Stanford Law Review

Volume 69 March 2017

NOTE

Lost in the Cloud: Cloud Storage, Privacy, and Suggestions for Protecting Users' Data

Eric Johnson*

Abstract. In the digital age, users store vast amounts of data—often data considered to be private—in the cloud. The privacy of this data is increasingly determined by the policies of the companies storing it. But how does the law currently protect that data from law enforcement? Do users maintain a reasonable expectation of privacy in the information they have uploaded to the cloud? And if so, can service providers' terms of service affect users' reasonable expectations of privacy? This Note answers those questions by examining the main legal protections relevant to data stored in the cloud: the Stored Communications Act and the Fourth Amendment. After analyzing these protections, this Note determines that data stored in the cloud may be protected by the Act. But more importantly, this Note analyzes the history of the third-party doctrine and determines that users do have a reasonable expectation of privacy in information stored in the cloud *until* the third-party doctrine is triggered. And this triggering can occur due to provider access pursuant to the terms of service.

In light of these findings, this Note concludes by suggesting that providers implement standard, scope, and notice provisions in their privacy policies or terms of service in order to enhance the protection of user privacy while also providing reasonable means for providers to secure and maintain their networks.

* J.D., Stanford Law School, 2016. Many thanks to Albert Gidari, Director of Privacy at the Stanford Center for Internet and Society, for his invaluable guidance and insight. Thanks also to Mark Lemley, William H. Neukom Professor of Law at Stanford Law School; Daphne Keller, Director of Intermediary Liability at the Stanford Center for Internet and Society; and the members of the *Stanford Law Review* for their thoughtful and challenging feedback.

Table of Contents

Introduction

Imagine law enforcement believes that a suspect is storing pirated movies in a Dropbox cloud storage account. The investigation is still in its early stages, but officers are worried that if they wait to establish the probable cause necessary for a warrant, the suspect will continue to collect and distribute the movies. So the authorities send a subpoena to Dropbox demanding all information from the suspect's account, including subscriber information, metadata, and, most importantly, the digital contents. When the suspect signed up for a Dropbox account, he agreed to the "Dropbox Terms of Service," which allow Dropbox to "review [his] conduct and content for compliance with [its] Terms and [its] Acceptable Use Policy,"[1] as well as turn over content information to third parties to "comply with the law" and "prevent fraud or abuse of Dropbox or [its] users."[2]

Is the government's subpoena sufficient to compel Dropbox to turn over the user's content information? Should Dropbox demand a warrant? Or has the user already given up his Fourth Amendment privacy rights by entrusting his information to a third party? Should Dropbox access the suspect's account to investigate the authorities' claims and determine whether the suspect has violated Dropbox's "Acceptable Use Policy," which expressly forbids "violat[ing] the law in any way"?[3] And if Dropbox decides to investigate, does accessing the user's stored information affect any reasonable expectation of privacy the user may have held in that information? Would Dropbox's actions make the subpoena sufficient?

If pirated movies seem of little concern, consider other instances of known law enforcement surveillance. In 1963, the Federal Bureau of Investigation wiretapped the phones of Martin Luther King, Jr. under the pretense of determining King's ties to members of the American Communist Party.[4] And after 9/11, the New York Police Department, with significant assistance from

1. *Dropbox Terms of Service*, DROPBOX (Dec. 8, 2016), https://www.dropbox.com/terms2017.

2. *Dropbox Privacy Policy*, DROPBOX (Dec. 8, 2016), https://www.dropbox.com/privacy2017.

3. *Dropbox Acceptable Use Policy*, DROPBOX, https://www.dropbox.com/terms#acceptable_use (last visited Mar. 3, 2017).

4. David J. Garrow, *The FBI and Martin Luther King*, ATLANTIC (July/Aug. 2002), http://www.theatlantic.com/magazine/archive/2002/07/the-fbi-and-martin-luther-king/302537.

the Central Intelligence Agency, spent years monitoring Muslim neighborhoods and community centers.[5] Targets come in all forms.

The evolution of the Internet has presented people with new options for storing information, but the privacy provided by those options is questionable. Cloud storage, one such option, is a method of data storage wherein clients send data through the Internet for storage on one or (typically) multiple data servers, which are owned and operated by a company offering data storage services (a "cloud storage provider").[6] Often, providers store information in a manner that allows them to access user information to conduct maintenance and ensure compliance with their terms of service.[7] Usually such access occurs through automated scans—scans that are fully computerized and do not involve a human personally accessing the data.[8]

As more information moves into the cloud and big data[9] quantifies our lives, questions about data privacy become increasingly common and important. Privacy in the modern world rests heavily on the decisions made by cloud storage providers, which find themselves in possession of a wealth of stored information—from personal e-mails and calendars to business files and correspondence. Much of this information likely would be considered "private" in common parlance, but the law may not recognize the privacy of that information. For while the Fourth Amendment protects against *unreasonable* searches and seizures, the Supreme Court, under the third-party doctrine, has

5. Matt Apuzzo & Adam Goldman, *With CIA Help, NYPD Moves Covertly in Muslim Areas*, SEATTLE TIMES (Aug. 25, 2011, 12:00 AM), http://www.seattletimes.com/seattle-news/politics/with-cia-help-nypd-moves-covertly-in-muslim-areas.

6. Jonathan Strickland, *How Cloud Storage Works*, HOWSTUFFWORKS, http://computer.howstuffworks.com/cloud-computing/cloud-storage.htm/printable (last visited Mar. 3, 2017).

7. *See, e.g.*, *Google Privacy Policy*, GOOGLE, https://www.google.com/policies/privacy (last updated Aug. 29, 2016) ("We use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and our users."); *see also* Samuel Gibbs, *Gmail Does Scan All Emails, New Google Terms Clarify*, GUARDIAN (Apr. 15, 2014, 8:24 AM EDT), https://www.theguardian.com/technology/2014/apr/15/gmail-scans-all-emails-new-google-terms-clarify (reporting that Google, a cloud storage provider, updated its terms of service to detail that it performs automated scanning of e-mails for purposes such as "customised search results, tailored advertising, and spam and malware detection").

8. *See* Jon M. Chang, *Google to Make Case that Gmail Practices Do Not Violate Privacy Laws*, ABC NEWS (Sept. 5, 2013), http://abcnews.go.com/Technology/google-gmail-make-case-practices-violate-privacy-laws/story?id=20168964; Gibbs, *supra* note 7 (discussing Google's automated scanning practices).

9. *See* Gil Press, *12 Big Data Definitions: What's Yours?*, FORBES (Sept. 3, 2014, 8:01 AM), http://www.forbes.com/sites/gilpress/2014/09/03/12-big-data-definitions-whats-yours/#5382d6fa21a9 (describing a variety of definitions of the term "big data").

traditionally considered warrantless searches and seizures of information entrusted to third parties to be reasonable.[10]

This Note argues that cloud storage users have a reasonable expectation of privacy in the information stored in their cloud storage accounts. This expectation persists in spite of automated scans that cloud storage providers may perform for the general maintenance of their networks.

But any further access to cloud storage a user grants a provider pursuant to the provider's terms of service can affect the user's reasonable expectation of privacy in two ways. First, the terms of service can grant the provider such sweeping access to, and use of, user information that the user's expectation of privacy is simply unreasonable. Second, and far more commonly, the user can, by agreeing to the provider's terms of service, contract to grant the provider access to and use of her information in its normal course of business under particular circumstances. For example, users may agree to human searches of their accounts to investigate potential violations of the terms of service.[11] But simple agreement to such a contract does not eliminate entirely the user's reasonable expectation of privacy. Rather, the user retains full Fourth Amendment privacy rights in her information until the contractually agreed-upon circumstances occur. At that point, the provider's access and use triggers the third-party doctrine and eliminates the user's reasonable expectation of privacy.

Because terms of service can drastically affect a user's privacy, cloud storage providers should protect user privacy by including provisions in their terms of service that formalize the standard for, and scope of, provider access and should promise notice to users when access that affects user privacy occurs. Of course, this risks exposing providers to greater liability because it means making additional promises to users that could be violated, intentionally or unintentionally. Providers should balance this risk with the competitive advantage they may gain in the marketplace given concerns about government access to data in the post-Snowden era.[12] Furthermore, users should keep privacy in mind when deciding which cloud storage service to use and should opt for a service that transparently limits the service provider's access to and

10. *See infra* Part II.B.1.

11. *See, e.g.*, *Is Dropbox Safe to Use?*, DROPBOX, https://www.dropbox.com/en/help/27 (last visited Mar. 3, 2017) ("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).").

12. *See generally* Ewen MacAskill & Gabriel Dance, *NSA Files: Decoded; What the Revelations Mean for You*, GUARDIAN (Nov. 1, 2013), http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded (outlining numerous concerns about and viewpoints on government collection of private data after the disclosures made by Edward Snowden).

use of user information. Together, providers and users can make a strong push for ensuring the privacy of data stored in the cloud.

This Note makes this argument in five Parts. Part I discusses how users interact with cloud storage services and how cloud storage providers can access users' data. Part II delves into the Stored Communications Act (SCA) and the Fourth Amendment to determine if they afford privacy protections to data stored in the cloud. It also discusses the development of the third-party doctrine and its unclear application to the Internet. Part III determines that users do have Fourth Amendment protection for information held in cloud storage and examines if, and when, the third-party doctrine should be applied to cloud storage. Part IV examines a select group of cloud storage providers' terms of service to find when providers can access users' data and how that access affects users' privacy. Finally, Part V shows the problem with the current state of access allowed by terms of service agreements and suggests reasonable solutions to help providers protect users' privacy.

I. What Is Cloud Storage?

Cloud storage services, which became available to mainstream consumers in the 2000s,[13] "allow[] users to store data and applications on remote servers owned by others."[14] These remote servers are essentially "global storage facilities [used] to store information electronically and grant access to uploaded information using any electronic device from any location at any time."[15] Users generally must consent to nonnegotiable terms of service when they sign up for an account with a cloud storage provider.[16] The terms of service govern the relationship between the service and user and usually contain terms regarding the provider's access to and use of information and the manner in which a user can and cannot use the service.[17]

13. *See 30 Years of Accumulation: A Timeline of Cloud Computing*, GCN (May 30, 2013), https://gcn.com/Articles/2013/05/30/GCN30-Timeline-Cloud.aspx?Page=1; *see also* Arif Mohamed, *A History of Cloud Computing*, COMPUTERWEEKLY (Mar. 2009), http://www.computerweekly.com/feature/A-history-of-cloud-computing.

14. Timothy Peterson, *Cloudy with a Chance of Waiver: How Cloud Computing Complicates the Attorney-Client Privilege*, 46 J. MARSHALL L. REV. 383, 384 (2012).

15. Laurie Buchan Serafino, *"I Know My Rights, So You Go'n Need a Warrant for That": The Fourth Amendment,* Riley*'s Impact, and Warrantless Searches of Third-Party Clouds*, 19 BERKELEY J. CRIM. L. 154, 161 (2014).

16. *Id.* at 162.

17. Kristina Irion, *Your Digital Home Is No Longer Your Castle: How Cloud Computing Transforms the (Legal) Relationship Between Individuals and Their Personal Records*, 23 INT'L J.L. & INFO. TECH. 348, 358 (2015).

Different types of storage providers offer a range of different services. This Note addresses cloud storage services like Dropbox,[18] Carbonite,[19] and Google Drive,[20] which allow users to create an account and upload files to the cloud for perpetual storage (so long as the account remains open). Many services also offer collaboration tools that allow users to, for example, share files or extend invitations to edit files within the service.[21]

Importantly, while nearly all cloud storage accounts are password protected,[22] most cloud storage services do not encrypt information uploaded by users in a manner that prevents the provider from accessing the content stored on its servers.[23] Even Apple, which famously encrypts iMessage data from end to end,[24] also backs up those messages by default on its iCloud servers in a manner that makes the content accessible to the company.[25]

Usually, cloud storage providers retain access to user data due to concerns about security, stability, and control of their networks.[26] Cloud storage services employ different types of automated and human scanning. For

18. *See* DROPBOX, https://www.dropbox.com (last visited Mar. 3, 2017).

19. *See* CARBONITE, https://www.carbonite.com (last visited Mar. 3, 2017).

20. *See* GOOGLE DRIVE, https://www.google.com/drive (last visited Mar. 3, 2017).

21. *See* Kia Kokalitcheva & Jordan Novet, *Dropbox Takes on Google Drive with Collaboration Tools for Microsoft Office*, VENTUREBEAT (Apr. 9, 2014, 12:44 PM), http://venturebeat.com/2014/04/09/dropbox-takes-on-google-drive-with-collaboration-tools-for-ms-office; *see also Collaborate with Shared Folders*, DROPBOX, https://www.dropbox.com/guide/business/share/collaborate (last visited Mar. 3, 2017).

22. *See, e.g.*, *Dropbox Login Page*, DROPBOX, https://www.dropbox.com/login (last visited Mar. 3, 2017); *Google Accounts Sign In Page*, GOOGLE, https://accounts.google.com/login#identifier (last visited Mar. 3, 2017); *see also Is Dropbox Safe to Use?*, *supra* note 11 ("You can also take advantage of two-step verification, a login authentication feature which you can enable to add another layer of security to your account.").

23. *See* Peterson, *supra* note 14, at 397 (noting that providers have not been quick to implement large security changes such as encrypting stored data).

24. "End-to-end encryption" means that providers cannot access the content of messages because the messages are encrypted when sent and are only decrypted upon reaching the intended recipient's device. *See Privacy*, APPLE, http://www.apple.com/privacy/approach-to-privacy (last visited Mar. 3, 2017) ("Apple has no way to decrypt iMessage and FaceTime data when it's in transit between devices.").

25. Kavita Iyer, *Apple Can Still Read Your End-to-End Encrypted iMessages*, TECHWORM (Jan. 25, 2016), http://www.techworm.net/2016/01/apple-can-still-read-end-end-encrypted-imessages.html.

26. *See, e.g.*, *Google Privacy Policy*, *supra* note 7 ("We use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and our users."); *see also* Gibbs, *supra* note 7 (reporting that Google, a cloud storage provider, updated its terms of service to detail that it performs automated scanning of e-mails for purposes such as "customised search results, tailored advertising, and spam and malware detection").

example, information may go through automated scanning to detect malware and illegal content or to make sure that the service can properly transmit the data.[27] Further, some services use automated scanning of user content to deliver targeted information, such as advertisements, to users.[28] Finally, services may use human access to investigate and confirm that a user has violated the terms of service.[29]

Significantly, the different types of access to and use of user information pursuant to providers' terms of service have drastic effects on users' privacy, as sometimes provider access can trigger the third-party doctrine, thus compromising users' privacy.[30]

II. What Laws Protect the Privacy of Data in the Cloud?

A two-step inquiry is useful to determine the extent of privacy afforded to users' information stored in the cloud.[31] First, in deference to the doctrine of constitutional avoidance,[32] one must look at the SCA to see if Congress has statutorily afforded users privacy in their data held by cloud storage providers. Second, if the SCA does not protect information stored in the cloud, or if its protections are questionable, the analysis must focus on whether the Fourth Amendment protects information in cloud storage.

---

27. *See, e.g.*, Gibbs, *supra* note 7; *Google Privacy Policy*, *supra* note 7.

28. *See, e.g.*, *Google Terms of Service*, GOOGLE, https://www.google.com/policies/terms (last updated Apr. 14, 2014) ("Our automated systems analyze your content . . . to provide you personally relevant product features, such as . . . tailored advertising . . . .").

29. *See, e.g.*, *Is Dropbox Safe to Use?*, *supra* note 11 ("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).").

30. This Note does not delve into the complicated and technical issue of determining the point at which a scan becomes "use" for purposes of the third-party doctrine. An entire article could (and should) be devoted to that topic. For brevity, this Note assumes that automated scanning for the security, stability, and control of the network does not implicate the Fourth Amendment, while human access to verify a terms of service violation does.

31. There exists an array of state laws relevant to digital communications (for example, California's Electronic Communications Privacy Act). *See, e.g.*, CAL. PENAL CODE § 1546.1 (West 2017) (detailing California's protection of electronic communications). However, this Note will address only federal and constitutional law.

32. *See* Spector Motor Serv., Inc. v. McLaughlin, 323 U.S. 101, 105 (1944) ("If there is one doctrine more deeply rooted than any other in the process of constitutional adjudication, it is that we ought not to pass on questions of constitutionality . . . unless such adjudication is unavoidable.").

A. The Stored Communications Act

Congress enacted the SCA as Title II of the Electronic Communications Privacy Act (ECPA) in 1986.[33] Today, it is a relic forced to adapt to an ever-evolving technological world.[34] Originally enacted in part due to "uncertainty over whether and when Internet users can retain a 'reasonable expectation of privacy' in information sent to network providers,"[35] the SCA "provides privacy protection to communications held by two types of providers": providers of electronic communications service (ECS) and providers of remote computing service (RCS).[36] ECPA defines ECS as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[37] It defines RCS as "the provision to the public of computer storage or processing services by means of an electronic communications system."[38] But whether data actually qualify as ECS or RCS is largely context-specific.[39] For example, Orin Kerr describes a clear-cut distinction:

> [W]hen an e-mail sits unopened on an [Internet Service Provider's] server, the [Internet Service Provider (ISP)] is acting as a provider of ECS with respect to that e-mail. On the other hand, if I author a document and send it via [file transfer protocol] to a commercial long-term storage site for safekeeping, the storage site is acting as a provider of RCS with respect to that file.[40]

The distinction between ECS and RCS is important, for the SCA provides different types of protection for data held by providers of ECS and RCS. A provider of ECS must "disclose contents of communications in its possession that are in temporary 'electronic storage' for 180 days or less" only upon receiving a search warrant;[41] contents older than 180 days fall outside the warrant requirement.[42] However, the 180-day distinction has been called into

33. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, tit. II, 100 Stat. 1848, 1860-68 (codified as amended at 18 U.S.C. §§ 2701-2712 (2015)).

34. *See* Aaron J. Gold, Note, *Obscured by Clouds: The Fourth Amendment and Searching Cloud Storage Accounts Through Locally Installed Software*, 56 WM. & MARY L. REV. 2321, 2333 (2015) ("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.").

35. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1210 (2004).

36. *Id.* at 1213-14; *see also* 18 U.S.C. § 2702(a)(1)-(2).

37. 18 U.S.C. § 2510(15).

38. *Id.* § 2711(2).

39. Kerr, *supra* note 35, at 1215-16.

40. *Id.* at 1216 (footnote omitted).

41. *Id.* at 1218.

42. 18 U.S.C. § 2703(a) (allowing government access to the contents of ECS older than 180 days using any of the methods available for the ascertainment of the contents of RCS delineated in subsection (b), which does not require a warrant).

question since the Sixth Circuit, in *United States v. Warshak*, found that a user has a reasonable expectation of privacy in the contents of his e-mails regardless of their age.[43] Although *Warshak* is binding only in the Sixth Circuit, many circuits have recognized the validity of this approach,[44] and the Department of Justice has acquiesced to the holding nationwide by instituting a policy requiring the use of warrants when requesting disclosure of the contents of e-mails.[45] Therefore, law enforcement, in all likelihood, will need a warrant to obtain any content held by providers of ECS.

Unlike its approach to content held by ECS providers, the SCA gives the government three alternatives for obtaining content held by a provider of RCS: (1) a search warrant,[46] requiring probable cause;[47] (2) prior notice and a subpoena,[48] the latter requiring a showing of relevance, specificity, and admissibility;[49] or (3) prior notice and a court order[50] with "specific and articulable facts showing that there are reasonable grounds to believe that the contents . . . are relevant and material to an ongoing criminal investigation."[51] Clearly, the standards for obtaining a subpoena and court order fall far short of the probable cause required for a warrant.

---

43. 631 F.3d 266, 288 (6th Cir. 2010).

44. *See In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197, 222-23 (2d Cir. 2016) (Lynch, J., concurring in the judgment) (citing *Warshak* to support the proposition that the SCA "requirements are in many ways less protective of privacy than many might think appropriate" but declining to address the defects of the SCA); Vista Mktg., LLC v. Burkett, 812 F.3d 954, 969 (11th Cir. 2016) ("[A] subscriber enjoys a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial ISP.'" (quoting *Warshak*, 631 F.3d at 288)); United States v. Davis, 785 F.3d 498, 528-29 (11th Cir.) ("If our expectation of privacy in our personal communications has not changed from what it was when we only wrote letters to what it is now that we use telephones to conduct our personal interactions, it has not changed just because we now happen to use email to personally communicate." (citing *Warshak*, 631 F.3d at 288)), *cert. denied*, 136 S. Ct. 479 (2015).

45. *In re Warrant to Search a Certain E-Mail Account*, 829 F.3d at 222 n.1 (Lynch, J., concurring in the judgment) ("In the wake of *Warshak*, it has apparently been the policy of the Department of Justice since 2013 always to use warrants to require the disclosure of the contents of emails under the SCA, even when the statute permits lesser process.").

46. 18 U.S.C. § 2703(b)(A).

47. *See* Illinois v. Gates, 462 U.S. 213, 226-27, 239 (1983) (discussing the probable cause necessary for law enforcement to obtain a warrant).

48. 18 U.S.C. § 2703(b)(B)(i).

49. United States v. Nixon, 418 U.S. 683, 700 (1974).

50. 18 U.S.C. § 2703(b)(B)(ii), (d).

51. *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 606 (5th Cir. 2013) (quoting 18 U.S.C. § 2703(d)); Kerr, *supra* note 35, at 1219.

The problem is that cloud storage does not fit neatly within the parameters of either ECS or RCS. Nor did Congress mean for it to; cloud storage did not become available to consumers until years after passage of the SCA.[52] And as Kerr describes, "[a] provider can act as an RCS with respect to some communications, an ECS with respect to other communications, and neither an RCS nor an ECS with respect to other communications."[53] Cloud storage services certainly can act as providers of RCS because they store electronically transmitted content data for long periods of time.[54] But they are simultaneously "more than capable of transmitting the sort of media defined by [the] statute" as ECS.[55]

The Ninth Circuit in *Theofel v. Farey-Jones*[56] offered one solution to the problem of hybrid providers. It held that regardless of whether the content itself is clearly ECS or RCS, the lesser standard for obtaining information from providers of RCS *only* applies when that provider does not offer ECS services.[57] But many courts have disagreed with this view,[58] and Kerr believes that *Theofel* "offers a new view of the SCA's basic structure that is quite different from the traditional understanding that the Justice Department has followed."[59]

Thus, users of cloud storage may enjoy protection under the SCA because (1) many cloud storage services act as providers of both ECS and RCS; (2) *Theofel* held that the government must use the stricter ECS standard for all stored data when a provider offers both ECS and RCS services; (3) the SCA statutorily requires a warrant to obtain content less than 180 days old from a provider of ECS; and (4) *Warshak* arguably expanded that warrant requirement to cover all content, regardless of age.[60]

However, at most, this reading of the SCA only protects users' information in cloud storage accounts if the provider offers both ECS and RCS. And because

52. *See 30 Years of Accumulation: A Timeline of Cloud Computing*, *supra* note 13; *see also* Mohamed, *supra* note 13 ("[S]ince the internet only started to offer significant bandwidth in the nineties, cloud computing for the masses has been something of a late developer.").

53. Kerr, *supra* note 35, at 1215-16.

54. *See* Gold, *supra* note 34, at 2335 ("[C]loud storage has the possibility of long-term data protection.").

55. *Id.* at 2334.

56. 359 F.3d 1066 (9th Cir. 2004).

57. *Id.* at 1076-77.

58. Anzaldua v. Ne. Ambulance & Fire Prot. Dist., 793 F.3d 822, 840-41 (8th Cir. 2015) (discussing the debate surrounding the reasoning and the outcome of *Theofel*).

59. Kerr, *supra* note 35, at 1208-09.

60. *Warshak*'s application to content stored by cloud storage providers is not entirely certain because *Warshak* only dealt with e-mail. *See* United States v. Warshak, 631 F.3d 266, 282 (6th Cir. 2010).

Theofel is binding only in the Ninth Circuit and many other courts have disagreed with the holding on a variety of grounds,[61] users' privacy likely mostly relies on the protections afforded by the Fourth Amendment.

B. The Fourth Amendment

The Fourth Amendment guarantees people protection against unreasonable searches and seizures of "their persons, houses, papers, and effects"[62] by the government or private parties acting as an "instrument or agent of the Government."[63] When a person has a reasonable expectation of privacy against government actors, Fourth Amendment protection applies, and a warrantless search is presumptively unreasonable.[64]

Justice Harlan introduced the reasonable expectation of privacy standard in his 1967 concurrence in *Katz v. United States*.[65] In *Katz*, government agents used an electronic listening device placed on a public phone booth to monitor a phone call without obtaining a warrant.[66] The Court held that the "Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[67]

In his concurrence, Justice Harlan formulated a two-part test to determine whether a person has a reasonable expectation of privacy and thus Fourth Amendment protection against an unreasonable search or seizure. First, the person must exhibit "an actual (subjective) expectation of privacy."[68] Second, "the expectation [must] be one that society is prepared to recognize as 'reasonable.'"[69] Since *Katz*, the Court has adopted this test as determinative of

61. *See Anzaldua*, 793 F.3d at 840-41 (discussing cases distinguishing and disagreeing with the reasoning of *Theofel*).

62. U.S. CONST. amend. IV.

63. Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 614 (1989).

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

65. *Id.*; David A. Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2207 (2009) ("The reasonable-expectation-of-privacy test arose out of *Katz v. United States*, where Justice Harlan, concurring, outlined a two-part requirement . . . .").

66. *Katz*, 389 U.S. at 348, 356-57.

67. *Id.* at 353.

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

69. *Id.*

whether a person has a reasonable expectation of privacy for Fourth Amendment purposes.[70]

Katz also stands for two additional important principles. First, the Fourth Amendment applies to people, not places.[71] Thus, the man placing the telephone call maintained his Fourth Amendment rights even though he was using a public telephone booth.[72] In relation to cloud storage, this means that a person's data can still receive Fourth Amendment protection even if they are stored online with a cloud storage provider. Second, the Fourth Amendment protects "intangible" media, such as the oral communications in *Katz*.[73] With respect to cloud storage, this means digital data can also receive Fourth Amendment protection.[74]

Subsequent Supreme Court decisions have expanded Fourth Amendment doctrine as it relates to cloud storage in two important ways. First, the Court has clarified that Fourth Amendment protection does not rely on a property interest in the area being searched.[75] This means that a cloud storage user need not "own" his account or the server on which his data are located for the Fourth Amendment to apply. Second, a person may waive his Fourth Amendment rights, but that waiver must be voluntary as determined by the totality of the circumstances.[76] This means that a cloud storage user has control over when and how she waives her Fourth Amendment rights.

This doctrine provides a foundation for the existence of a reasonable expectation of privacy in cloud storage, but the third-party doctrine can eliminate that expectation entirely.

1. The third-party doctrine

The third-party doctrine is an incredibly problematic Fourth Amendment doctrine for providers of data services seeking to resist government intrusion into their users' data. Generally, the third-party doctrine maintains that a

70. *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 950 (2012) ("Our later cases have applied the analysis of Justice Harlan's concurrence in [*Katz*], which said that a violation occurs when government officers violate a person's 'reasonable expectation of privacy.'" (quoting *Katz*, 389 U.S. at 360 (Harlan, J., concurring))); Bond v. United States, 529 U.S. 334, 338 (2000); California v. Ciraolo, 476 U.S. 207, 211 (1986); Smith v. Maryland, 442 U.S. 735, 740 (1979).

71. *Katz*, 389 U.S. at 351.

72. *See id.* at 352.

73. *Id.* at 353 ("[W]e have expressly held that the Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements . . . .").

74. *See, e.g.*, United States v. Warshak, 631 F.3d 266, 285-86 (6th Cir. 2010) (recognizing that Fourth Amendment protection extends to e-mails).

75. Mancusi v. DeForte, 392 U.S. 364, 367-68 (1968).

76. Schneckloth v. Bustamonte, 412 U.S. 218, 219, 227 (1973).

person who voluntarily turns over information to a third party for use in its normal course of business "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[77] This is problematic for cloud storage because, at its most basic level, cloud storage requires users to give their data to a third party.

In *Hoffa v. United States*, the Court first discussed the reasoning behind what would become known as the third-party doctrine.[78] In *Hoffa*, the famed James (Jimmy) Hoffa made statements to a companion who then disclosed the information to the government.[79] Hoffa argued that his conversations with the informant were private and thus that the government had obtained the information in violation of the Fourth Amendment.[80] The Court disagreed, holding that the Fourth Amendment does not protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it" to the government.[81] Three subsequent cases have clarified this doctrine: *United States v. Miller*,[82] *Smith v. Maryland*,[83] and *Couch v. United States*.[84]

Ten years after *Hoffa*, in *United States v. Miller*, the Court applied the third-party doctrine to records given to a bank, thus extending the doctrine to information given to a third-party business. In *Miller*, government agents issued subpoenas to two banks and obtained banking records suggesting that the depositor possessed an illegal still.[85] The depositor argued that the Fourth Amendment protected his records because they constituted his private information.[86] Furthermore, because banks were required by law to keep the records, applying the third-party doctrine would allow the government to effectively circumvent the Fourth Amendment by (1) requiring the collection of private information and then (2) arguing that compliance with the law eliminated the privacy protections provided by the Fourth Amendment.[87]

The Court rejected the depositor's arguments and refused to find that the depositor had a reasonable expectation of privacy in his bank records.[88] The

77. United States v. Miller, 425 U.S. 435, 442-43 (1976).

78. 385 U.S. 293, 302-03 (1966).

79. *Id.* at 296.

80. *See id.* at 300.

81. *Id.* at 302.

82. 425 U.S. 435.

83. 442 U.S. 735 (1979).

84. 409 U.S. 322 (1973).

85. 425 U.S. at 437.

86. *See id.* at 438-39.

87. *Id.* at 439.

88. *Id.* at 443.

Court looked to "the nature of the particular documents sought to be protected in order to determine whether there [wa]s a legitimate 'expectation of privacy' concerning their contents."[89] Because the depositor could "assert neither ownership nor possession" of the records, the Court found that they were simply "the business records of the banks."[90] Most importantly, "[a]ll of the documents obtained, including financial statements and deposit slips, contain[ed] only information *voluntarily conveyed* to the banks and *exposed to their employees in the ordinary course of business*."[91] Thus, the Court held,

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[92]

Just three years later, in *Smith v. Maryland*, the Court reinforced the third-party doctrine, finding that a telephone user had no reasonable expectation of privacy in the phone numbers he dialed.[93] In *Smith*, the government installed a pen register (a device that captures the phone numbers dialed from a particular phone line) on a telephone company's equipment in order to determine if a man was making threatening calls to a woman.[94] The man argued that he had a reasonable expectation of privacy in the phone numbers he dialed on his personal phone and thus that the government's installation of the pen register constituted an illegal search.[95] The Court determined that subscribers must have realized the phone company could make "permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills."[96] The Court summarized the reasons behind its application of the third-party doctrine, stating that "[t]elephone users . . . typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes."[97] As in *Miller*, the Court emphasized that the telephone user

89. *Id.* at 442.

90. *Id.* at 440.

91. *Id.* at 442 (emphasis added).

92. *Id.* at 443.

93. 442 U.S. 735, 742 (1979).

94. *Id.* at 737.

95. *Id.* at 741-42.

96. *Id.* at 742.

97. *Id.* at 743.

exposed his information to the telephone company for use "in the ordinary course of business."[98]

Notably, the Court in *Smith* also determined it did not matter that the telephone company used automated switching equipment instead of a human operator for the calls in question.[99] It remained the case, "[r]egardless of the phone company's election, [that] petitioner voluntarily conveyed to it information that it had facilities for recording and that it was free to record."[100] The *Smith* Court also distinguished the electronic monitoring in *Katz* from the interception of phone numbers in *Smith*. In *Katz*, government agents secretly intercepted the content of calls.[101] But in *Smith*, the government only ascertained information the third-party telephone company had the right to record—the phone numbers dialed.[102]

Finally, in another case applying the third-party doctrine, Justice Brennan provided examples of when the doctrine would not apply to information given to third parties. In *Couch v. United States*, the Court ruled on codependent Fourth and Fifth Amendment claims, holding that the IRS could obtain bank, payroll, and expenditure records from a woman's accountant using only a summons because the woman had voluntarily given the records to her accountant for use in completing her tax returns.[103] Justice Brennan, concurring, attempted to clarify when an individual may rely upon the law to create a "private enclave where [she] may lead a private life,"[104] stating,

> [T]he privilege is available to one who turns records over to a third person for *custodial safekeeping rather than disclosure* of the information; to one who turns records over to a third person at the *inducement of the Government*; to one who places records in a *safety deposit box or in hiding*; and to similar cases *where reasonable steps have been taken to safeguard the confidentiality of the contents of the records*. The privilege cannot extend, however, to the protection of a taxpayer's records conveyed to a retained accountant for use in preparation of an income tax return, where the accountant is himself obligated to prepare a complete and lawful return.[105]

98. *Id.* at 744 (quoting United States v. Miller, 425 U.S. 435, 442 (1976)).

99. *Id.* at 744-45.

100. *Id.* at 745.

101. *See* Katz v. United States, 389 U.S. 347, 348 (1967).

102. *Smith*, 442 U.S. at 741. *But see* United States v. Warshak, 631 F.3d 266, 287 (6th Cir. 2010) (discussing how telephone operators during the time of *Katz* "had a right to monitor calls in certain situations").

103. 409 U.S. 322, 323-24, 325 n.6, 335, 336 n.19 (1973).

104. *Id.* at 338 (Brennan, J., concurring) (alteration in original) (quoting Murphy v. Waterfront Comm'n, 378 U.S. 52, 55 (1964)).

105. *Id.* at 337 (emphasis added) (footnote omitted) (citations omitted).

Thus, the Court articulated through *Miller*, *Smith*, and *Couch* that the third-party doctrine eliminates a person's reasonable expectation of privacy in (1) information voluntarily disclosed (2) for use by a third party (3) in its normal course of business. *Each* of these elements is required for the third-party doctrine to apply when a user divulges information to a third party for business purposes. But companies often provide services over the Internet that do not fit neatly into the third-party doctrine's defined boundaries. In fact, because of the various methods and purposes with which data are stored and produced online, it is unclear how the third-party doctrine applies to the Internet.

2. A cloudy battleground: the third-party doctrine and the Internet

Like the SCA, the third-party doctrine has failed to keep pace with technological change, and the Supreme Court has yet to explain how the doctrine operates in the digital age. For example, in 2014, the Court missed an opportunity to elaborate on how the third-party doctrine interacts with the Internet in *Riley v. California*, where the Court held that law enforcement must obtain a warrant to access cell phone data.[106] But in its holding, the Court made no mention of the third-party doctrine, even though the doctrine seemed to be implicated because cell phone data can be stored locally (entirely on the phone) or remotely in the cloud.[107] The Court's holding nonetheless suggested that data stored in the cloud "may enjoy some Fourth Amendment protection" for three reasons.[108] First, the Court recognized "the intrusiveness of police access to cloud-based data,"[109] noting that searching files stored in the cloud "would be like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house."[110] "Second, the Court suggested that privacy is compatible with certain data stored online."[111] The Court noted that an "Internet search and browsing history . . . could reveal an individual's private interests or concerns."[112] Finally, and perhaps most importantly, "the Court suggested that the precise medium in which digital data is stored is

106. 134 S. Ct. 2473, 2493-95 (2014) (implying that users have a reasonable expectation of privacy in cell phone data, as a warrant is only necessary when the search would otherwise violate an individual's reasonable expectation of privacy).

107. *See id.*

108. Ryan Watzel, Riley*'s Implications for Fourth Amendment Protection in the Cloud*, 124 YALE L.J.F. 73, 76 (2014).

109. *Id.*

110. *Riley*, 134 S. Ct. at 2491.

111. Watzel, *supra* note 108, at 77.

112. *Riley*, 134 S. Ct. at 2490 (citing United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring)).

irrelevant to whether that data receives Fourth Amendment protection."[113] It noted that "[c]ell phone users often may not know whether particular information is stored on the device or in the cloud, *and it generally makes little difference*."[114] So while the relationship between the third-party doctrine and the Internet remains unclear, the Court has at least somewhat acknowledged the need for data privacy regardless of where the data are stored.

Of the Justices, only Justice Sotomayor has offered clear insight into the interplay between the third-party doctrine and the Internet. In *United States v. Jones*, the majority found that the government's collection of GPS data from a car over a period of four weeks violated the driver's Fourth Amendment rights based on trespass theory.[115] But Justice Sotomayor dug deeper into the technological implications of such tracking, observing,

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.[116]

Justice Sotomayor further explained, "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."[117]

While there certainly exists a debate over the modern application of the third-party doctrine, many privacy advocates would agree with Justice Sotomayor's views or go even further, arguing not only that the third-party doctrine does not suit the digital age but that *Miller* and *Smith* were wrongly decided.[118] Thus, the stage is set for the Court to recognize the inadequacy of the legal doctrines currently protecting digital privacy rights and to acknowledge the inherent differences between the storage of data in the digital age and the foundational principles of the third-party doctrine.

---

113. Watzel, *supra* note 108, at 77.

114. *Riley*, 134 S. Ct. at 2491 (emphasis added).

115. 132 S. Ct. at 948-50.

116. *Id.* at 957 (Sotomayor, J., concurring) (citations omitted).

117. *Id.*

118. *See, e.g.*, Orin Kerr & Greg Nojeim, *The Data Question: Should the Third-Party Records Doctrine Be Revisited?*, A.B.A. J. (Aug. 1, 2012, 9:20 AM CDT), http://www.abajournal.com/magazine/article/the_data_question_should_the_third-party_records_doctrine_be_revisited (debating the modern-day application of the third-party doctrine and the legal principles upon which the doctrine was founded).

III. Cloud Storage and the Fourth Amendment

With the evolution and purpose of Fourth Amendment protection in mind, cloud storage must be examined to determine whether a user should enjoy privacy in her data stored in the cloud. To that end, first, *Katz* must be applied to establish whether a user has a reasonable expectation of privacy in her information stored in the cloud. If a reasonable expectation of privacy exists, then it must be determined whether the third-party doctrine eliminates a user's privacy because the user has relinquished her data to a third-party company.

A. Applying *Katz* to Cloud Storage

For Fourth Amendment protection to apply, users must have a reasonable expectation of privacy in their data stored in the cloud.[119] While the Supreme Court has not addressed this issue, the Sixth Circuit's decision finding that users have a reasonable expectation of privacy in e-mail offers guidance in applying *Katz* to other Internet services. In *United States v. Warshak*, the government requested that an ISP "preserve the contents of any emails to or from [a user's] email account" beginning in October 2004.[120] In January 2005, pursuant to the SCA, the government served a subpoena on the ISP and obtained the user's archived e-mails because they were more than 180 days old.[121] To determine whether the search violated the user's Fourth Amendment rights, the Sixth Circuit applied *Katz* and found that the user had exhibited a subjective expectation of privacy based on the "often sensitive and sometimes damning substance of [the user's] emails."[122] The court further found that society is prepared to recognize the user's subjective expectation of privacy as reasonable because the Fourth Amendment protects traditional forms of communication like letters.[123] Thus, the court held that users have a reasonable expectation of privacy in their e-mails, explaining that "[g]iven the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection."[124]

A similar application of *Katz* in the context of cloud storage suggests that users have a reasonable expectation of privacy in the contents of their cloud storage accounts. First, a user exhibits a subjective expectation of privacy by creating a password-protected account and relying on a provider's representa-

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

120. 631 F.3d 266, 283 (6th Cir. 2010).

121. *See id.* at 282-83.

122. *Id.* at 284.

123. *Id.* at 285-86.

124. *Id.*

tion that it will keep any information the user uploads secure.[125] This is the equivalent of renting a safety deposit box, locking it, and trusting the bank not to break the lock.[126] Users likely expect the files in cloud storage to remain secure unless they themselves share the files with other users. Furthermore, as with the e-mails in *Warshak*, this subjective expectation of privacy could be shown on a case-specific basis by examining the contents of the user's account and the user's actions with regard to the security of the account.[127]

Second, a cloud storage user's expectation of privacy in her cloud storage account is one that society is prepared to find reasonable. In *Warshak*, the Sixth Circuit warned that the Fourth Amendment "must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish."[128] It then determined that the Fourth Amendment protects e-mails based on its historic protection of other "traditional forms of communication."[129] The same parallels can be drawn between cloud storage and the Fourth Amendment's historic protection of traditional forms of storage. Traditional storage areas—such as lockers, storage units, and safety deposit boxes—have long been used to store an individual's private documents and effects. And courts have afforded Fourth Amendment protection to such storage areas.[130] Now, as information is increasingly produced and stored in digital form, cloud storage has become the digital equivalent of a traditional storage area.

An argument could be made that since Edward Snowden revealed the extensive interception of Americans' Internet traffic by the National Security Agency (NSA), society might not accept a cloud storage user's expectation of

125. *See, e.g.*, *Google Privacy Policy*, *supra* note 7 (discussing the methods by which Google secures data to keep them private); *Is Dropbox Safe to Use?*, *supra* note 11 (describing security measures implemented by Dropbox to protect data).

126. *See* Couch v. United States, 409 U.S. 322, 337 (1973) (Brennan, J., concurring) ("[T]he privilege is available to . . . one who places records in a *safety deposit box or in hiding* . . . ." (emphasis added)).

127. *See Warshak*, 631 F.3d at 284 (finding a subjective expectation of privacy based on the "often sensitive and sometimes damning substance of [the defendant's] emails"); *see also* United States v. Miller, 425 U.S. 435, 442 (1976) (looking to "the nature of the particular documents sought to be protected in order to determine whether there [wa]s a legitimate 'expectation of privacy' concerning their contents").

128. 631 F.3d at 285.

129. *Id.* at 285-86.

130. *See, e.g.*, United States v. Chadwick, 433 U.S. 1, 11 (1977) ("By placing personal effects inside a double-locked footlocker, respondents manifested an expectation that the contents would remain free from public examination."), *abrogated by* California v. Acevedo, 500 U.S. 565 (1991); *Couch*, 409 U.S. at 337 (Brennan, J., concurring) (suggesting that individuals have a reasonable expectation of privacy in the contents of a safety deposit box); Garcia v. Dykstra, 260 F. App'x 887, 899 (6th Cir. 2008) (implying a reasonable expectation of privacy in a storage unit).

privacy as "reasonable."[131] But government programs of dubious legality should not rob the Fourth Amendment of its core—protection against *unreasonable* searches and seizures. This finds support in *Riley*, where following the Snowden revelations, the Court still found a reasonable expectation of privacy in the digital contents of a phone and expressed concern about the information stored in the cloud. Even though the searches in *Riley* occurred before the Snowden revelations, it is telling that the Court never mentioned the NSA's surveillance programs.[132] This suggests that general government interception of phone data does not affect the reasonable expectation of privacy in the phone's digital contents.

In fact, the government has increased the reasonableness of a cloud storage user's expectation of privacy rather than obliterated it. The Federal Trade Commission (FTC), for instance, brings enforcement actions against companies that fail to comply with their stated privacy standards.[133] Recent FTC consent decrees reveal the government's recognition of a social expectation that data stored in the cloud will be stored privately, as promised in providers' terms of service and privacy policies.[134] The government could

131. *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013, 6:05 AM EDT), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (revealing that the NSA was collecting telephone numbers of Verizon users on a daily basis); Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN (June 7, 2013, 3:23 PM EDT), https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (describing an NSA surveillance program that collected the "search history, the content of emails, file transfers and live chats" of users of a number of major technology services); *see also* Sarah Childress, *How the NSA Spying Programs Have Changed Since Snowden*, PBS (Feb. 9, 2015), http://www.pbs.org/wgbh/frontline/article/how-the-nsa-spying-programs-have-changed-since-snowden (describing the minimal changes in NSA practices since the Snowden revelations).

132. *See* Riley v. California, 134 S. Ct. 2473, 2491 (2014).

133. *See Enforcing Privacy Promises*, FED. TRADE COMMISSION, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises (last visited Mar. 3, 2017) (describing the FTC's policy for bringing actions to enforce companies' promises; stating that the "FTC has brought legal actions against organizations that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information"; and giving updated press releases on FTC enforcement actions).

134. *See, e.g.*, *Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises*, FED. TRADE COMMISSION (Nov. 29, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep (discussing a settlement with Facebook following "charges that [Facebook] deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public"); *FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network*, FED. TRADE COMMISSION (Mar. 30, 2011), https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz (discussing a settlement with Google following allegations that Google "used deceptive tactics and

footnote continued on next page

not rationally argue that users have no reasonable expectation of privacy in information stored in the cloud but, at the same time, penalize companies that fail to live up to their promised privacy standards.

Thus, courts should bring the Fourth Amendment up to speed with the technological progress that has brought about cloud storage by looking to traditional protection of storage areas and to the government's enforcement actions.

B. The Third-Party Doctrine and the Reasonable Expectation of Privacy in Cloud Storage

Absent provider access pursuant to its terms of service, the third-party doctrine does not eliminate a cloud storage user's reasonable expectation of privacy in information stored in the cloud because there has been no *use* of the information. The Sixth Circuit addressed this issue in relation to ISPs in *Warshak*. There, the court looked at the function of ISPs, noting that an "ISP is the intermediary that makes email communication possible" and thus is "the functional equivalent of a post office or a telephone company."[135] In light of this role, the court came to two key conclusions as to when use of an ISP does not eliminate a user's Fourth Amendment privacy rights under the third-party doctrine.

First, "the mere *ability* of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy."[136] As an example, the court offered that the operator in *Katz* had the ability to listen to and record the relevant phone calls.[137] Still, the *Katz* Court found that a reasonable expectation of privacy existed.[138] The court likewise noted by analogy the ability of a mail carrier to open a letter entrusted to him but stated that "trusting a letter to an intermediary does not necessarily defeat a reasonable expectation that the letter will remain private."[139]

---

violated its own privacy promises to consumers when it launched its social network, Google Buzz"); *Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False*, FED. TRADE COMMISSION (May 8, 2014), https://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were (discussing a settlement with Snapchat following allegations that Snapchat "deceived consumers over the amount of personal data it collected and the security measures taken to protect that data from misuse and unauthorized disclosure").

135. United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010).

136. *Id.* at 286-87.

137. *Id.* at 285, 287.

138. *Id.* at 287; *see also* Katz v. United States, 389 U.S. 347, 359 (1967).

139. *Warshak*, 631 F.3d at 285.

Second, the ISP's *right* of access also does not necessarily eliminate the user's reasonable expectation of privacy.[140] For this proposition, the court found support in the fact that the telephone company in *Katz* had the right to monitor the call because "telephone companies could listen in when reasonably necessary to 'protect themselves and their properties against the improper and illegal use of their facilities.'"[141] Yet, again, the Sixth Circuit recognized that the *Katz* Court found a reasonable expectation of privacy still existed.[142] Thus, the user's reasonable expectation of privacy did not rest solely on the ISP's ability or right to access the information but also on its promise of when, why, and how it did so.

The court also analogized e-mail to three areas traditionally protected by the Fourth Amendment. First, the court looked at traditional forms of communication and found that the Fourth Amendment protected intangible, oral communications[143] and sealed letters[144] despite the ability of a third-party intermediary (such as an operator or mail carrier) to intrude on the communication. Second, the court noted that "[h]otel guests . . . have a reasonable expectation of privacy in their rooms . . . even though maids routinely enter hotel rooms to replace the towels and tidy the furniture."[145] Finally, the court explained that "tenants have a legitimate expectation of privacy in their apartments . . . [that] persists, regardless of the incursions of handymen to fix leaky faucets."[146]

In all of these cases, third parties have both the ability and the right to access that in which a person maintains a reasonable expectation of privacy. But in none of these cases is there *use* of that which has been accessed. The intermediary enabling communications only maintains its network; the maid and handyman perform only their limited maintenance activities. The *Warshak* court recognized these analogous limitations and found that because the ISP's subscriber agreement only "indicat[ed] that '[the ISP] *may* access and use individual Subscriber information in the operation of the Service and as necessary to protect the Service' . . . [,] the degree of access granted to [the ISP]

140. *Id.* at 287.

141. *Id.* (quoting Bubis v. United States, 384 F.2d 643, 648 (9th Cir. 1967)).

142. *Id.*; *see also Katz*, 389 U.S. at 359.

143. *Warshak*, 631 F.3d at 285 (citing Smith v. Maryland, 442 U.S. 735, 746-47 (1979) (Stewart, J., dissenting); and *Katz*, 389 U.S. at 352).

144. *Id.* (citing United States v. Jacobsen, 466 U.S. 109, 114 (1984); and *Ex parte* Jackson, 96 U.S. 727, 733 (1877)) (noting that police must obtain a warrant to search a sealed letter "despite the fact that sealed letters are handed over to perhaps dozens of mail carriers, any one of whom could tear open the thin paper envelopes that separate the private words from the world outside").

145. *Id.* at 287.

146. *Id.*

does not diminish the reasonableness of [the user's] trust in the privacy of his emails."[147] This same logic extends to data stored in the cloud.

Notably, *Warshak* takes a different approach to the third-party doctrine than do *Miller* and *Smith*. In *Miller*, the Court disregarded both the limited purpose for which the depositor gave the bank information and the confidence the depositor had in the bank that it would not reveal that information to the government.[148] But *Warshak* adapts to the digital age by recognizing the limited access and use described in the subscriber agreement and basing the user's reasonable expectation of privacy on his confidence that the ISP will not overstep those limitations.[149] This means that the simple act of handing digital information over to a third party is insufficient to relinquish the reasonable expectation of privacy in that information.[150] Rather, the purpose for which the information will be used and the third party's promises of privacy enter into the equation and can be the basis for a user's reasonable expectation of privacy.

Further, in *Smith*, the Court determined that the use of an automated operator did not matter and rested that determination on the fact that the telephone company could record all the numbers called regardless of whether the operator was a human or computer.[151] But in *Warshak*, the user retained a reasonable expectation of privacy in the contents of e-mails that were automatically routed as they passed through the ISP's servers, even though the ISP could store the contents of those e-mails.[152] There is, of course, a difference between recording a phone number (metadata[153]) and storing the content of a communication. But *Warshak* shows the limitations of *Smith*—that the ability and right to access or record digital information do not necessarily eliminate a user's reasonable expectation of privacy in that information. Recognizing these limitations is a major step toward acknowledging the inherent flaw in blindly applying the third-party doctrine to cloud storage.

147. *Id.* (quoting *NuVox Acceptable Use Policy*, WINDSTREAM, http://business.windstream.com/Legal/acceptableUse.htm (last visited Aug. 12, 2010)).

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

149. *Warshak*, 631 F.3d at 286-87.

150. *See* Couch v. United States, 409 U.S. 322, 337 (1973) (Brennan, J., concurring) (stating that the third-party doctrine does not apply when records are turned over "for custodial safekeeping" or when other steps are taken "to safeguard the confidentiality of the contents of the records").

151. Smith v. Maryland, 442 U.S. 735, 745 (1979).

152. *Warshak*, 631 F.3d at 286.

153. For a discussion of metadata, see Brad Turner, *When Big Data Meets Big Brother: Why Courts Should Apply* United States v. Jones *to Protect People's Data*, 16 N.C. J.L. & TECH. 377, 398-401 (2015).

C. Why the Third-Party Doctrine Does Not Fit Cloud Storage

It might seem that the third-party doctrine applies to many Internet services and functions. One of the main concepts of the doctrine—relinquishment of information to a third party—certainly applies to innumerable online data services. But that understanding ignores the requirements of *voluntary* relinquishment pertinent to the third party's *use* of that information in the normal course of business for a user to lose her Fourth Amendment privacy rights. And use by cloud storage services differs fundamentally from use by the services provided in *Smith* and *Miller*.[154] This difference explains why the third-party doctrine should not apply to all information in cloud storage.

In *Miller*, the depositor voluntarily gave his documents to the banks for their use in the ordinary course of business.[155] Thus, when the depositor turned over the documents, he expected them to be used and retained by the bank as part of the bank's records.[156] Similarly, in *Smith*, the Court noted that telephone users understand (1) that phone companies have to use telephone numbers in their ordinary course of business to complete calls[157] and (2) that phone companies could keep those phone numbers in their records, as shown by users' phone bills.[158] Thus, the third-party doctrine evolved to cover voluntary disclosure of information to a third party with the understanding that the third party would use—and could keep a record of—that information in its normal course of business. But cloud storage services do not operate in this way. Courts have identified two critical issues with applying the third-party doctrine to cloud storage.

First, especially in cases involving e-mail contents, cell-site location data, and GPS location data, the Court has questioned whether users *voluntarily* store their information in the cloud.[159] Logically, it follows that a person cannot voluntarily consent to cloud storage if she does not know what information she has stored in the cloud. However, while voluntariness may be questioned in cases where users may not understand or know how and when their data are

154. For the sake of argument, this Note assumes that the Court correctly decided *Miller* and *Smith*.

155. United States v. Miller, 425 U.S. 435, 442 (1976).

156. *See id.* at 440.

157. Smith v. Maryland, 442 U.S. 735, 742 (1979).

158. *Id.*

159. Riley v. California, 134 S. Ct. 2473, 2491 (2014) ("Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference."); United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (stating that the third-party doctrine "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").

backed up to the cloud, a court would likely find that users voluntarily supply information to services like Dropbox because the users must affirmatively create accounts and upload files into storage.[160] This is to say that there is a difference between a user purchasing a phone and not knowing how and where the information it contains is stored versus a user actively engaging with a cloud storage service for the purpose of data storage. Therefore, for this type of cloud storage service, courts likely would find that users voluntarily consented to cloud storage, and the difference for these services must rest in "use."

The second issue with applying the third-party doctrine to cloud storage is that most users likely do not store information on cloud storage services with the understanding that cloud storage providers will access and use that information in their normal course of business. While defining "use" is beyond the scope of this Note,[161] users of cloud storage services likely do not expect providers to make or keep records of their content in any manner resembling the bank records in *Miller* or the telephone bill in *Smith* unless the terms of service so state. Users may understand that scanning for advertisement or customization purposes results in the creation of a user "profile,"[162] but it is a stretch to argue that users expect that profile to include a comprehensive log of all content information stored in their accounts. Rather, these profiles likely contain keywords gleaned from the content but not the content itself.[163] The

160. Google Drive is an exception to this generalization, as it does not require opening a separate account; rather, it is included with a Google e-mail account. However, Google Drive only stores files the user has specifically uploaded to Drive or created within Drive. *See Get Started with Google Drive*, GOOGLE, https://support.google.com/drive/answer/2424384?hl=en (last visited Mar. 3, 2017).

161. For insightful thoughts on the reasoning behind "use" in the third-party doctrine and the doctrine's application to modern technology, see Orin Kerr, *The Case for the Third Party Doctrine*, A.B.A., https://www.americanbar.org/groups/public_services/law_national_security/patriot_debates2/the_book_online/ch4/ch4_ess2.html (last visited Mar. 3, 2017), which argues that the third-party doctrine should be invoked anytime a third party is not "merely a conduit for information"; and Greg Nojeim, *Reply to Orin Kerr*, A.B.A., https://www.americanbar.org/groups/public_services/law_national_security/patriot_debates2/the_book_online/ch4/ch4_res1.html (last visited Mar. 3, 2017), which replies to Kerr and argues that there should be more exceptions to the third-party doctrine so that more than just content—that is, the information for which the third party is a mere conduit—is protected.

162. *See, e.g.*, Sarah Kessler, *Google Thinks I'm a Middle-Aged Man: What About You?*, MASHABLE (Jan. 25, 2012), http://mashable.com/2012/01/25/google-cookies/#yo0ngcaxomqv (describing Google's profiles for targeted advertising).

163. *See id.* (discussing how Google's "Ads Preferences" tab shows categories based on web browsing habits); Jason Mick, *Google: Yes, We "Read" Your Gmail*, DAILYTECH (Aug. 15, 2013, 3:30 PM), http://www.dailytech.com/Google+Yes+we+Read+Your+Gmail/article33184.htm (reviewing Google's legal brief explaining that Google uses keywords from e-mails to target users with advertising). More information about specific (likely

footnote continued on next page

only list or record a user expects to be made of the full contents of her cloud storage account is the one she sees when she logs in. And this list is provided for organizational purposes, not as a record for use by the provider. This is in stark contrast to situations like those in *Smith* and *Miller*, where the relevant records were created by the companies specifically for their use in the normal course of business.

Instead, cloud storage is simply a digital space owned by a third party and "leased" to the user. Apt analogies can be drawn to physical spaces such as hotel rooms,[164] desks,[165] lockers,[166] and storage units[167]—all of which enjoy Fourth Amendment protection. These analogies also draw support directly from the Fourth Amendment itself. The "papers" and "effects"[168] of 1791 are now in the form of digital files. A lock is now a password.[169] Technology has changed the medium, but the underlying purpose remains the same. Thus, to understand how the third-party doctrine affects a user's reasonable expectation of privacy in cloud storage accounts, it is useful to understand when a person enjoys a reasonable expectation of privacy in a locked physical space owned by a third party.

Overwhelmingly, the Court has determined that individuals have a reasonable expectation of privacy in such spaces. For example, the Court has found that both hotel guests[170] and rooming house tenants[171] have reasonable expectations of privacy in their rooms. Similarly, public employees have a reasonable expectation of privacy in their offices—including desks and filing

confidential) technology is needed to solidify the claim that user profiles do not contain full records of content information.

164. *See, e.g.*, Stoner v. California, 376 U.S. 483, 490 (1964) ("[A] guest in a hotel room is entitled to constitutional protection against unreasonable searches and seizures.").

165. *See, e.g.*, O'Connor v. Ortega, 480 U.S. 709, 719 (1987) (plurality opinion) (finding a reasonable expectation of privacy in a public employee's desk).

166. *See, e.g.*, United States v. Chadwick, 433 U.S. 1, 11 (1977) ("By placing personal effects inside a double-locked footlocker, respondents manifested an expectation that the contents would remain free from public examination."), *abrogated by* California v. Acevedo, 500 U.S. 565 (1991).

167. *See, e.g.*, Garcia v. Dykstra, 260 F. App'x 887, 892-93 (6th Cir. 2008) (finding a reasonable expectation of privacy in a storage unit).

168. 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 . . . .").

169. *See* United States v. Buckner, 473 F.3d 551, 554 n.2 (4th Cir. 2007) (finding that the district court's determination that the defendant had a reasonable expectation of privacy in password-protected computer files was not clearly erroneous).

170. Stoner v. California, 376 U.S. 483, 490 (1964) ("[A] guest in a hotel room is entitled to constitutional protection against unreasonable searches and seizures.").

171. McDonald v. United States, 335 U.S. 451, 452, 454, 456 (1948) (finding the warrantless search and seizure of items from a tenant's room violated the Fourth Amendment).

cabinets—although that expectation "may be reduced by virtue of actual office practices and procedures, or by legitimate regulation."[172] And more generally, people can maintain their reasonable expectation of privacy in spaces by closing[173] or locking the space.[174]

The Third Circuit followed this trend in a case involving a physical locker,[175] which is directly analogous to cloud storage. In *United States v. Speights*, the Third Circuit found that a police officer had a reasonable expectation of privacy in his police locker, which had been secured by both personal and police-issued locks.[176] The court noted that because the officer "was permitted to keep personal belongings in his locker," there "was no regulation or notice that the lockers might be searched" and that because the officer "took affirmative action to secure his privacy" by placing a personal lock on the locker, the officer had made a "prima facie showing of a reasonable expectation of privacy."[177]

Similarly, in the context of storage units, the Tenth Circuit observed that "[p]eople generally have a reasonable expectation of privacy in a storage unit, because storage units are secure areas that 'command a high degree of privacy.'"[178] Moreover, the Tenth Circuit has stated that the "type of container at issue is . . . an important consideration" because the

> [c]ommon experience of life, clearly a factor in assessing the existence and the reasonableness of privacy expectations, surely teaches all of us that the law's 'enclosed spaces'—mankind's valises, suitcases, footlockers, strong boxes, etc.—are frequently the objects of his highest privacy expectations, and that the expectations may well be at their most intense when such effects are deposited temporarily . . . *in places under the general control of another.*[179]

And although appellate courts rarely have occasion to confront the issue whether a person has a reasonable expectation of privacy in her safety deposit

172. O'Connor v. Ortega, 480 U.S. 709, 717 (1987) (plurality opinion).

173. *See, e.g.*, United States v. Monghur, 588 F.3d 975, 981 (9th Cir. 2009) (discussing a defendant's reasonable expectation of privacy in a closed container).

174. *See* United States v. Chadwick, 433 U.S. 1, 11 (1977) ("By placing personal effects inside a double-locked footlocker, respondents manifested an expectation that the contents would remain free from public examination."), *abrogated by* California v. Acevedo, 500 U.S. 565 (1991).

175. United States v. Speights, 557 F.2d 362, 362 (3d Cir. 1977).

176. *Id.* at 362, 365.

177. *Id.* at 363.

178. United States v. Johnson, 584 F.3d 995, 1001 (10th Cir. 2009) (quoting United States v. Salinas-Cano, 959 F.2d 861, 864 (10th Cir. 1992)) (citing United States v. Chaves, 169 F.3d 687, 690-91 (11th Cir. 1999); and United States v. Johns, 851 F.2d 1131, 1135-36 (9th Cir. 1988)).

179. *Salinas-Cano*, 959 F.2d at 864 (second alteration in original) (emphasis added) (quoting United States v. Block, 590 F.2d 535, 541 (4th Cir. 1978)).

box, Justice Brennan's concurrence in *Couch* strongly suggests this expectation exists.[180] The Seventh Circuit agreed by analogy in *United States v. Shelby* when it explained that "garbage cans cannot be equated to a safety deposit box. The contents of the cans could not reasonably be expected by defendant to be secure, nor entitled to respectful, confidential and careful handling on the way to the dump."[181] In all of these cases, the third-party doctrine failed to eliminate the storing user's reasonable expectation of privacy in the storage area even though other people could access the storage space.

Some may argue that cloud storage is different and that a user's expectation of privacy cannot be reasonable because of the prevalence of hacking and data breaches.[182] But these weaknesses do not make users' trust in the security of cloud storage any less reasonable than their trust in physical storage spaces. For example, a physical locker could be broken into by snapping the lock. A safety deposit box could be ransacked during a bank robbery. But as shown by the cases suggesting a reasonable expectation of privacy in both of those spaces,[183] the illicit actions of third parties are not typically considered in the Fourth Amendment analysis.

Thus, the overarching purpose of the third-party doctrine weighs against its application to cloud storage services. Cases involving physical storage spaces show that application of the third-party doctrine to cloud storage is improper because of the lack of *use* by the third party. However, a cloud storage provider can define its ability to "use" user information in its terms of service. Thus, whether the Fourth Amendment protects the contents of cloud storage may rest upon when providers "use" user data pursuant to their terms of service.

IV. Terms of Service and Privacy in Cloud Storage

As shown by Fourth Amendment analysis, "use" is key to the elimination of a user's reasonable expectation of privacy under the third-party doctrine. Historically, network providers have been allowed to access certain

180. Couch v. United States, 409 U.S. 322, 337 (1973) (Brennan, J., concurring) ("[T]he privilege is available . . . to one who places records in a safety deposit box . . . .").

181. 573 F.2d 971, 973 (7th Cir. 1978).

182. *See, e.g.*, Nicole Perlroth, *Yahoo Says Hackers Stole Data on 500 Million Users in 2014*, N.Y. TIMES (Sept. 22, 2016), http://nyti.ms/2cV0i7T (discussing a data breach where hackers stole the account information of 500 million users).

183. United States v. Chadwick, 433 U.S. 1, 11 (1977) (finding a reasonable expectation of privacy in a locked footlocker), *abrogated by* California v. Acevedo, 500 U.S. 565 (1991); *Couch*, 409 U.S. at 337 (Brennan, J., concurring) (suggesting a person would have a reasonable expectation of privacy in the contents of her safety deposit box).

information on their networks.[184] But while cloud storage providers can access and use information on their networks in a variety of ways, only certain types of access lead to the elimination of a user's reasonable expectation of privacy in her information.

A. Historical Acceptance of Provider Access to User Data

Society has long recognized a fundamental necessity for network providers (such as telegraph, telephone, and Internet providers) to control, maintain, secure, and ensure the stability of their networks by accessing user information.[185] And the law has accommodated that necessity without regard for law enforcement's professed need for access.[186] Without detailing this entire history, this Note begins with Congress's enactment in 1968 of Title III of the Omnibus Crime Control and Safe Streets Act.[187]

In that Act, Congress protected users of networks by forbidding law enforcement from "intercepti[ng] . . . wire, oral, or electronic communication" without a judicial order.[188] But it specifically granted network providers access to users' content by stating,

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity *which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service* . . . .[189]

184. *See, e.g.*, Bubis v. United States, 384 F.2d 643, 648 (9th Cir. 1967) (noting communication systems' "fundamental right to take reasonable measures to protect themselves and their properties against the illegal acts of a trespasser").

185. *See id.* at 647-48.

186. *See, e.g.*, Nardone v. United States, 302 U.S. 379, 380-81, 383 (1937) (finding the Federal Communications Act's provision that "no person who, as an employe [sic], has to do with the sending or receiving of any interstate communication by wire shall divulge or publish it or its substance to anyone other than the addressee or his authorized representative or to authorized fellow employes [sic]" means the information cannot be disclosed to law enforcement officers without requisite process because "Congress may have thought it less important that some offenders should go unwhipped of justice than that officers should resort to methods deemed inconsistent with ethical standards and destructive of personal liberty"); *see also* United States v. Warshak, 631 F.3d 266, 286-87 (6th Cir. 2010) (discussing how the phone operators in *Katz* had the ability and right to listen to the relevant phone calls but the *Katz* Court did not take that to mean law enforcement could intercept the communications without a warrant).

187. Pub. L. No. 90-351, tit. III, 82 Stat. 197, 211-25 (1968) (codified as amended at 18 U.S.C. §§ 2510-2522 (2015)).

188. 18 U.S.C. § 2518(1)-(3).

189. *Id.* § 2511(2)(a)(i) (emphasis added).

Courts have followed Congress's lead, finding that "communications systems" have a "fundamental right to take reasonable measures to protect themselves and their properties."[190] For example, in 1967, the Ninth Circuit explained,

> When a subscriber of a telephone system uses the system's facilities in a manner which reasonably justifies the telephone company's belief that he is violating his subscription rights, then he must be deemed to have consented to the company's monitoring of his calls to an extent reasonably necessary for the company's investigation.[191]

Today, the Federal Wiretap Act—an amendment to the Omnibus Crime Control Act that further restricts government wiretaps and other interception of communications data—allows ISPs to access the information on their networks in two relevant situations.[192] First, an ISP can access information in the ordinary course of its business[193] so long as the interception "facilitate[s] the communication service or [i]s incidental to the functioning of the provided communication service."[194] This limited right of access likely does not eliminate a user's reasonable expectation of privacy, as it is far narrower than the type of "sweeping" access the Sixth Circuit speculated about in *Warshak*.[195]

Second, the ISP can access user information with the user's consent.[196] When examining consent, courts look to "whether the parties whose communications were intercepted had adequate notice of the interception. That the person communicating knows that the interceptor has the *capacity* to

190. Bubis v. United States, 384 F.2d 643, 648 (9th Cir. 1967) (interpreting 47 U.S.C. § 605, which prohibits intercepting, divulging, or publishing the contents of conversations held over wire or radio, and holding that a telephone company could monitor phone calls in a limited manner that was "reasonably necessary").

191. *Id.*

192. 18 U.S.C. § 2511(2)(a)(i)-(ii). There are four situations in which an ISP can access information on its network: (1) for purposes related to providing service, (2) pursuant to the Foreign Intelligence Surveillance Act, (3) with a user's consent, and (4) for FCC regulatory purposes. *Id.* This Note only addresses access based on user consent and maintaining and securing the network.

193. The Federal Wiretap Act prohibits the interception of electronic communications through the use of any electronic, mechanical, or other device. *Id.* §§ 2510(4), 2511(1). The definition of "electronic, mechanical, or other device," however, excludes any instrument, equipment, or facility used "in the ordinary course of . . . business." *Id.* § 2510(5)(a)(i).

194. *In re* Google Inc. Gmail Litig., No. 13-MD-02430-LHK, 2013 WL 5423918, at *8 (N.D. Cal. Sept. 26, 2013).

195. United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010) ("[A] subscriber agreement might, in some cases, be sweeping enough to defeat a reasonable expectation of privacy in the contents of an email account . . . .").

196. 18 U.S.C. § 2511(2)(d).

monitor the communication is insufficient to establish implied consent."[197] And at least one court has found that consent can be limited "to the interception of only part of a communication or to the interception of only a subset of . . . communications."[198] In *In re Google Inc.*, Judge Koh looked to Google's terms of service and privacy policy to determine whether Google explicitly told users it would intercept the content of e-mails for the purpose of creating profiles and targeted advertising.[199] Judge Koh found that Google did not receive consent from its users because the terms of service did not specifically state that Google would intercept e-mail content for advertising purposes and because Google stated only that it had the *capacity* to intercept content, not that it *would* intercept the information.[200]

The SCA[201] adds to the protection supplied by the Federal Wiretap Act by allowing providers of ECS and RCS to disclose users' content information only in certain instances, including (1) with the user's consent,[202] (2) "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service,"[203] and (3) "to a law enforcement agency[] if the contents[] were inadvertently obtained by the service provider[] and [] appear to pertain to the commission of a crime."[204]

The SCA and the Federal Wiretap Act both define when providers can access and disclose users' information and limit law enforcement's access to that information. But providers have contractually expanded their access to users' information using their terms of service, creating consequences for users' privacy.

B. The Effect of Terms of Service Agreements

Many courts have held that terms of service affect a user's reasonable expectation of privacy[205] by defining the amount of privacy the user

197. *In re Google Inc.*, 2013 WL 5423918, at *12 (citing Berry v. Funk, 146 F.3d 1003, 1011 (D.C. Cir. 1998)).

198. *Id.* (quoting *In re* Pharmatrak, Inc., 329 F.3d 9, 19 (1st Cir. 2003)).

199. *Id.* at *13.

200. *Id.*

201. *See supra* Part II.A.

202. 18 U.S.C. § 2702(b)(3) (2015).

203. *Id.* § 2702(b)(5).

204. *Id.* § 2702(b)(7).

205. *See, e.g.*, Antman v. Uber Techs., Inc., No. 3:15-CV-01175-LB, 2016 WL 164294, at *3 (N.D. Cal. Jan. 14, 2016) (noting that Comcast, a nonparty subject to a subpoena, used terms of service that may have left the subscriber with a merely minimal expectation of privacy); United States v. DiTomasso, 56 F. Supp. 3d 584, 597 (S.D.N.Y. 2014) ("A reasonable person, having read carefully through the [terms of use] policy, would certainly understand that by using Omegle's chat service, he was running the risk that

footnote continued on next page

relinquishes.[206] For example, in *United States v. Heckenkamp*, the Ninth Circuit found that a college student did not lose his reasonable expectation of privacy in data on his computer when he connected to his university's network.[207] The court conceded that "privacy expectations may be reduced if the user is advised that information transmitted through the network is not confidential and that the systems administrators may monitor communications transmitted by the user."[208] But the university's computer policy stated,

> [I]n general, all computer and electronic files should be free from access by any but the authorized users of those files. Exceptions to this basic principle shall be kept to a minimum and made only where essential to . . . protect the integrity of the University and the rights and property of the state.[209]

The Ninth Circuit determined this only "establish[ed] limited instances in which university administrators may access [the student's] computer in order to protect the university's systems" and thus did not eliminate the student's reasonable expectation of privacy.[210]

Similarly, in *Warshak*, the Sixth Circuit found that the user of an e-mail service maintained his reasonable expectation of privacy in the contents of his e-mail because the terms of service only "indicat[ed] that '[the ISP] *may* access and use individual Subscriber information in the operation of the Service and as necessary to protect the Service.'"[211] However, the Sixth Circuit warned that "a subscriber agreement might, in some cases, be sweeping enough to defeat a

---

another party—including Omegle—might divulge his sensitive information to law enforcement."); McVicker v. King, 266 F.R.D. 92, 96 (W.D. Pa. 2010) (finding that Trib Total Media's privacy policy creates an expectation of privacy for its users because the policy states that users' personally identifiable information will be disclosed only in "very limited situations"); Sony Music Entm't Inc. v. Does 1-40, 326 F. Supp. 2d 556, 566 (S.D.N.Y. 2004) (finding that defendants can have "little expectation of privacy" when the terms of service explain that the provider can disclose information in response to law enforcement requests).

206. This Note assumes that terms of service bind the user regardless of whether the user reads those terms or could negotiate the terms. *See, e.g.*, Darnaa, LLC v. Google, Inc., No. 15-CV-03221-RMW, 2015 WL 7753406, at *2 (N.D. Cal. Dec. 2, 2015) (upholding use of the terms of service despite the fact that the plaintiff did not read the terms); Song Fi, Inc. v. Google Inc., 72 F. Supp. 3d 53, 62-63 (D.D.C. 2014) (upholding use of YouTube's terms of service despite the fact that "Plaintiffs lacked bargaining power").

207. 482 F.3d 1142, 1147 (9th Cir. 2007).

208. *Id.* (citing United States v. Angevine, 281 F.3d 1130, 1134 (10th Cir. 2002); and United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000)).

209. *Id.* (second alteration in original) (quoting UW-Madison Ad Hoc Elec. Data Advisory Comm., Policies and Procedure Governing Access to Electronic Files (1991), https://kb.wisc.edu/itpolicy/page.php?id=59192&no_frill=1).

210. *Id.*

211. United States v. Warshak, 631 F.3d 266, 287 (6th Cir. 2010) (quoting *NuVox Acceptable Use Policy*, WINDSTREAM, http://business.windstream.com/Legal/acceptableUse.htm (last visited Aug. 12, 2010)).

reasonable expectation of privacy in the contents of an email account."[212] As an example, it offered that "if the ISP expresses an intention to 'audit, inspect, and monitor' its subscriber's emails, that might be enough to render an expectation of privacy unreasonable."[213]

The effect on the user's reasonable expectation of privacy may also be *limited* by the terms of service. In 2014, in *Negro v. Superior Court*, a California state appellate court looked at the information that must be divulged under the SCA pursuant to a civil subpoena and determined that production of content by an ISP "can go no farther than the consent [the user] has given."[214] By extension, this conclusion may mean that a cloud storage provider's terms of service agreement can define the precise parameters of what may be disclosed to a third party, including law enforcement.

Given the current state of the law, cloud storage providers have the right and ability to access user information for general network maintenance. And they can use their terms of service to expand their access to and use of that information, likely affecting users' privacy.

C. Examples of Cloud Storage Providers' Terms of Service

Cloud storage providers have recognized the importance of terms of service and given themselves varying levels of access to user information. This Part will examine three cloud storage services—Carbonite, Dropbox, and Google Drive—that use three different approaches when discussing provider access in their terms of service.

Of the three services, Carbonite has the most restrictive policy regarding its access to users' information and thus likely provides the strongest protection of its users' privacy. Carbonite's privacy policy states, "Carbonite *will not view the contents of Your encrypted stored data* . . . without Your consent."[215] The only other time Carbonite says it may relinquish user data is "if such action is necessary to comply with applicable law or to enforce Carbonite's Terms of Service."[216] But nowhere else in its privacy policy does Carbonite say that it will affirmatively use or access the content of user data for any purpose without user consent. And although Carbonite does collect some information, such as location data, folder names, and file extensions, from users for "product optimization" and "to improve [its] Services," the unequivocal

212. *Id.* at 286.

213. *Id.* at 287 (quoting Warshak v. United States, 490 F.3d 455, 472 (6th Cir. 2007)).

214. 179 Cal. Rptr. 3d 215, 234 (Ct. App. 2014).

215. *Carbonite Privacy Policy*, CARBONITE (Sept. 30, 2016), https://www.carbonite.com/en/terms-of-use/privacy (emphasis added).

216. *Id.*

refusal to independently access user content even for maintenance purposes is key for user privacy.[217]

Dropbox takes a slightly different approach in its promises to protect user information. Dropbox's terms of service state,

> When you use our Services, you provide us with things like your files, content, messages, contacts and so on ("Your Stuff"). . . .
>
> . . . These and other features *may require our systems to access, store and scan Your Stuff*. . . .
>
> . . . .
>
> We may review your conduct and content for compliance with these Terms and our Acceptable Use Policy.[218]

These terms make clear that Dropbox *may* access users' information. Dropbox's privacy policy adds, "We may disclose your information to third parties if we determine that such disclosure is reasonably necessary to (a) comply with the law; (b) protect any person from death or serious bodily injury; (c) prevent fraud or abuse of Dropbox or our users; or (d) protect Dropbox's property rights."[219] This part of the policy protects Dropbox should it decide to voluntarily disclose information and gives users an outline of the circumstances under which their data could be disclosed by the provider. The privacy policy continues, "We believe that our users' data should receive the same legal protections regardless of whether it's stored on our services or on their home computer's hard drive."[220] While this belief may not come to fruition because of Dropbox's terms of service, the stated intent deserves praise because it recognizes the importance of user privacy and communicates the company's commitment to maintaining that privacy.

Finally, Google also grants itself automated access to user information but uses more definite language. Google's terms of service state,

> When you upload, submit, store, send or receive content to or through our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify . . .[,] communicate, publish . . .[,] and distribute such content. . . .
>
> *Our automated systems analyze your content* (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, *and when it is stored*.[221]

Google's privacy policy adds,

---

217. *Id.*

218. *Dropbox Terms of Service*, *supra* note 1.

219. *Dropbox Privacy Policy*, *supra* note 2.

220. *Id.*

221. *Google Terms of Service*, *supra* note 28 (emphasis added).

> We will share personal information with companies, organizations or individuals outside of Google if we have a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to:
>
> meet any applicable law, regulation, legal process or enforceable governmental request[;]
>
> enforce applicable Terms of Service, including investigation of potential violations[;]
>
> detect, prevent, or otherwise address fraud, security or technical issues[;]
>
> protect against harm to the rights, property or safety of Google, our users or the public as required or permitted by law.[222]

For customer convenience, Google uses only one privacy policy across a majority of its diverse products, and it has voiced its intent to limit the number of terms of service agreements it uses.[223] But there may be privacy implications caused by the broad nature of the resulting policy. For example, Google may have included some terms, such as a worldwide license, to protect itself from copyright liability (a Google spokesperson has said that it will not rely on this license to use a user's photos without "explicit permission"[224]). But regardless of the intent, Google's terms of service still allow Google broad access to, and use of, users' information. It is unclear whether a court would find that a user retains her reasonable expectation of privacy given her consent to Google's terms.

All three service agreements allow the providers to access users' information to maintain and secure their networks. As noted above, this access is not problematic, as the law has historically recognized this type of provider access without Fourth Amendment implications.[225]

But notice the differences among the terms of service. Carbonite "*will not* view the contents of Your encrypted stored data."[226] Dropbox says it "*may* . . . access, store and scan Your Stuff."[227] And Google says it *does* "analyze your content" using "automated systems" and gives itself further rights, like a

222. *Google Privacy Policy*, *supra* note 7.

223. Alma Whitten, *Updating Our Privacy Policy and Terms of Service*, GOOGLE OFFICIAL BLOG (Jan. 24, 2012), https://googleblog.blogspot.com/2012/01/updating-our-privacy-policies-and-terms.html.

224. Evan Selleck, *Google Clarifies Privacy Issue in New Photos Storage Service's Licensing Language*, IPHONEHACKS (June 3, 2015), http://www.iphonehacks.com/2015/06/google-photos-privacy-issue-licensing.html (discussing Google's response to an article pointing out privacy concerns related to Google's terms of service).

225. *See supra* Part IV.A; *see also* Bubis v. United States, 384 F.2d 643, 648 (9th Cir. 1967) (noting communication systems' "fundamental right to take reasonable measures to protect themselves and their properties against the illegal acts of a trespasser").

226. *Carbonite Privacy Policy*, *supra* note 215 (emphasis added).

227. *Dropbox Terms of Service*, *supra* note 1 (emphasis added).

worldwide license, to use certain data.[228] These differences illustrate the different approaches cloud storage services take to user privacy. And they are purposeful: providers can protect themselves from civil liability in some cases by specifically reserving broad rights to access and use user information.[229]

But as terms of service grant providers more access to a user's information, providers will have more opportunities to "use" the user's information. And with that "use" comes a higher chance that the provider will trigger the third-party doctrine and eliminate the user's Fourth Amendment privacy rights.

V. Possible Solutions to Problems Created by Terms of Service and Privacy Policies

To summarize, the third-party doctrine maintains that a person loses her reasonable expectation of privacy in information voluntarily disclosed to a third party for use in its normal course of business.[230] When it comes to cloud storage services, a provider's terms of service contractually define whether and when the provider may access a user's information and "use" that information in the course of its business, thereby implicating the third-party doctrine. But until the provider has reason under the terms of service to access and use the user's information, and actually does so, the third-party doctrine does not eliminate the user's reasonable expectation of privacy. Only when the provider, pursuant to the terms of service, accesses the user's account and "uses" her information does the provider trigger the third-party doctrine, causing the user to lose her Fourth Amendment privacy rights in her data stored in the cloud.[231] Put another way, the user contractually grants the cloud storage provider access to and use of her information under certain circumstances but retains her reasonable expectation of privacy until those circumstances occur and the provider uses her data. The user's knowledge about whether circumstances have arisen that may allow the provider access to her information should not matter because the user knows of possible use pursuant to the terms of service, meaning only the provider's determination to actually access and use the data triggers the third-party doctrine. Given these privacy implications, the range of access providers grant themselves should cause concern among consumers.

228. *Google Terms of Service*, *supra* note 28.

229. *Cf. In re* Google Inc. Gmail Litig., No. 13-MD-02430-LHK, 2013 WL 5423918, at *13 (N.D. Cal. Sept. 26, 2013) (finding that Google's terms of service and privacy policy were not specific enough to allow Google broad access to users' e-mail content for the purpose of targeted advertising).

230. *See supra* Part II.B.1.

231. *See supra* Part III.B.

First, this Part will illustrate how current terms of service agreements can compromise user privacy. Second, it will make suggestions for how cloud storage providers can change their terms of service in order to maintain privacy for users while also enabling access to protect the providers' networks.

A. The Problem with Current Third-Party Doctrine Implications for the Cloud: An Example

The problem with the third-party doctrine as it applies to the cloud lies in the vast scope, minimal standard, and nonexistent notice promised by cloud storage providers' terms of service. For example, suppose Dropbox's automated scanning reveals that a user, Bob, has stored a copyright-infringing work in his account. Bob has two folders in his account: "Movies 1" and "Movies 2." The scanning software indicates there may be copyrighted material in "Movies 1," so a Dropbox employee investigates for a violation of the terms of service but finds nothing. Then the employee looks at the other folders in Bob's account and notices the folder called "Movies 2." Thinking the illegal works may be there, the employee looks in "Movies 2" and finds personal, legal, sexually explicit videos but no material that violates Dropbox's terms of service. The employee closes the investigation of Bob's account, and Bob is never notified of the access.

Simultaneously, and unbeknownst to Dropbox, law enforcement has been investigating a number of people for copyright infringement and distributing pirated movies. Although the officers do not have probable cause for a warrant, they suspect Bob may be involved and may be using Dropbox to store the infringing works. Dropbox could not voluntarily turn over Bob's information to law enforcement because it does not fall into any of the categories for voluntary disclosure listed in the privacy policy.[232] But law enforcement could still try to ascertain the information in Bob's account from Dropbox in two ways.

First, law enforcement could subpoena a list of all users Dropbox investigated for terms of service violations relating to copyright infringement. But the recent Supreme Court holding in *City of Los Angeles v. Patel* can be interpreted as finding that a company has a reasonable expectation of privacy in its business records.[233] Thus, cloud storage services have an argument

232. *Dropbox Privacy Policy*, *supra* note 2 (noting that Dropbox may disclose user information if such disclosure is reasonably necessary to "comply with the law," "protect any person from death or serious bodily injury," "prevent fraud or abuse of Dropbox or [its] users," or "protect Dropbox's property rights").

233. 135 S. Ct. 2443, 2447, 2454 (2015) (striking down a municipal ordinance mandating warrantless access to hotel guest records for law enforcement but framing the issue narrowly as a special needs and administrative search case where the hotel owners were not given the opportunity to seek precompliance review of a subpoena).

against turning over a broad swath of internal business records about users, and they likely would not have to supply this information pursuant to a mere subpoena.

Second, the government could issue a subpoena to Dropbox asking (1) if Dropbox investigated Bob's account in the past six months, (2) why Dropbox investigated Bob's account, and (3) whether Dropbox viewed any files in Bob's account. This demand likely satisfies the requirements of relevance, reasonable particularity, and reasonable period of time necessary for a valid subpoena[234] and is limited enough to not be considered an unreasonable search of business records that would invoke *Patel*.[235] So Dropbox would likely need to answer that it investigated Bob's account for a violation of the terms of service related to copyright infringement and viewed files within the account.

At this point, Dropbox has accessed ("used") the content in Bob's account in its normal course of business with Bob's consent from the terms of service agreement. This means that the information viewed falls under the third-party doctrine, and thus Bob can no longer claim a reasonable expectation of privacy in that information. The scope of Bob's consent does not come into play because Dropbox's current terms of service only provide an applicable scope if Dropbox proactively gives information to law enforcement; there is no scope specified for provider searches.[236] And the government now knows it has the ability to obtain Bob's information using only a subpoena because Dropbox triggered the third-party doctrine. Therefore, the government may subpoena all information Dropbox accessed during its investigation, and Dropbox must turn over *all* content its employees viewed—including the sexually explicit videos—because Bob no longer has a reasonable expectation of privacy in any of the information Dropbox accessed during its investigation.

B. Better Business Practices to Help Cloud Storage Providers Protect User Data

In light of the ramifications terms of service and privacy policies have on user privacy and the amount of "private" information users store online in today's digitized world, cloud storage providers should use balanced policies that both protect user privacy and maintain the access necessary to ensure a

234. *See In re* Grand Jury Subpoena Duces Tecum Addressed to Provision Salesmen Union, Local 627, 203 F. Supp. 575, 578 (S.D.N.Y. 1961); *see also* FED. R. CRIM. P. 17(c).

235. *Patel*, 135 S. Ct. at 2447.

236. *Compare Dropbox Privacy Policy*, *supra* note 2 ("We may disclose your information to third parties if . . . such disclosure is reasonably necessary to . . . comply with the law . . . ."), *with Dropbox Terms of Service*, *supra* note 1 ("[Our] features may require our systems to access, store and scan Your Stuff. You give us permission to do those things . . . .").

stable and secure network. Doing so not only benefits users but is also in the interest of businesses, as concerns about digital privacy are now a source of mainstream news.[237]

When creating balanced policies, companies should place limits on their abilities to access information. Different processes are necessary for different types of data requests by the government. In order for law enforcement to obtain a search warrant, it must have probable cause.[238] To obtain a subpoena, law enforcement need show only relevance, reasonable particularity, and a reasonable time restriction.[239] But cloud storage services can contractually grant themselves access to users' accounts without explaining the standard they use to determine when and what to investigate. And such access, and the terms of service that govern it, have massive effects on user privacy in relation to law enforcement.

Thus, cloud storage providers can better protect their users' privacy by adding specificity to their terms of service. Specificity is especially necessary in three areas: the standards governing when providers may access user information, the scope of such access, and the notice providers give to users when such access occurs.

First, cloud storage providers' terms of service should include a standard specifying when they may access the content of a user's account for any reason allowed by their terms of service (for example, investigation for a violation of the terms of service).[240] The current system—in which providers can access and use files at the company's discretion and investigate without an applicable standard—creates too great a risk of arbitrary loss of user privacy. The provider's standard for accessing a user's account should require some reasonable level of suspicion. This suspicion could be generated by automated means, such as scanning or hash searches,[241] assuming that these automated means do not themselves affect the user's reasonable expectation of privacy.

---

237. *See, e.g.*, Paul Blake, *WhatsApp Sharing Data with Facebook Raises Alarm for Privacy Advocates*, ABC NEWS (Aug. 29, 2016, 12:37 PM ET), http://abcnews.go.com/Business/Technology/whatsapp-sharing-data-facebook-raises-alarm-privacy-advocates/story?id=41717305 (discussing Facebook's decision to begin collecting data from WhatsApp users); Mark Scott, *Facebook Ordered to Stop Collecting Data on WhatsApp Users in Germany*, N.Y. TIMES (Sept. 27, 2016), http://www.nyti.ms/2dglV4J (reporting on a decision by German regulators ordering Facebook to stop collecting data from WhatsApp users in Germany).

238. *See, e.g.*, Illinois v. Gates, 462 U.S. 213, 226-27, 239 (1983) (discussing the sufficiency of certain evidence to constitute the probable cause necessary for law enforcement to obtain a warrant).

239. *In re Grand Jury Subpoena*, 203 F. Supp. at 578.

240. For the reasons stated above, this excludes automated scanning. *See supra* note 30.

241. *See generally* Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. F. 38, 39 (2006) (defining and discussing hash searches); Michael Mestitz,

footnote continued on next page

This type of suspicion requirement is already in use in certain circumstances. For example, Google's privacy policy states that it will share information with third parties when "access, use, preservation or disclosure of the information is *reasonably necessary*."[242] The same (or a similar) standard should apply for a provider to access user information for investigations. In fact, by implementing a standard for investigative human review, providers may help nudge courts toward acknowledging the difference—in the third-party doctrine analysis—between using sweeping automated access for advertising purposes and using limited human access for investigative purposes. Cloud service providers should make users aware of the standards for access in their terms of service and provide clear examples of how each provider may satisfy its standard. Providers then could be held accountable through FTC enforcement, as their standards would be considered promises to their users.

Critics may argue that companies will be hesitant to adopt a standard that could increase their risk of civil liability and scrutiny from the FTC should a company breach its terms of service. This argument is legitimate and accurately assesses the consequences of implementing such a standard. Thus, consumers must also play a role by looking for services that offer digital privacy. And if businesses are willing to commit to protecting user data[243] and want to market that commitment to consumers, such a standard is a reasonable first step. The provider would be making strides toward defending user privacy while not overburdening itself because it would have discretion over the wording of the applicable standard. This gives providers the opportunity to push toward a legal framework where the "users' data should receive the same legal protections regardless of whether it's stored on [the provider's] services or on [the user's] home computer's hard drive,"[244] and to do it on the providers' own terms. Users, in turn, should—or at least can—make informed decisions when picking a cloud storage service based on the privacy each affords.

A second way providers can protect users is by using the terms of service to limit the scope of information the user consents to allowing the provider to access during its investigations. During an investigation, the terms of service should limit the provider to accessing *only* the files the provider "reasonably

Note, *Unpacking Digital Containers: Extending* Riley*'s Reasoning to Digital Files and Subfolders*, 69 STAN. L. REV. 321, 352-53 (2017) (discussing hash searches).

242. *Google Privacy Policy*, *supra* note 7 (emphasis added).

243. *See, e.g.*, *Dropbox Privacy Policy*, *supra* note 2 ("We believe that our users' data should receive the same legal protections regardless of whether it's stored on our services or on their home computer's hard drive.").

244. *Id.*

suspects"[245] have violated the terms of service. If the files contain content that violates the terms of service, the provider should not access any other files in the user's account and should warn the user of the violation or, depending on the severity, deactivate the user's account. By using the terms of service to limit the scope of the user's consent, the provider limits the elimination of the user's reasonable expectation of privacy to only the files accessed and used during the investigation.[246]

Finally, the provider should notify a user whenever the provider accesses information in the user's account in a manner likely to trigger the third-party doctrine (for example, by human investigation of the account) and finds that the user did not violate the terms of service.[247] Rescission of service or a warning of a terms of service violation should suffice as notice for those who violate the terms of service. Notice will inform the user that information has been accessed by the provider in the provider's normal course of business. Because this requires informing a user of the consequences of a complicated legal doctrine, transparency is key. The provider should explain that the user arguably no longer has a reasonable expectation of privacy in the content it accessed should law enforcement request the user's information. The user can then elect to leave the data on the service or remove the data to protect her privacy. Like the additions of a standard and scope governing provider investigations, the addition of notice could expose the provider to civil liability (for example, for negligent failure to warn) as well as FTC enforcement. But again, as privacy becomes more important to users, providers who desire to compete in the market based on privacy protection should be willing to take those chances.

This also, of course, relies on the assumption that consumers will consider privacy when choosing a cloud storage service. The argument could be made that consumer decisions have traditionally been driven by price and convenience. But again, the digital landscape is changing, and privacy is

245. This Note uses "reasonably suspects" to signify the type of suspicion standard a provider could choose to implement.

246. This analysis assumes that courts would find a difference between robotic scanning and human searching when determining a provider's "use" of user data. If a court were to determine that robotic scanning of the content of a file for purposes like malware detection or advertising invokes the third-party doctrine, then limiting the scope of human investigation would do little to constrain the information available to law enforcement.

247. Privacy advocates have argued that the government should also notify individuals when it has accessed their private communications, as such notice is an important means of ensuring individuals' ability to vindicate their rights. *See EFF to Court: Government Must Inform People that It's Accessing Their Emails, Personal Data*, ELECTRONIC FRONTIER FOUND. (Sept. 2, 2016), https://www.eff.org/press/releases/eff-court-government-must-inform-people-its-accessing-their-emails-personal-data.

becoming a growing concern for consumers.[248] Consumers should weigh privacy heavily when choosing a cloud storage service and look for a provider willing to defend its users' privacy.

Implementing standard, scope, and notice provisions will help companies offer better privacy to their users by preventing inadvertent elimination of users' Fourth Amendment protections and giving users some control over their data privacy. Further, this approach will push companies to compete for business based on the strength of the privacy they offer. Consumers using cloud storage should understand how and when their privacy is protected. When armed with accessible and understandable information, consumers will hopefully opt to give business to providers that best meet their privacy needs.

Conclusion

Cloud storage holds a unique position in the modern digital world. Anyone with Internet access and an e-mail address can open a cloud storage account and store their files—be they private or public, important or inconsequential—in a "secure" location. But the privacy of those data is undermined—legally and out of necessity—by cloud storage providers' terms of service. Providers must balance their interest in offering private storage for users with their interest in limiting their liability and protecting their networks and rights. Providers can and should strike this balance by making small changes to their terms of service that would allow them to monitor and protect their networks while also increasing the scope of user information that remains private and giving users opportunities to make decisions about how much privacy they retain in their data.

248. *See, e.g.*, Natasha Lomas, *UK Report Finds Rising Digital Privacy Concerns*, TECHCRUNCH (Apr. 21, 2016), https://techcrunch.com/2016/04/21/uk-report-finds-rising-digital-privacy-concerns (discussing a British study that found a rise in concerns about digital privacy in the United Kingdom); *see also* Perlroth, *supra* note 182 (discussing a recent data breach that affected approximately 500 million Yahoo users).