited Apr. 11, 2015).

46. United States v. Galpin, 720 F.3d 436, 444 (2d Cir. 2013); CLANCY, *supra* note 39, at 581-83; Kerr, *supra* note 13, at 545.

47. Andrew Vahid Moshirnia, Note, *Separating Hard Fact from Hard Drive: A Solution for Plain View Doctrine in the Digital Domain*, 23 HARV. J.L. & TECH. 609, 612 (2010).

48. *Id.* at 612-13.

49. *Id.*

among other things.[50] As mentioned, this is not always the case with a computer file.

The Second Circuit dealt with some of these computer search difficulties in *United States v. Galpin*. In that case, the police searched a convicted sex offender's computer for violating a registration requirement for an online screen name.[51] While conducting the search, investigators opened various types of files, including images and video, and inadvertently found depictions of child pornography.[52] When remanding the case to the district court, the Second Circuit warned of a need for heightened sensitivity to warrant particularity during computer searches.[53] It called upon the fact finder to determine whether a search for registration violations truly necessitated opening video files.[54]

The Second Circuit's attempt to constrain a broad interpretation of the plain view doctrine does not address the aforementioned issues. It fails to account for the fact that file extensions might be changed, or for content hidden in files that is different from their natural format. Moreover, as the opinion admits, authorities still have no way to tell what is inside a file without close examination.

This combination of issues underscores the problem with using access to individual computers as permission to search data stored on the cloud. If law enforcement obtains a warrant to search a whole computer for incriminating evidence, "the government may claim

---

50. Horton v. California, 496 U.S. 128, 136-37 (1990). For a more in-depth discussion of the plain view criteria and how attempts to search cloud storage complicate this approach, see *infra* Part III.A .

51. *Galpin*, 720 U.S. at 440. Originally, the police's warrant was overbroad and permitted a search of the computer for any "violations of Penal Law statutes, Corrections Law statutes and or Federal statutes." *Id.* The district court redacted the warrant believing that the valid portions were severable from the invalid portions. *Id.* at 449. The Second Circuit vacated that judgment and remanded the case for further proceedings to develop a factual record to help determine severability. *Id.* at 439. The court held that if the invalid portions of the warrant could not be severed, the initial search itself would be unconstitutional. *Id.* at 451.

52. *Id.* at 444.

53. *Id.* at 447. The opinion notes that courts should pay special attention to the particular nature of a crime, as the expanse of information under the plain view doctrine could potentially turn any warrant to search a computer into a general warrant for criminal activity. *See id.*

54. *Id.* at 452.

that the contents of every file it chose to open were in plain view."[55] There may indeed be files stored similarly to Winston's: namely, that they exist on servers that connect to local computers via the Internet, but with no copies stored on the actual machine. Despite this, programs installed on his computer could detect those files and download them directly, without having to access external websites through a web browser. If all files on a computer are in plain view, then police seemingly have a carte blanche to search information accessible through programs installed on the hard drive. This would include cloud accounts linked to local software.

The balance of this discussion will demonstrate why law enforcement officers do not have such power. First, Part II lays out why consumers truly can retain an expectation of privacy in their cloud storage accounts. Second, Part III will examine why the plain view doctrine and other exceptions do not apply to cloud files accessible through local software.

II. CLOUD STORAGE AND A REASONABLE EXPECTATION OF PRIVACY

A. Is There a Reasonable Expectation to Begin With?

To claim constitutional protections, users must have a reasonable expectation of privacy in their cloud files.[56] Affirmatively stating that the Fourth Amendment extends to cloud content requires acknowledging that people can maintain a reasonable expectation of privacy in their general Internet accounts. Courts appear increasingly willing to confer such protection on e-mail,[57] and at least one leading Fourth Amendment commentator recognizes that user reliance on password protection can create a reasonable privacy expectation for Internet accounts.[58]

---

55. *Id.* at 447. Consequently, if the government finds evidence of a crime they were not searching for, they may still use that evidence to prosecute the suspect. *Id.*

56. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

57. United States v. Warshak, 631 F.3d 266, 282 (6th Cir. 2010); Quon v. Arch Wireless Operating Co., 529 F.3d 892, 905-06 (9th Cir. 2008) (analogizing the content of e-mails to the content of letters), *rev'd sub nom. on other grounds*, City of Ontario v. Quon, 130 S. Ct. 2619 (2010).

58. 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.6(f) (4th ed. 2004); *see also Katz*, 389 U.S. at 352 (majority opinion) ("One who occupies [a telephone booth and] shuts the door behind him ... is surely entitled to assume that the words

Supreme Court decisions offer no exclusive test for what makes expectations of privacy reasonable, and Professor Kerr suggests that courts employ various models in reaching their conclusions.[59] No method is mutually exclusive, and courts ultimately may rely on syntheses of these approaches in arriving at their outcomes.[60]

In what Professor Kerr terms the "probabilistic" model, a reasonable expectation of privacy hinges "on the chance that a sensible person would predict that he would maintain his privacy."[61] This approach requires consideration of the societal norms at play.[62]

Societal norms are indeed evolving and doing so in stride with technological progress. Most citizens would not view data in remote storage as being any less confidential than data on their home computers.[63] As previously stated, however, relying on one model and considering social norms and practice is not the exclusive way to deduce a reasonable expectation of privacy. Statutory law is also instructive.

---

he utters into the mouthpiece will not be broadcast to the world.").

59. Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 505 (2007). Kerr points out that these models cannot serve as the sole guide to determining Fourth Amendment protection, but they are useful in examining how courts come to their decisions. *See id.* at 531-42.

60. *Id.* at 508.

61. *Id.*

62. *Id.* at 508 n.19 (citing Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978)) (discussing "understandings that are recognized and permitted by society"); *see* Georgia v. Randolph, 547 U.S. 103, 111 (2006) ("The constant element in assessing Fourth Amendment reasonableness in the consent cases, then, is the great significance given to widely shared social expectations."); Minnesota v. Olson, 495 U.S. 91, 98 (1990); State v. Hempele, 576 A.2d 793, 802 (N.J. 1990); Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 124 (2002); Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 619 (2011) (arguing that courts should apply a principle of "technosocial continuity" of viewing privacy, accounting for how advancing technology can make citizens more vulnerable); *see also* Kerr, *supra* note 13, at 536.

63. State v. Bellar, 217 P.3d 1094, 1110-11 (Or. Ct. App. 2009) (Sercombe, J., dissenting); *see also* United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc); Couillard, *supra* note 16, at 2205.

1. Positive Model of Privacy and the Electronic Communications Privacy Act

A simultaneous alternative and complement to considering social norms is the "positive" model of Fourth Amendment protection. This approach requires the court to ask whether some law, other than the Fourth Amendment, prohibits government intrusion.[64] The notion is that there is a reasonable expectation of privacy if the government needs to circumvent one of its own laws to access information.[65]

There is no specific government statute dealing with data in cloud storage. In fact, the primary law addressing privacy and data passing through the Internet is Title II of the Electronic Communication Privacy Act of 1986 (ECPA), otherwise known as the Stored Communications Act (SCA).[66] The SCA recognizes two types of Internet services—Electronic Communication Services (ECS)[67] and Remote Computing Services (RCS)[68]—and creates a privacy framework for each by prohibiting disclosure of storage contents, except in limited circumstances.[69] This law is nearly thirty years old. Courts and commentators alike take on the thorny duty of applying the SCA's provisions to modern technology, and its compatibility with cloud storage is far from clear. It is necessary to analyze cloud storage under the dual frameworks offered in the SCA, beginning first with the ECS, which ultimately suffers a hazy application and, as currently written, likely would not encompass cloud storage.

a. Electronic Communication Services

The Electronic Communications Services (ECS) provision applies to services capable of "send[ing] or receive[ing] ... electronic communications."[70] Strictly speaking, users with cloud storage accounts

64. Kerr, *supra* note 59, at 516-18.

65. *Id.* Additionally, this approach asks whether the public could already access such information at the time of the alleged instruction. *See id.*

66. 18 U.S.C. §§ 2701-2712 (2012).

67. *Id.* § 2702(a)(1).

68. *Id.* § 2702(a)(2).

69. *Id.* § 2702(a)-(c).

70. *Id.* § 2510(15).

might not employ them for pure communication from one person or entity to another if the users' primary purpose is preserving their own data. Regardless, the law broadly defines electronic communication to include "signs, signals, writings, images, sounds, data or intelligence of any nature."[71] Cloud storage is more than capable of transmitting the sort of media defined by statute,[72] and nowhere does the law limit the concept of communication to transmissions involving two or more parties. Indeed, a broad understanding of communicative media goes hand in hand with an expansive view of communication. Cloud account holders can share their materials with other account holders, and more than one person can use the same account from different locations.[73] It is premature to assume as a matter of course that users do not use this sharing function as a surrogate method of communication.

Alternatively, cloud storage permits communication between a single user's individual devices, sometimes with outright synchronization between them.[74] As such, no reason exists to exclude cloud storage categorically from consideration as an ECS. Furthermore, there are other commentators that consider cloud storage analogous to e-mail accounts, which would gain clearer protection under the law.[75]

There are other requirements necessary for the ECS to apply. For example, storage must be "temporary[,] intermediate[,] ... [and] incidental to the electronic transmission," and "for purposes of backup protection."[76] The Ninth Circuit construed the term "backup" narrowly: a file must serve as a spare copy.[77] If the remote storage is the only place where the user keeps the data, it would not be a backup, and thus would not receive statutory protection.[78] Additionally,

---

71. *Id.* § 2510(12).

72. *See* Strickland, *supra* note 9.

73. For example, members of the *William & Mary Law Review* share a cloud storage account provided by Dropbox. All members have the password and use the account to pool information to ready each issue for publication.

74. Real time synchronization between devices is an example of when devices are actively communicating with each other. *See* Paul, *supra* note 10.

75. Wilson, *supra* note 18, at 273.

76. 18 U.S.C. § 2510(17)(A)-(B).

77. *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1077 (9th Cir. 2004).

78. *See id.*

cloud storage has the possibility of long-term data protection.[79] There is nothing inherently temporary about this data, and there is no way to glean a user's intended use ex ante merely from the appearance of files in storage.

b. Remote Computing Services

The Stored Communications Act's Remote Computing Services (RCS) provisions grant cloud storage a measure of privacy protection that is not as stringent as a full warrant requirement, though not without some difficulty. An RCS must contain content, be a "computer storage or processing service[ ] by means of an electronic communications system,"[80] and receive data from users electronically.[81] Additionally, the service must be maintained "solely for the purpose of providing storage or computer processing services to such subscriber or customer, *if the provider is not authorized to access* the contents of any such communications for purposes of providing any services other than storage or computer processing."[82]

Cloud storage satisfies the first of the necessary elements: it is by its very nature storage transmitted electronically, and the transferred files make up the content.[83] The last two requirements, however, lead some commentators to believe that cloud accounts may not fall under the Act's umbrella.[84] A primary concern is that business models for many cloud providers include accessing and employing user-uploaded data for advertising and other purposes.[85] Providers often gain consent for such actions within the terms of service, which users agree to when registering. The claim then becomes that users are no longer transmitting data *solely* for the purposes of storage and processing.[86]

---

79. Robison, *supra* note 16, at 1209.
80. 18 U.S.C. § 2711(2).
81. *Id.* § 2702(a)(2)(A).
82. *Id.* § 2702(a)(2)(B) (emphasis added).
83. *See supra* notes 4-12 and accompanying text.
84. Robison, *supra* note 16, at 1208-09.
85. *Id.* at 1213-14.
86. *Id.* at 1215-16. For discussion on how ToS agreements relate to the third-party doctrine, see *infra* Part II.B.

Careful reading of the statute does not preclude considering a service to be an RCS, even if it retains the ability to make use of the data in ways other than exclusively for storage. The law indicates that the purpose of services must be limited to storage and processing *unless* the user has authorized the provider to access his data for another reason.[87] Many service agreements do just that,[88] and courts seem willing to use those permissions to preserve application of the SCA.[89]

Necessarily, the extent to which the RCA applies depends on what the terms of service say. In a situation where files are stored on a cloud via local software, police would have no way of knowing if files came under RCS protection unless they did some investigation into the nature of the user agreement with the cloud provider.

2. The Current Law's Future and Policy Judgments

It requires noting that as the ECPA currently stands, the privacy protections of the SCA technically dissolve 180 days after data is first stored in an ECS,[90] and RCS services gain even less protection from an outright government search.[91] There are some courts that consider these permissive privacy elements to be unconstitutional.[92] In addition, as noted, statutory protection is but one foundation for a reasonable expectation of privacy to stand, and the courts may adopt a litany of approaches that work together. Even if the SCA suffers an imperfect application in the cloud-computing context, progressing social norms help buttress the notion that people can reasonably expect their data to remain concealed from government eyes. Indications from Congress show that some lawmakers share a similar view.

87. 18 U.S.C. § 2702(a)(2)(B).

88. *Terms of Service*, YOUTUBE (June 9, 2010), http://www.youtube.com/t/terms [http://perma.cc/KS6M-J33M].

89. Viacom Int'l, Inc. v. Youtube Inc., 253 F.R.D. 256, 264 n.8 (S.D.N.Y. 2008).

90. *Id.* § 2703(a).

91. *Id.* § 2703(b).

92. *See* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010); *see also* Kerr, *supra* note 16, at 1043.

The ECPA was an attempt by Congress to address privacy concerns that existed at the time.[93] Some current members recognize that the ECPA's limited provisions no longer comport with the realities of modern technology.[94] In 2013, representatives in both chambers introduced legislation that would eliminate the 180-day rule and require warrants regardless of how long users keep data in electronic storage.[95] Although each bill received favorable consideration, neither was enacted.[96]

The changing tides in Congress, along with the societal assumption that there is privacy in online accounts, provides mounting justification for courts to draw a normative policy decision favoring expectations of privacy in cloud storage. Professor Kerr notes that from a realist perspective, changing societal assumptions may often be the driving factor behind the Supreme Court's rationale.[97] He explains that this is what occurred in *Katz*, in which the Justices considered and weighed the vital role that the telephone had come to play in society.[98]

This approach is on display in *Kyllo v. United States*, which held that warrantless use of infrared technology to scan the interior of a home violated the Fourth Amendment.[99] The Court acknowledged that technology has affected citizens' privacy rights under the Fourth Amendment,[100] but noted that it must take a long view of

---

93. *Electronic Communications Privacy Act: Hearings on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties & the Admin. of Justice of the H. Comm. on the Judiciary*, 99th Cong. 6-8 (2013) (statement of Sen. Pat Leahy).

94. Zach Walton, *Senate Judiciary Committee to Debate ECPA Reform This Week*, WEBPRONEWS (Apr. 15, 2013), http://www.webpronews.com/senate-judiciary-committee-to-debate-ecpa-reform-this-week-2013-04 [http://perma.cc/WE6F-GG38].

95. *Electronic Communications Privacy Act Amendments Act of 2013*, S. 607, 113th Cong. (2013); H.R. 1852, 113th Cong. (2013). In addition to Congress, many major cloud storage providers have begun claiming that they will withhold user data from law enforcement unless presented with a valid warrant. *See* Brendan Sasso, *Facebook, E-mail Providers Say They Require Warrants for Private Data Seizures*, THE HILL (Jan. 25, 2013, 10:40 PM), http://thehill.com/policy/technology/279441-facebook-email-providers-require-warrant-for-private-data [http://perma.cc/78UB-8PNM].

96. *Bill & Summary Status 113th Congress (2013-2014) S. 607 All Congressional Actions*, LIBRARY OF CONGRESS, http://thomas.loc.gov/cgi-bin/bdquery/z?d113:SN00607:@@@X [http://perma.cc/RC58-R8LQ] (last visited Apr. 11, 2015).

97. Kerr, *supra* note 59, at 519.

98. *Id.* (citing Katz v. United States, 389 U.S. 347, 352 (1967)).

99. Kyllo v. United States, 533 U.S. 27, 40 (2001).

100. *Id.* at 33.

Fourth Amendment limitations.[101] To roll back protection from this advancing form of technology in light of the societal expectation of privacy in the home risked "erod[ing] the privacy guaranteed by the Fourth Amendment."[102]

The factors driving *Katz*, *Kyllo*, and the Court's most recent decision, *Riley v. California*, extend to data housed in cloud storage accounts.[103] The Internet and data stored within its vast framework play an integral role in modern society, much as the telephone did and continues to do. The number of cloud storage users continues to grow faster and faster.[104] Using the logic articulated in *Katz*, it is arguable that cloud storage data is already private and is merely awaiting formal judicial recognition of its role in society. Moreover, shirking from providing a full-fledged privacy interest as technology progresses runs afoul of the spirit of *Kyllo* and *Riley*, in which the Court meshed the expectation of privacy with technological leaps.

B. The Third-Party Doctrine and Cloud Storage

This combination of social norms and positivist thinking supports the notion that people retain a reasonable expectation of privacy in their cloud storage accounts. Nonetheless, this does not mean that alternative principles might not eliminate that expectation before a user could assert it. This potential lies in the third-party doctrine, which holds that one eliminates his own reasonable expectation of privacy when he voluntarily shares information with a third party.[105] Even a reasonable belief that the third party would not share the information fails to preserve an expectation of privacy.[106]

The Court employed this rationale in several cases that form the basis of the doctrine. In *United States v. Miller*, an individual could

---

101. *Id.* at 40; *see also* Kerr, *supra* note 59, at 520.

102. *Kyllo*, 533 U.S. at 34.

103. Riley v. California, 134 S. Ct. 2473 (2014); *Kyllo*, 533 U.S. 27; Katz v. United States, 389 U.S. 347 (1967).

104. *See* Frenkel, *supra* note 17; Frederic Lardinois, *Report: Cloud Storage Services Now Have Over 375M Users, Could Reach 500M by Year-End*, TECH CRUNCH (Oct. 15, 2012) http://techcrunch.com/2012/10/15/report-cloud-storage-services-now-have-over-375m-users-could-reach-500m-by-year-end [http://perma.cc/7YRE-73VU].

105. Smith v. Maryland, 422 U.S. 735, 743-44 (1979); Katz v. United States, 389 U.S. 347, 363 (1967) (White, J., concurring).

106. United States v. Miller, 425 U.S. 435, 443 (1976).

not claim that he had a reasonable expectation of privacy in records kept by his bank regarding his account.[107] Similarly, in *Smith v. Maryland*, a person could not claim privacy in the phone numbers he had voluntarily dialed that the phone company used to complete the call.[108] In both cases the defendant had willingly shared with the third party the substance of their information. The question becomes whether storing information on cloud servers is tantamount to the "sharing" of information the Court dealt with in *Smith* and *Miller*, and consequently enough to surrender a reasonable expectation of privacy.[109]

There are essentially three different types of service agreements that users can have with storage providers.[110] The first are agreements in which the provider retains the expressed right to access and, in some cases, use the information provided.[111] Second are those in which providers engage in generic monitoring of content, but do not intend to use information for alternate purposes.[112] Third are agreements in which providers expressly limit their own ability to access storage contents.[113] Each type of agreement requires measuring the level of data shared with the provider.

---

107. *Id.* at 442.

108. *Smith*, 422 U.S. at 742.

109. This is, of course, if the third-party doctrine itself is truly valid in the context of the Internet. In her concurrence to *United States v. Jones*, Justice Sotomayor expressed her belief that the third-party approach flowing from *Smith* is "ill suited to the digital age," and that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring). This is in large part because "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Id.*; *see also* Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 MISS. L.J. 1, 76-80 (2005) (arguing that the third-party doctrine does not apply to digital intermediaries, rather digital intermediaries act as servants and aides within a reasonable expectation of privacy than a true third party).

110. For a more thorough discussion of issues surrounding service agreements, see Constantine, *supra* note 16, at 525-27.

111. *See, e.g.*, *Google Terms of Service*, GOOGLE, http://www.google.com/policies/terms/ [http://perma.cc/H3Z7-PTHM] (last updated Apr. 14, 2014).

112. *See, e.g.*, *Microsoft Services Agreement*, WINDOWS, http://windows.microsoft.com/en-us/windows/microsoft-services-agreement [http://perma.cc/LQR5-USSD] (last updated June 11, 2014) ("Content that violates this agreement, which includes the Microsoft Anti-Spam Policy ... and the Microsoft Code of Conduct ... or your local law isn't permitted on the services. Microsoft reserves the right to review content for the purpose of enforcing this agreement.").

113. *See, e.g.*, *Mozy Privacy Policy*, MOZY (May 14, 2009), http://www.mozy.com/privacy [http://perma.cc/7S63-RYJR].

The last type of agreement is where users most easily retain an expectation of privacy. The provider's professed lack of access creates a situation different from the third-party service at issue in *Miller* and *Smith*. By storing data in a cloud account and protecting it with a password, the account should become a separate container with its own expectation of privacy.[114] In a way, the account becomes a technological successor to the safe deposit box.[115] Even though the provider of such storage *could* enter and view the contents, the understanding is that the provider will not access the account, and therfore, law enforcement authorities do not have the right to enter such private spaces.[116]

Providers with a terms of service conferring broader access rights present a more complicated issue.[117] Each terms of service allows providers to have some measure of access to files that users upload, though some restrict their involvement to merely screening for objectionable content,[118] whereas others reserve the right to use the content for other purposes.[119] Seemingly, the portion of these terms of service agreements that permit considering cloud storage an RCS would paradoxically defeat an expectation of privacy.[120] After all, by signing up for services with broad access rights, people are voluntarily permitting access to their data, even if in a limited way. Nevertheless, despite the necessary disclosure of information to providers, changes in technology justify evolving considerations of the Fourth Amendment.[121] Correspondingly, such changes call for a new

114. *See* Couillard, *supra* note 16, at 2237-38.

115. Wilson, *supra* note 18, at 276; *see also* United States v. First Nat'l City Bank, 568 F.2d 853, 860-61 (2d Cir. 1977) (demonstrating that there can be a reasonable expectation of privacy in safe deposit boxes).

116. *See* Couillard, *supra* note 16, at 2237-38; Wilson, *supra* note 18, at 276.

117. Constantine, *supra* note 16, at 514-15.

118. *See, e.g.*, *Microsoft Services Agreement*, *supra* note 112 (listing the terms of service applying to SkyDrive cloud storage).

119. *See, e.g.*, *Google Terms of Service*, *supra* note 111 (listing the terms of service applying to all Google services, including Google Drive).

120. *See* 18 U.S.C. § 2702(a)(2)(B) (2012) (addressing voluntary disclosures of consumer information).

121. *See* Katz v. United States, 398 U.S. 347, 352 (1967) (conferring privacy rights in telephone conversations by evaluating changing technology).

understanding of the third-party doctrine to properly address the realities of digital storage.[122]

To assess the expectation of privacy in cloud storage, it is important to consider the ways in which transferring information to a cloud provider differs from the classic third party cases. Professor Patricia Bellia suggests limited application of the third-party doctrine and offers a useful approach.[123] She posits that highlighting those differences requires asking: (1) What "type of *information* is at issue"? (2) What is the purpose in transferring the information to the third party? (3) How relevant is the information's *substance* to the third party's activities? and (4) How limited is "the third party's *ability to access and use the information*"?[124]

One can answer the first two questions simply. In *Miller* and *Smith,* the Court considered financial information and phone numbers transferred to third parties to complete a multistep task on the transferors' behalf.[125] The information within the files uploaded to the cloud can potentially contain limitless varieties of data, including bank records and phone numbers. The difference, however, is in the transfer's purpose.

Those who store data in cloud accounts seek safe receptacles for their information, as opposed to commissioning the cloud provider to provide a service beyond preservation.[126] Rather than seeking a multistep partnership, the cloud account users engage with providers so that they may act as mere custodians of the data, thus ensuring that such data is neither lost nor damaged. There is only one step: storing the data. One is not "revealing his affairs to another" as the *Miller* defendant did,[127] because the user is not engaging the provider for some other task beyond receipt and preservation. Virtually all cloud storage providers, even those with an expansive

122. *See* Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1403-05 (2004) (describing why the third-party doctrine should be construed narrowly in the computer/Internet context).

123. *Id.*

124. *Id.*

125. Smith v. Maryland, 422 U.S. 735, 743-44 (1979); United States v. Miller, 425 U.S. 435, 442 (1976).

126. David S. Barnhill, *Cloud Computing and Stored Communications: Another Look at* Quon v. Arch Wireless, 25 BERKELEY TECH. L.J. 621, 645 (2010).

127. Bellia, *supra* note 122, at 1404 (citing *Miller*, 425 U.S. at 443).

terms of service, preserve that distinction at least in terms of the purpose behind the transmission,[128] which is storing user data.

Regarding the third question, whether the substance of the data a user provides is relevant to third party activity, hinges on how one defines activity. Limiting the understanding of "activity" to the service the provider performs on behalf of the user means that activity is limited to the storage itself; the content of files and the substance of the data is not relevant to that activity.[129] Even providers that monitor uploaded file data to remove objectionable content[130] cannot claim that the substance of the file is relevant to their activity of storage. A broad understanding of activity that encompasses all of the actions cloud providers *might* take with user data is inadequate. The narrow approach corresponds with the purpose of why users engage cloud providers in the first place: to store data, not to crowdsource content for a company.[131]

It is the last of Professor Bellia's questions that may permit different conclusions stemming from different terms of service. The limits on third-party access to information do vary substantially based on the agreement between the parties.[132] Providers that primarily access uploaded data for the purpose of monitoring for objectionable content are not *using* the substance of the content to perform their activity, which is storage. Instead, they are considering it through a retroactive screening function, and the substance of uploaded data has no bearing on the act of storing itself.

Providers, such as Google, are another matter. Google retains broad rights to access and use customer-uploaded content.[133] Even with Google and other comparable companies that might retain

128. *See, e.g.*, *Microsoft Services Ageement*, *supra* note 112.

129. File size would be relevant to this activity, as every cloud provider considers storage size capacities in price and service computation. Jill Duffy, *The Best Cloud Storage Services for 2015*, PCMAG (Mar. 26, 2015), http://www.pcmag.com/article2/0,2817,2413556,00.asp [http:// perma.cc/95RU-2RZ6].

130. *See Microsoft Services Agreement*, *supra* note 112 (outlining the terms of service applying to SkyDrive cloud storage).

131. *See* Bellia, *supra* note 122, at 1404-05.

132. *See supra* notes 110-12 and accompanying text.

133. *Google Terms of Service*, *supra* note 111 (defining terms of service that give Google access to "content" submitted by users, implying more than just file management, but also what the files contain). Additionally, Google not only stores data, but also retains the right to use data for "operating, promoting, and improving ... services, and to develop new ones." *Id.*

extensive rights, most of the salient questions point to keeping an expectation of privacy. However, given the wholesale revelation and access rights, a court could possibly conclude that one surrenders his expectation of privacy when he gives information over to the most prying of providers. By the nature of these agreements, the user does not substantively limit the scope of the provider's access.

III. CLOUD STORAGE AND LOCAL SOFTWARE

As demonstrated in Part II, there is ample justification to believe that users maintain a reasonable expectation of privacy in their cloud storage accounts. Considering the differing terms of service, societal expectations of privacy, muddled statutory law, and the fact that privacy policies for Internet services often change, law enforcement cannot simply assume that it can access cloud data without a warrant.[134] Law enforcement agents would need some exception to the warrant requirement to view these contents without judicial approval. Therefore, when the police obtain a warrant to search an individual suspect's computer and find cloud-connected local software, as they did with the hypothetical character Winston, they must find a justification to sidestep the warrant requirement.[135] The two most likely reasons they might offer would be the plain view and exigent circumstances exceptions.

A. Plain View

For evidence to come under the plain view exception, it must meet three requirements: (1) the incriminating nature of the evidence must be readily apparent, (2) officers must have a lawful vantage point to view it, and (3) officers must be in a location to lawfully seize the evidence.[136] Regarding the first element, cloud computing retains the same plain view concerns as local computing: there is essentially no way to know what is inside of a file without

134. Without examining privacy policies and practices of the storage providers, the police cannot know if the suspect has surrendered a reasonable expectation of privacy, and, as the cloud files are *not* on the machine they are searching, such content is outside the scope of the warrant.

135. *See* Katz v. United States, 389 U.S. 347, 357 (1967).

136. Horton v. California, 496 U.S. 128, 136-37 (1990).

examining it.[137] Despite that similarity, the nature of the cloud does change the analysis with regard to the second and third parts of the exception. Relevant doctrine supports the notion that law enforcement does not have a lawful vantage point from which to view cloud data or to seize it while using local software.

Practically speaking, when police obtain a warrant to search a computer, they can access all of the files stored on that machine. Such a search is not restricted to only pure data files; it also includes programs and applications installed on the machine. Seemingly, that search would also include files one can see in those installed applications.

That assumption, however, is premature, as the Fourth Amendment protects a person's *individual* effects from government intrusion as well.[138] One such "effect" is a container, which is an object capable of containing another object.[139] The Court affords containers full Fourth Amendment protection and does not evaluate their worthiness.[140] Although it is digital and does not contain physical objects per se, many courts and commentators believe that a computer hard drive is functionally equivalent to a container.[141] There is no meaningful distinction between storing files on a remote drive or a local one beyond the difference in location. Like a computer itself, the information stored on Internet accounts is analogous to items in locked containers.[142]

The seeming consensus is that the existence of password protection for virtual accounts, drives, and files preserves the expectation of privacy.[143] There is a chance that a person might leave his cloud

137. *See supra* Part I.B.

138. *See* U.S. CONST. amend. IV.

139. New York v. Belton, 453 U.S. 455, 460 n.4 (1981).

140. United States v. Ross, 456 U.S. 798, 822 (1982).

141. *See, e.g.*, Davis v. Gracey, 111 F.3d 1472, 1480 (10th Cir. 1997); United States v. Al-Marri, 230 F. Supp. 2d 535, 541 (S.D.N.Y. 2002); People v. Gall, 30 P.3d 145, 153-54 (Colo. 2001) (analogizing computers as containers similar to filing cabinets); Kerr, *supra* note 13, at 549.

142. Strandburg, *supra* note 62, at 660.

143. *Id.*; *see* Kerr, *supra* note 16, at 1021; *see also* United States v. Stabile, 633 F.3d. 219, 233 (3d Cir. 2011) (considering whether password protection is used to determine whether a reasonable expectation of privacy exists for a computer hard drive); United States v. Buckner, 473 F.3d 551, 554 n.2 (4th Cir. 2007) (recognizing a reasonable expectation of privacy in password-protected computer files); Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001) (same).

program logged in or with the password saved. This too would not destroy his reasonable expectation of privacy. Even though it might not be locked digitally from that specific location, accessing the cloud account from another computer would require a password. Moreover, a separate expectation of privacy exists in the computer that can access the account. As such, the true hinging point is not always the existence of the password, but whether the user has left his data open for the whole world to see.

The account is still a closed container, and as the police still need to take steps to access the contents, one cannot fairly say that cloud accounts are merely transparent vessels for the police to peer into.[144] Even though the police might technically be able to "see" the contents of user accounts through the cloud-connected software because of the seized computer, law enforcement must obtain warrants for containers "closed against inspection, wherever they may be."[145] The access gained by searching a suspect's local computer is accordingly not a lawful vantage point to view cloud files.

Additionally, searching a suspect's computer does not put law enforcement in a position to lawfully seize the data. Cloud storage has the dual characteristics of being an effect as a virtual closed container, as well as a separate location, both physical and virtual.[146] Recall that commercial cloud storage is remote by nature, and commercial providers use networked clusters of servers to host data.[147] Such generality violates the Fourth Amendment's demand of specificity in places to be searched.[148] Not only do cloud servers occupy a different physical space, but they also represent a different

144. *See* Robbins v. California, 453 U.S. 420, 427 (1981) (plurality opinion) (noting that a transparent container would not preserve a reasonable expectation of privacy against law enforcement because such "container[s] proclaim[ ] [their] contents"), *overruled on other grounds by* United States v. Ross, 456 U.S. 798, 802 (1982).

145. Courtney M. Bowman, Note, *A Way Forward After* Warshak*: Fourth Amendment Protections for E-Mail*, 27 BERKELEY TECH. L.J. 809, 811 (2012) (citing *Ex parte* Jackson, 96 U.S. 727, 733 (1877)).

146. *See supra* notes 4-12 and accompanying text.

147. *See* Strickland, *supra* note 9.

148. *See* U.S. CONST. amend. IV.

virtual place.[149] Essentially, the police would be going into an entirely new location, one that the warrant gives them no right to go.[150]

B. Exigent Circumstances

The plain view doctrine is not the only way to sidestep the warrant requirement. Another long-accepted justification to forgo a warrant in criminal investigations is when police face exigent circumstances.[151] These are instances when law enforcement's failure to obtain a warrant is reasonable given the surrounding events.[152] The need to prevent the destruction of evidence is one such recognized circumstance.[153]

The plain view doctrine, if properly followed and adapted to advancing technology, would not empower law enforcement to gather cloud data files through locally installed programs. It would be difficult for a suspect to remotely delete data on a seized computer in police custody.[154] Still, cloud data is stored on remote servers, and is accessible on virtually any Internet-capable device.[155] It is easy to

---

149. This situation is not unlike when police have a warrant to search a single building on a piece of property with multiple structures. If the police want to search a house, they can search a house. Yet, that same warrant does not necessarily empower them to search the curtilage or structures on a person's property, such as a guesthouse. State v. Hamilton, 290 P.3d 271, 275 (N.M. Ct. App. 2012). Ownership of the structure (in this case ownership of the account) is not enough. United States v. Schroeder, 129 F.3d 439, 442 (8th Cir. 1997). Just because these places are easily accessible from the lawful vantage point does not make extending a search equally lawful.

150. It is also quite likely that some of these remote servers might be in a wholly different jurisdiction than the one that issued the search warrant in the first place. This would pose problems, as the warrant requirement to search the original computer in one state may be different than what is necessary for a search in the actual jurisdiction where the cloud drives are located, at least in terms of state law. *See* Susan W. Brenner, *Law, Dissonance, and Remote Computer Searches*, 14 N.C. J.L. & TECH. 43, 55-60 (2012) (examining the problem of jurisdiction-straddling computer searches as they apply to searching individual drives). Although justified at their actual location, the police could indeed be breaking the law at the source of the information for which they are searching.

151. An exigent circumstance is one that makes law enforcement's failure to obtain a warrant reasonable. Warden v. Hayden, 387 U.S. 294, 299 (1967).

152. *See* Mincey v. Arizona, 437 U.S. 385, 393-94 (1978).

153. Brigham City v. Stuart, 547 U.S. 398, 403 (2006); Ker v. California, 374 U.S. 23, 40-41 (1963).

154. All police officers would need to do in most situations is block Internet access and any remote users would be cut off.

155. *See* Rouse, *supra* note 4.

think that police would fear that data they see on cloud servers might be destroyed before they can get a warrant to search it. After all, the suspect could simply go to another computer and delete the contents.

That fear is not groundless. Access is remote, and as long as a cloud account holder has Internet access, they have access to the account and the ability to manage their files. However, the realities of cloud and computer storage remove any exigency. The risk of losing the data is small, thus not nearly enough of a concern to bypass the Fourth Amendment. Even after a user deletes his data or closes his account, many cloud storage providers will preserve data on their servers for a period of time.[156] There are also storage providers that do not expressly acknowledge that data will remain on their servers after a user-initiated deletion.[157]

Regardless, despite any user attempts to remove data from their account, exigent circumstances are unlikely to exist. Simply deleting data from a drive does not completely destroy the files hosted there, and "deleted" data is actually recoverable.[158] Totally eliminating data requires taking extra steps beyond merely selecting a delete option. That would require physical access to the hosting drive, such as smashing it to bits, or expanded logical access likely beyond the capabilities of an end-user.[159]

---

156. *See, e.g.*, *Dropbox Privacy Policy*, DROPBOX (Feb. 20, 2014), https://www.dropbox.com/privacy#privacy [http://perma.cc/DT74-78N8]; *iCloud Terms and Conditions*, APPLE, http://www.apple.com/legal/Internet-services/icloud/en/terms.html [http://perma.cc/U435-4DTK] (last updated Oct. 20, 2014); *Google Terms of Service*, *supra* note 111; *Microsoft Services Agreement*, *supra* note 112 (outlining the terms of service applying to SkyDrive cloud storage).

157. *See, e.g.*, *Mozy Privacy Policy*, *supra* note 113.

158. *See How to Permanently Erase Data off a Hard Drive*, WIKIHOW, http://www.wikihow.com/Permanently-Erase-Data-Off-a-Hard-Drive [http://perma.cc/H3EQ-EX6J] (last visited Apr. 11, 2015) (describing "deleted" data as merely marked for overwrite, unless one takes further action to fully erase the file).

159. *See* Josiah Dykstra & Damien Riehl, *Forensic Collection of Electronic Evidence from Infrastructure-as-a-Service Cloud Computing*, 19 RICH. J.L. & TECH 1, 12 (2012); Mossberg, *supra* note 7.

IV. A POSSIBLE SOLUTION

The law leans against the police if officers want to use local software to gain access to cloud data absent a warrant, but desire to access such information is understandable. As cloud storage grows increasingly ubiquitous, it will progressively host more documents and data of interest to law enforcement. Conceivably, there will be those who make exclusive use of remote drives to store their data.[160] Perhaps the simplest answer is to obtain a warrant for the account the officers wish to examine.

Nonetheless, this approach presents problems of its own. Many different companies offer cloud storage services.[161] Though warrants call for specificity in what will be searched, trying to guess what cloud service a suspect employs prior to searching his computer is impractical given the many options.[162] Numerous cloud providers exist, and it is difficult to tell beforehand if and what provider a suspect uses. In reconciling the particularity requirement with the Internet, courts should address cloud accounts in a manner similar to what Professor Kerr suggests. He argues that courts should issue a warrant to search all of a person's online accounts rather than just one at time.[163] This approach would ensure that police could search any online accounts linked to a suspect's computer, but it is more expansive than it needs to be.

Professor Kerr developed his approach only for searching Internet communications,[164] rather than searching for files stored on the web. Although e-mail services can act as a vessel for pure communication *and* store files through message attachments, accounts and services

160. *See* Tom Cheredar, *Bitcasa Grabs $11M for Its "Infinite" Cloud Storage*, VENTUREBEAT (Nov. 11, 2013, 10:45 AM), http://verturebeat.com/2013/11/11/bitcasa-grabs-11m-for-its-infinite-cloud-storage/ [http://perma.cc/XA6M-SR6N] (describing how users can have unlimited space to store their files).

161. *See* Paul Lilly, *Top 20 Cloud Storage Services: The Great Hard Drive in the Sky*, TECHADVISOR (Jan. 22, 2013), http://www.pcadvisor.co.uk/features/storage/3421715/top-20-cloud-storage-services [http://perma.cc/NYP5-T6CE].

162. *Id.*

163. Kerr, *supra* note 16, at 1045-47.

164. *Id.* at 1045.

exist that are limited to one or the other.[165] Accordingly, for searching cloud storage accounts, courts should take a narrower version of Kerr's approach and issue a warrant only for services that can store data files beyond text-based communication.

Such an approach would better serve the Fourth Amendment's particularity requirement than an authorization encompassing all of a suspect's online accounts. It is highly unlikely that police searching for images of child pornography will find such files in the text log of an online chat program. However, permitting police to search all accounts attached to an individual enables to them to go combing through digital locations where evidence of the pertinent crime cannot, or is highly unlikely to, exist. Limiting a warrant to storage accounts versus a general warrant[166] for all Internet services would preserve a degree of a suspect's privacy, while at the same time enabling police to do their job. Should law enforcement inadvertently access account information outside the scope of the warrant, a court can exclude evidence of criminal activity found therein.

CONCLUSION

The Internet and its boundless capabilities have reshaped society. The Ninth Circuit aptly calls it the "new frontier" of the Fourth Amendment, in which the limits of privacy protection are an "open question."[167] Questions involving cloud computing do require answering and analysis. One thing is clear though: in at least a number of circumstances, people can retain a reasonable expectation of privacy in their cloud storage. That expectation is separate and apart from that which they enjoy in their physical computer. A warrant authorizing the search of one computer does not destroy

165. *See, e.g.*, Jon Brodkin, *Rather Than Recreate Google Drive, Yahoo Integrates Dropbox into Mail*, ARSTECHNICA (Apr. 2, 2013, 7:15 PM), http://arstechnica.com/information-technology/2013/04/rather-than-recreate-google-drive-yahoo-integrates-dropbox-into-mail/ [http://perma.cc/BJY2-YSKE] (explaining that although users can use Dropbox within Yahoo's mail service, the two are separate services because Yahoo elected to partner with Dropbox rather than develop its own competition to Google).

166. Recall that the Fourth Amendment's tradition strongly disfavors general warrants. *See* MCINNIS, *supra* note 40, at 15-20.

167. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904 (9th Cir. 2008) *rev'd sub nom. on other grounds*, City of Ontario v. Quon, 130 S. Ct. 2619 (2010).

expectations of privacy in other computers that communicate with it. The same applies to cloud accounts that a computer links to, as they are detached and distinct. The convenience of peering through locally installed software does nothing to change that. If a police officer wants to search the data in one of those accounts, as they wanted to do with the theoretical Winston, they should get a warrant.

Aaron J. Gold[*]

* J.D. Candidate 2015, William & Mary Law School; B.A. 2011, American University. I would like to thank Professors Jennifer Stevenson and Adam Gershowitz for their helpful comments and insight. Additionally, many thanks to the editors and staff of the *William & Mary Law Review*, in particular Kayla McCann Marty, for their assistance in preparing this Note for publication.