2009

Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing

David A. Couillard

Note

Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing

David A. Couillard∗

Internet use has changed over time, expanding beyond text-based forums and e-mails to include images, videos, documents, interactive online applications, online storage, and more.[1] Experts have coined the term "Web 2.0" to describe the shift in Internet usage from consumption to participation[2] and metaphorically refer to this virtual platform as "the cloud," where users interact with Internet applications and store data on distant servers rather than on their own hard drives.[3] Despite the shift in Internet usage, users expect their information

∗ J.D. Candidate 2010, University of Minnesota Law School; B.A. 2006, University of Minnesota. The author thanks Professor William McGeveran and Jennifer Cross for their advice and encouragement. The author also thanks Elizabeth Borer, Dan Ganin, Jeffrey Justman, Allison Lange, and the many other *Minnesota Law Review* editors and staff for their suggestions and guidance throughout the process of writing this Note. Special thanks to the author's parents, Brad and Penny Couillard, and his sister, Melissa, for their constant support, and Eric Gerdts for putting up with impromptu brainstorming sessions.

1. *See, e.g.*, Scott Spanbauer, *New Improved Web: Ready for the Next Online Revolution?*, PC WORLD, Dec. 23, 2005, http://www.pcworld.com/article/123790/new_improved_web.html.

2. *Id. See generally* Tim O'Reilly, *What Is Web 2.0*, O'REILLY NETWORK, Sept. 30, 2005, http://www.oreillynet.com/lpt/a/6228 (explaining what the term "Web 2.0" encompasses).

3. *See, e.g.*, Galen Gruman & Eric Knorr, *What Cloud Computing Really Means*, INFOWORLD, Apr. 7, 2008, http://www.infoworld.com/article/08/04/07/15FE-cloud-computing-reality_1.html (describing the "cloud" metaphor and the various definitions of "cloud computing" which include Internet-based applications and storage services); Erick Schonfeld, *IBM's Blue Cloud Is Web Computing By Another Name*, TECHCRUNCH, Nov. 15, 2007, http://www.techcrunch.com/2007/11/15/ibms-blue-cloud-is-web-computng-by-another-name (giving examples of companies such as Amazon, Google, Yahoo, and IBM using "massive server farms" to support remote online storage and applications).

to be treated the same on this virtual cloud as it would be if it were stored on their own computer, phone, or iPod.[4]

Meanwhile, the Fourth Amendment has also evolved over the past several decades, slowly adapting to various new technologies;[5] but it took the Supreme Court until 1967—nearly a full century after the invention of the telephone—to recognize telephone conversations as constitutionally protected against unreasonable searches.[6] Under a rubric of "reasonable expectations of privacy,"[7] the Court has since defined the contours of the Fourth Amendment's application in varying circumstances.[8] But technology and society's expectations are evolving faster than the law.[9] Although statutory schemes exist, some argue that these laws are outdated.[10] Meanwhile, the Supreme Court has not even addressed the Fourth Amendment's application to e-mail, let alone the expanding uses of cloud-computing platforms. Thus, Fourth Amendment law needs a framework that will adapt more quickly in order to keep pace with evolving technology.

This Note will analyze cloud computing specifically in the context of the Fourth Amendment, notwithstanding related

4. Grant Gross, *Cloud Computing May Draw Government Action*, INFOWORLD, Sept. 12, 2008, http://www.infoworld.com/article/08/09/12/Cloud_computing_may_draw_government_action_1.html (quoting Ari Schwartz, Vice President and Chief Operating Officer of the Center for Democracy and Technology).

5. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 29 (2001) (addressing the use of thermal-imaging devices to "search" a home); Katz v. United States, 389 U.S. 347, 352–53 (1967) (applying Fourth Amendment protections to telephone calls).

6. *Katz*, 389 U.S. at 352–53.

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

8. *See, e.g.*, Bond v. United States, 529 U.S. 334, 338–39 (2000) (holding that the squeezing of a bag to determine its contents invaded a reasonable expectation of privacy and was thus a search in violation of the Fourth Amendment).

9. For example, the Pew Internet and American Life Project recently released the results of a comprehensive survey regarding the use of cloud-computing applications and services which found that forty-nine percent of cloud-computing users in the United States would be "very concerned" if cloud service providers shared their files with law enforcement, while another fifteen percent of respondents said they would be "somewhat concerned." Memorandum from John B. Horrigan, Assoc. Dir., Pew Internet & Am. Life Project 2, 6–7 (Sept. 2008), http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Cloud.Memo.pdf.pdf [hereinafter Horrigan, Cloud Survey].

10. *See, e.g.*, Achal Oza, Note, *Amend the ECPA: Fourth Amendment Protection Erodes as E-mails Get Dusty*, 88 B.U. L. REV. 1043 (2008) (arguing that technology has outpaced the decades-old provisions of the Electronic Communications Privacy Act of 1986).

statutory provisions. Part I will examine the evolution of Fourth Amendment jurisprudence in the last several decades and describe the newly emerging field of cloud computing and the implications of that trend. Part II will describe how courts analogize Fourth Amendment precedent to these new and different cloud-computing concepts and will address whether society is reasonable to expect privacy in things stored on the Internet. In addition, it will look at judicial attempts to treat computer accounts and websites as virtual containers and how methods of virtual concealment have been treated under the law. Finally, Part II will also look at the role of third-party intermediaries in this complex privacy equation. So far, judicial approaches to these issues are unclear and vary by jurisdiction, or the issues have been avoided altogether. Part III will synthesize these concerns and lay out a framework for courts to follow when applying Fourth Amendment law to the cloud.

I. THE FOURTH AMENDMENT AND INFORMATION TECHNOLOGY

The Fourth Amendment provides that the people shall "be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . ."[11] The Amendment states that searches may be conducted with a warrant supported by probable cause,[12] and judicial precedent dictates that a search is "presumptively unreasonable without a warrant."[13] In defining what constitutes a search, however, courts have drawn various lines, which are now subsumed under a reasonable-expectation-of-privacy test.

The reasonable-expectation-of-privacy test arose out of *Katz v. United States*, where Justice Harlan, concurring, outlined a two-part requirement: (1) that the person demonstrated a subjective expectation of privacy over the object and (2) that the expectation was reasonable.[14] This test can be applied to both tangible and intangible objects.[15] However, when the object of a search—tangible or not—is voluntarily turned over to a

11. U.S. CONST. amend. IV.

12. *Id.*

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

14. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *see* Minnesota v. Carter, 525 U.S. 83, 97 (1998) ("[The] *Katz* test . . . has come to mean the test enunciated by Justice Harlan's separate concurrence in *Katz* . . . .").

15. *See Katz*, 389 U.S. at 353 (citing Silverman v. United States, 365 U.S. 505, 511 (1961)).

third party, the Supreme Court has held that a person loses their reasonable expectation of privacy in that object.[16] As these legal doctrines evolved, society adopted new technologies to facilitate the storage and transmission of digital data. An overview of these concurrent evolutions of law and technology provides the necessary background to address the cloud privacy problem.

A. THE FOURTH AMENDMENT AND REASONABLE EXPECTATIONS OF PRIVACY

The reasonable-expectation-of-privacy test that Justice Harlan outlined in *Katz*[17] has been the standard by which courts define what constitutes a search for Fourth Amendment purposes.[18] Courts traditionally treat objects as separate containers and inquire into a person's reasonable expectation of privacy in the contents of those containers.[19] To complicate matters, reasonable expectations of privacy extend beyond tangible objects and may encompass intangibles, such as oral communications.[20] It is important to consider these approaches as a guide for treating the Internet cloud as a searchable object.

1. Tangible Containers and the Reasonable-Expectation-of-Privacy Inquiry

The Fourth Amendment is not limited to the protection of homes;[21] the presumptive requirement of a warrant based on probable cause applies to luggage,[22] briefcases,[23] backpacks,[24]

16. *See, e.g.*, United States v. Miller, 425 U.S. 435, 442–43 (1976) (bank records); Couch v. United States, 409 U.S. 322, 335–36 (1973) (business and tax records).

17. *See Katz*, 389 U.S. at 361 (Harlan, J., concurring).

18. *E.g.*, California v. Ciraolo, 476 U.S. 207, 211 (1986); Renée McDonald Hutchins, *Tied Up in* Knotts*? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 427 (2007) (citing *Kyllo*, 533 U.S. at 32).

19. *See* United States v. Ross, 456 U.S. 798, 811–12 (1982) ("[C]losed packages and containers may not be searched without a warrant.").

20. For example, in some circumstances a person has a reasonable expectation of privacy in the content of their telephone conversations even though the Fourth Amendment does not refer to intangibles. *Katz*, 389 U.S. at 353 (citing *Silverman*, 365 U.S. at 511).

21. The Supreme Court has noted that "the Fourth Amendment protects people, not places." *Id.* at 351.

22. Bond v. United States, 529 U.S. 334, 338–39 (2000) (holding that the physical manipulation of petitioner's bag invaded his expectation of privacy and thus violated the Fourth Amendment).

23. *See* United States v. Freire, 710 F.2d 1515, 1519 (11th Cir. 1983).

purses,[25] opaque bags,[26] and lockers.[27] Aside from certain exceptions to the warrant requirement,[28] containers satisfying the *Katz* test are usually subject to Fourth Amendment protection.[29] Although the Court explicitly refuses to recognize a constitutional distinction between worthy and unworthy containers,[30] courts do inquire into the nature of the container with regard to the reasonable steps taken to conceal its contents. For example, in *Bond v. United States*, the Court reasoned that a bus passenger exhibited a subjective expectation of privacy in his luggage "by using an opaque bag and placing that bag directly above his seat."[31] Furthermore, in applying *Katz*'s second prong, the Court found that society is prepared to recognize a passenger's reasonable expectations of privacy in his bag even if that bag is brought onto a public bus where it might be moved by other passengers or bus employees.[32]

Although some courts recognize that a person exhibits a subjective expectation of privacy by locking a container,[33] the

24. Doe *ex rel.* Doe v. Little Rock Sch. Dist., 380 F.3d 349, 353 (8th Cir. 2004).

25. *Id.*

26. *Bond*, 529 U.S. at 338.

27. *See* Murdock v. State, 664 P.2d 589, 598 (Alaska Ct. App. 1983) ("[The petitioner] had a reasonable expectation of privacy in the property stored [in a rented locker] at the YMCA."); Ferris v. State, 640 S.W.2d 636, 638 (Tex. App. 1982) ("Under proper circumstances, a storage locker is a place entitled to Fourth Amendment . . . protection.").

28. *See, e.g.*, United States v. Robinson, 414 U.S. 218, 235 (1973) ("[I]n the case of a lawful custodial arrest a full search of the person [incident to that arrest] is not only an exception to the warrant requirement of the Fourth Amendment, but is also a 'reasonable' search under that Amendment.").

29. *See, e.g.*, Horton v. California, 496 U.S. 128, 141 n.11 (1990) (stating that the seizure of a container does not compromise the privacy interests in its contents because it still cannot be opened without a search warrant unless one of the exceptions to the warrant requirement applies) (citing Smith v. Ohio, 494 U.S. 541 (1990)).

30. United States v. Ross, 456 U.S. 798, 822 (1982) (noting that for purposes of the Fourth Amendment, "the most frail cottage in the kingdom is absolutely entitled to the same guarantees of privacy as the most majestic mansion," and thus a traveler's toothbrush and clothing carried in a paper bag or scarf should not be treated any differently than a "sophisticated executive" with a locked briefcase (citing Miller v. United States, 357 U.S. 301, 307 (1958))).

31. *Bond*, 529 U.S. at 338.

32. *Id.* at 338–39.

33. *See, e.g.*, United States v. Chadwick, 433 U.S. 1, 11 (1977) (recognizing that an expectation of privacy in a double-locked footlocker is no less reasonable than the expectations of one who locks his house to keep out intruders), *abrogated by* California v. Acevedo, 500 U.S. 565 (1991) (holding that it is con-

Bond Court found the opacity of the container and its close proximity to the passenger sufficient to satisfy the reasonable-expectation-of-privacy test even absent a lock.[34] A reasonable expectation of privacy is evaluated in light of the circumstances and the use of a container to conceal contents;[35] therefore, even an unlocked container may be afforded protection as long as its contents are reasonably concealed.[36]

In addition to considering the means of concealment, courts also take into account the nature of the contents being concealed. In *Doe ex rel. Doe v. Little Rock School District*, the Eighth Circuit considered whether secondary-school students have a reasonable expectation of privacy in the contents of their backpacks and purses.[37] Quoting the Supreme Court, the Eighth Circuit found that schools are "homes away from home" for students, and that schoolchildren bring with them personal items such as keys and money, as well as "highly personal items [such] as photographs, letters, and diaries."[38] The court found that students maintain a reasonable expectation of privacy in their belongings, and they are protected under the Fourth Amendment.[39] Similarly, in *United States v. Freire*, the Eleventh Circuit noted that a briefcase is often used for more

stitutionally permissible for police to search a closed container in a car if probable cause exists); United States v. Kelly, 913 F.2d 261, 265 (6th Cir. 1990) ("[A]bsent exigent circumstances or consent, an officer is not to search a locked suitcase without a search warrant.").

34. *See Bond*, 529 U.S. at 338–39; *see also* United States v. Bosby, 675 F.2d 1174, 1180 (11th Cir. 1982) ("Absent exigent circumstances, closed containers such as a briefcase or pieces of personal luggage even if unlocked cannot be searched absent a warrant.").

35. For this reason, the reasonable-expectation-of-privacy test has been criticized as being too subjective and having "limited predictive value." *E.g.*, James X. Dempsey, *Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology*, *in* 2 NINTH ANNUAL INSTITUTE ON PRIVACY AND SECURITY LAW 543, 552 (2008).

36. Although a person might maintain a reasonable expectation of privacy in an unlocked but closed container, "some containers so betray their contents as to abrogate any such expectation" and "are treated as being in plain view." United States v. Meada, 408 F.3d 14, 23 (1st Cir. 2005) (citations omitted). In *Meada*, the First Circuit held that a container with a "GUN GUARD" label on the outside made it reasonably identifiable as a gun case, rendering the contents unambiguous and destroying the defendant's reasonable expectation of privacy. *Id.*

37. Doe *ex rel.* Doe v. Little Rock Sch. Dist., 380 F.3d 349, 351, 353 (8th Cir. 2004).

38. *Id.* at 353 (quoting New Jersey v. T.L.O., 469 U.S. 325, 339 (1985)).

39. *Id.*

than just business documents.[40] Analogizing a briefcase to a large pocket containing "credit cards, address books, personal calendar/diaries, correspondence, and reading glasses," the court noted that a briefcase commands perhaps one of the most compelling expectations of privacy outside one's home.[41]

Several of these cases also indicate that a person does not necessarily lose his privacy interest in a closed container merely by having it in public or otherwise relinquishing direct control over it. The court in *Freire* concluded that the defendant's privacy interest in the briefcase was not abrogated by his act of entrusting it to his codefendant "for safekeeping."[42] The *Bond* Court held that the defendant retained a privacy interest in his bag even though it was brought on a public bus,[43] and other courts recognize that a person retains a reasonable expectation of privacy in luggage left on premises that are not his own.[44]

Therefore, courts often consider two major factors when applying *Katz* to tangible containers: the concealment efforts of the owner and the private nature of the items being concealed. Furthermore, bringing a closed container into public does not necessarily destroy an otherwise reasonable expectation of privacy. When the container is a sophisticated computer or the contents are intangible, however, the same factors may be relevant but applied in different ways.

2. Privacy in Intangibles and Computers as Containers

Although the reasonable-expectation-of-privacy analysis governs how courts generally define searches of containers under the Fourth Amendment, *Katz* also stood for another important principle of Fourth Amendment jurisprudence: that "the Fourth Amendment protects people, not places."[45] Although the Fourth Amendment refers only to "persons, houses, papers, and

40. United States v. Freire, 710 F.2d 1515, 1519 (11th Cir. 1983). The briefcase in *Freire* was unlocked as well. *Id.* at 1518.

41. *Id.* at 1519.

42. *Id.*

43. Bond v. United States, 529 U.S. 334, 338–39 (2000).

44. *See, e.g.*, United States v. Owens, 782 F.2d 146, 150 (10th Cir. 1986) (holding that luggage left in a motel room retains Fourth Amendment protection even if the checkout time has passed and the motel had a legal right to forcibly evict the hold-over guest).

45. Katz v. United States, 389 U.S. 347, 351 (1967).

effects,"[46] *Katz* extended protection to privacy interests in intangible communications.[47]

In *Katz*, the defendant appealed his conviction for violating a federal statute by communicating wagering information via telephone across state lines.[48] At trial, and over the defendant's objections, surreptitiously recorded tapes of his telephone conversation were introduced into evidence.[49] The Supreme Court reversed the conviction.[50] In so doing, the Court recognized the "vital role that the public telephone has come to play in private communication," and reasoned that even in a glass telephone booth, the defendant retained a privacy right in the content of his conversation.[51] The Court recognized that recent precedent broadened the view of the Fourth Amendment so that it "governs not only the seizure of tangible items, but extends as well to the recording of oral statements, overheard without any 'technical trespass under . . . local property law.'"[52]

The issue of intangible digital data creates a similar need for Fourth Amendment analogies. Although computers are more technologically complex than briefcases or even perhaps telephone calls, courts have held that computer searches are limited by the Fourth Amendment.[53] But the act of searching a computer has practical differences from searching tangible containers. In *United States v. Crist*, a federal district court in Pennsylvania held that, by removing the hard drive from a computer and creating a duplicate image of the digitized data stored on it, the government had performed a "search" under the Fourth Amendment, despite the lack of any physical inva-

46. U.S. CONST. amend. IV.

47. *Katz*, 389 U.S. at 353 (citing Silverman v. United States, 365 U.S. 505, 511 (1961)).

48. *Id.* at 348.

49. *Id.*

50. *Id.* at 359.

51. *Id.* at 352.

52. *Id.* at 353 (quoting *Silverman*, 365 U.S. at 511).

53. For example, in *Maes v. Folberg*, 504 F. Supp. 2d 339, 347 (N.D. Ill. 2007), an Illinois federal district court found that the plaintiff, a state employee, had a reasonable expectation of privacy in her government-issued laptop computer because there was no evidence that the plaintiff was on notice that her laptop was subject to search. The court relied upon *O'Connor v. Ortega*, which held that government employees are protected from unreasonable searches by their government employers. *Maes*, 504 F. Supp. 2d at 347–48 (citing O'Connor v. Ortega, 480 U.S. 709, 715–16, 725–26 (1987)); *cf.* Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002) (holding that plaintiff's privacy expectation was destroyed because his government employer "announced that it could inspect the laptops that it furnished for the use of its employees").

sion.[54] The court reasoned that "[b]y subjecting the entire computer to a hash value analysis[,] every file, internet history, picture, and 'buddy list' became available for Government review."[55] Furthermore, the court argued that a hard drive is not analogous to a single container, but is "comprised of many platters, or magnetic data storage units, mounted together."[56] The court reasoned that each platter of the hard drive should be considered a separate container.[57]

Under *Katz* and its progeny, a search has been performed and the Fourth Amendment is implicated when a reasonable expectation of privacy has been violated.[58] As the discussion above shows, two of the major factors courts consider in this analysis are concealment efforts and the private nature of the concealed effects.[59] Furthermore, taking a closed container out in public does not necessarily change the equation.[60] Although this standard is applied to both tangible and intangible personal effects,[61] a computer's internal structure and partitioning of data blurs the line between the tangible and intangible. Yet, as *Katz* itself demonstrates, courts may be willing to recognize vital roles of new technology, and adapt the Fourth Amendment to fit evolving societal expectations.[62]

B. THE THIRD-PARTY DOCTRINE

The *Katz* decision included the caveat that a person assumes the risk that a third party, such as the person on the other end of the telephone line, will report the contents of a

54. United States v. Crist, No. 1:07-cr-211, 2008 WL 4682806, at *9 (M.D. Pa. Oct. 22, 2008).

55. *Id. But see* Posting of Orin Kerr to The Volokh Conspiracy, http://volokh.com/posts/1225159904.shtml (Oct. 27, 2008, 22:11) ("[T]he Government failed to make the strongest argument that running the hash isn't a search: If the hash is for a known image of child pornography, then running a hash is a direct analog to a drug-sniffing dog in *Illinois v. Caballes*, 543 U.S. 405 (2005).").

56. *Crist*, 2008 WL 4682806, at *10.

57. *Id.*

58. Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring); *see also, e.g.*, Bond v. United States, 529 U.S. 334, 338–39 (2000); Doe *ex rel.* Doe v. Little Rock Sch. Dist., 380 F.3d 349, 353 (8th Cir. 2004).

59. *See, e.g.*, *Bond*, 529 U.S. at 338–39; *Little Rock Sch. Dist.*, 380 F.3d at 353 (citing New Jersey v. T.L.O. 469 U.S. 325, 339 (1985)).

60. *See Bond*, 529 U.S. at 338–39.

61. *See supra* note 20 and accompanying text.

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

conversation to the police.[63] By assuming that risk, Katz lost his expectation of privacy vis-à-vis the other party to the conversation.[64] Similarly, current law holds that transactional materials such as tax records, bank records, and the numbers dialed into a telephone retain no reasonable expectation of privacy vis-à-vis the third-party intermediary to whom they were voluntarily turned over.[65] The intermediary is considered a party to certain transactional aspects of the communication, and police may use that third party to obtain the information without a warrant.[66]

The Court has applied the third-party doctrine to transactional data on the grounds that an individual turns the data over to an intermediary with the knowledge that they will not remain completely private.[67] Transactional data, the Court argues, are a part of the intermediary's business records; rather than merely holding the documents as a neutral third party, the intermediary is in fact an interested party to the transaction.[68]

Electronic transactions further complicate these third-party relationships. In *Smith v. Maryland*, the Supreme Court held that the use of a pen register to record the numbers dialed from the defendant's home telephone did not constitute a search.[69] The Court noted that a pen register does not reveal who was on either end of the line or whether the call was even completed.[70] Callers convey dialed numbers to the telephone

63. *See, e.g.*, *id.* at 363 n.* (White, J., concurring) ("When one man speaks to another he takes all the risks ordinarily inherent in so doing, including the risk that the man to whom he speaks will make public what he has heard. The Fourth Amendment does not protect against unreliable (or law-abiding) associates." (citing Hoffa v. United States, 385 U.S. 293, 303 (1966))).

64. *See id.*

65. *See, e.g.*, Smith v. Maryland, 442 U.S. 735 (1979) (dialed telephone numbers); United States v. Miller, 425 U.S. 435 (1976) (bank records); Couch v. United States, 409 U.S. 322 (1973) (business and tax records); *see also* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009) [hereinafter Kerr, *Third-Party Doctrine*] (explaining that the "third-party doctrine" precludes an individual from claiming Fourth Amendment protection for information that was voluntarily revealed).

66. *See, e.g.*, sources cited *supra* note 65.

67. *See, e.g.*, *Couch*, 409 U.S. at 335.

68. *See Miller*, 425 U.S. at 440–41 (citing Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 48–49, 52 (1974)).

69. *Smith*, 442 U.S. at 745–46.

70. *Id.* at 741 (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 167 (1977)) (noting that a pen register does not hear sound, but merely discloses what numbers have been dialed).

company in order to complete a call, and are aware that the phone company keeps records of those numbers.[71] The Court noted that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[72] This doctrine has been characterized as either the waiver of a reasonable expectation of privacy or an implied consent to search.[73]

Thus, while communication contents may be protected under the Fourth Amendment, transactional information does not retain such protection vis-à-vis a third-party intermediary such as an accountant, bank, or telephone company.[74] This doctrine is particularly relevant in the cloud-computing world, where information is turned over to cloud service providers for remote storage and other quasi-transactional purposes with increasing frequency.[75] Because the widespread use of remote storage is such a new phenomenon, few cases have fully addressed the issue.

C. THE DIGITAL CLOUD AS A MODERN COMMUNICATIONS AND STORAGE MEDIUM, AND ITS TREATMENT BY THE COURTS

As courts have untangled and retangled these Fourth Amendment interpretations and doctrines, the Internet and the way it is used has changed. The last few years have seen a shift in usage from consumption to participation, and users now interact with applications and store data remotely rather than on their own computers.[76] This new Internet platform, spurred by advancements in networking technologies, has been called "Web 2.0."[77] A central aspect of this shift is the ability to "outsource storage" to service providers like Google rather than saving things such as e-mails, photos, calendars, or other documents on a personal hard drive.[78]

71. *Id.* at 742.

72. *Id.* at 743–44 (citing *Miller*, 425 U.S. at 442–44).

73. *See* Kerr, *Third-Party Doctrine*, *supra* note 65, at 588. Under the consent-based formulation, reasonable expectations of privacy are irrelevant when applying the third-party doctrine. *Id.*

74. *See, e.g.*, sources cited *supra* note 65.

75. *See, e.g.*, Spanbauer, *supra* note 1.

76. *See, e.g.*, *id.*

77. *See, e.g.*, Randal C. Picker, *Competition and Privacy in Web 2.0 and the Cloud*, 103 NW. U. L. REV. 1, 2 (2008). *See generally* O'Reilly, *supra* note 2 (explaining what the term "Web 2.0" encompasses).

78. *See* Picker, *supra* note 77, at 2–3.

The term "cloud computing" is based on the industry usage of a cloud as a metaphor for the ethereal Internet.[79] A cloud platform can either be external or internal.[80] An external cloud platform is storage or software access that is essentially rented from (or outsourced to) a remote public cloud service provider, such as Amazon or Google.[81] This software-as-a-service allows individuals and businesses to collaborate on documents, spreadsheets, and more, even when the collaborators are in remote locations.[82] By contrast, an internal or private cloud is a cluster of servers that is networked behind an individual or company's own firewall.[83]

Cloud platforms give users "anywhere access" to applications and data stored on the Internet.[84] Various companies are unveiling such platforms, allowing users to store backups of important files and access them from anywhere the Internet is available.[85] Recent reports indicate that Google plans to launch a new cloud platform that "could kill off the desktop computer."[86] Although not without its critics,[87] cloud computing is considered a "fast-growing and potentially enormous new market."[88]

79. *See, e.g.*, Gruman & Knorr, *supra* note 3.

80. *See* Marty Foltyn, *The Cloud Offers Promise for Storage Users*, ENTERPRISE STORAGE F., Dec. 10, 2008, http://www.enterprisestorageforum.com/ipstorage/features/article.php/3790381.

81. *See id.* Microsoft recently announced its own cloud platform called Azure. Benjamin J. Romano, *New Computing Strategy Sends Microsoft to Clouds*, SEATTLE TIMES, Oct. 28, 2008, at A10.

82. *See, e.g.*, Google Docs Tour, Share and Collaborate in Real Time, http://www.google.com/google-d-s/tour2.html (last visited Apr. 17, 2009) (describing the collaborative capabilities of Google Docs).

83. *See* Foltyn, *supra* note 80.

84. *See* Romano, *supra* note 81.

85. *See, e.g.*, Mike Masnick, *Rackspace Wants to Take On Amazon's Cloud Computing Efforts*, TECHDIRT, Oct. 22, 2008, http://techdirt.com/articles/20081022/1344222618.shtml.

86. David Smith, *Google Plans to Make PCs History*, GUARDIAN, Jan. 25, 2009, http://www.guardian.co.uk/technology/2009/jan/25/google-drive-gdrive-internet. Dave Armstrong, the head of product and marketing for Google Enterprise, is quoted as saying, "There's a clear direction . . . away from people thinking, 'This is my PC, this is my hard drive,' to 'This is how I interact with information, this is how I interact with the web.'". *Id.*

87. *See, e.g.*, Bobbie Johnson, *Cloud Computing Is a Trap, Warns GNU Founder Richard Stallman*, GUARDIAN, Sept. 29, 2008, http://www.guardian.co.uk/technology/2008/sep/29/cloud.computing.richard.stallman.

88. *See* Romano, *supra* note 81. Microsoft, for example, has spent billions of dollars to implement its new Azure platform. *Id.*

Because these remotely stored data are not intended for public access, they are generally protected by unlisted links, password protection, or encryption.[89] An unlisted link, like an unlisted telephone number, does not technically block access; it merely makes the web link inaccessible through regular search results, instead requiring one to actually know the web address.[90] For security, an authentication key consisting of a random string of characters is embedded within the link, making the web address difficult to guess.[91]

Businesses that use cloud-computing services must balance the financial benefits of outsourcing storage and services to the cloud against the costs of data security.[92] Security experts advise that whenever data are moved into the cloud, encryption and key management are the best security practices.[93] Encryption, based on the science of cryptography, is the process of encoding information such that a key is required to decode it.[94] Some encryption products available to consumers are so powerful that law enforcement cannot crack them even with supercomputer technology.[95] As demand for data security increases, encryption methods are improving even further.[96]

89. *E.g.*, Google Video Help, What Are "Unlisted" Videos?, http://video.google.com/support/bin/answer.py?hl=en&answer=48320 (last visited Apr. 17, 2009) [hereinafter Google Video Privacy] (explaining the Google Video "unlisted" option); *see also* Jonathan Strickland, *How Cloud Storage Works*, HOWSTUFFWORKS, http://communication.howstuffworks.com/cloud-storage3.htm (last visited Apr. 17, 2009).

90. Posting of Philipp Lenssen to Google Blogoscoped, http://blogoscoped.com/archive/2006-10-07-n43.html (Oct. 7, 2006).

91. *See, e.g.*, Google Video Privacy, *supra* note 89; Lenssen, *supra* note 90 (explaining that an "unlisted" address, while not password protected, contains meta data allowing it to be shared with friends but preventing it from being listed in search results); Picasa & Picasa Web Albums Help, Album Privacy: Authorization Key, http://picasa.google.com/support/bin/answer.py?hl=en&answer=48446 [hereinafter Picasa Album Privacy] (last visited Apr. 17, 2009) (explaining that unlisted photo albums contain an authorization key in the web address consisting of a letter and number combination, making it "very difficult to guess").

92. Warwick Ashford, *Cloud Computing Presents a Top Security Challenge*, COMPUTERWEEKLY, Dec. 10, 2008, http://www.computerweekly.com/Articles/2008/12/10/233839/cloud-computing-presents-a-top-security-challenge.htm.

93. Foltyn, *supra* note 80.

94. *See, e.g.*, SIMON SINGH, THE CODE BOOK: THE SCIENCE OF SECRECY FROM ANCIENT EGYPT TO QUANTUM CRYPTOGRAPHY 6, 11 (1999).

95. *E.g.*, Dan Froomkin & Amy Branson, *Deciphering Encryption*, WASH. POST, May 8, 1998, http://www.washingtonpost.com/wp-srv/politics/special/encryption/encryption.htm. This has led to law enforcement complaints that encryption is a roadblock to detecting terrorist plots or investigating criminals.

Although server-side e-mail storage was one of the earliest iterations of what is now considered cloud computing,[97] the Supreme Court has yet to decide how e-mails and other data stored online will be treated under Fourth Amendment doctrine, and only a few lower courts have addressed the issue. A recent case out of the Ninth Circuit, *Quon v. Arch Wireless Operating Co.*, held that government employees have an expectation of privacy in the content of their text messages.[98] The court found "no meaningful distinction" between e-mails, text messages, and letters.[99] Thus, the government employer could not search those contents without violating the Fourth Amendment.[100]

In *United States v. D'Andrea*, an anonymous caller informed police of child pornography on the defendants' password-protected website and provided the website's username and password.[101] The federal district court analogized the website to a closed container;[102] however, the court did not define what would constitute a sufficient effort to conceal such a virtual closed container because a private party had already invaded the website and the subsequent warrantless search did not exceed the scope of that private search.[103]

Many aspects of people's private lives are being uploaded into the cloud for storage and access purposes, but Fourth Amendment law has been slow to address this phenomenon. Despite *Quon*'s broad language regarding e-mails, the holding was specific to text messages, leaving the fate of e-mails and other cloud storage data unclear.[104] Similarly, *D'Andrea* has limited predictive value because the court made no effort to ex-

Id.

96. For example, recently unveiled quantum encryption offers security using the "inherently unbreakable" laws of quantum theory. Roland Pease, *'Unbreakable' Encryption Unveiled*, BBC NEWS, Oct. 9, 2008, http://news.bbc.co.uk/2/hi/science/nature/7661311.stm.

97. *See, e.g.*, Paul Festa, *Google to Offer Gigabyte of Free E-mail*, CNET NEWS, Apr. 1, 2004, http://news.cnet.com/Google-to-offer-gigabyte-of-free-email/2100-1032_3-5182805.html.

98. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 905–06 (9th Cir. 2008).

99. *Id.* at 905.

100. *Id.* at 910.

101. United States v. D'Andrea, 497 F. Supp. 2d 117, 118 (D. Mass. 2007).

102. *Id.* at 122 n.16.

103. *Id.* at 122–23.

104. *See Quon*, 529 F.3d at 910.

plore the virtual-container theory in detail.[105] Thus, the application of the Fourth Amendment to law-enforcement searches of the cloud remains murky.

II. LEGAL MURKINESS IN THE CLOUD: A BREAKDOWN OF ANALOGIES

Courts often address new technologies by analogizing to older technologies, in the same way novel legal theories generally find their proper footing by analogy to precedent.[106] Even so, there is relatively little guidance from the courts as to how the Fourth Amendment will apply to data stored in the cloud. While some jurisdictions protect certain narrowly defined online content in a piecemeal fashion,[107] others protect more broadly the virtual container in which that content resides.[108] The *Katz* requirements—society's reasonable expectations paired with a defendant's subjective expectations, as demonstrated by reasonable efforts to conceal[109]—have not been adapted for the new cloud-computing environment. The third-party doctrine and judicial attempts to distinguish between content and transactional data in the cloud complicate the matter even further.

A. SOCIETY'S PREPAREDNESS TO RECOGNIZE THAT IT IS REASONABLE TO EXPECT PRIVACY IN THE CLOUD

The types of data stored and transmitted in the cloud are as varied as tangible objects carried in physical containers. Modern Internet users enjoy access to digital calendars,[110] pho-

105. In a footnote, the court assumed without discussion that a website or computer file is analogous to a physical container. *D'Andrea*, 497 F. Supp. 2d at 122 n.16.

106. *See, e.g.*, *Quon*, 529 F.3d at 905 (finding "no meaningful difference" between e-mails, text messages, and letters); Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1586 (2004) ("E-mail and other electronic files are modern-day papers." (citing ACLU v. Reno, 929 F. Supp. 824, 834 (E.D. Pa. 1996))).

107. *See, e.g.*, *Quon*, 529 F.3d at 910.

108. *See, e.g.*, *D'Andrea*, 497 F. Supp. 2d at 122.

109. Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).

110. *E.g.*, Welcome to Google Calendar, http://www.google.com/googlecalendar/overview.html (last visited Apr. 17, 2009); Windows Live Calendar Beta, http://www.windowslive-hotmail.com/calendar/default.aspx?page=default&locale=en-US (last visited Apr. 17, 2009).

tographs,[111] address books,[112] correspondence in the form of e-mail messages,[113] and diaries in the form of personal blogs.[114] Such a list of items may sound familiar—it includes the same materials deemed "highly personal" by the Supreme Court,[115] a sentiment later echoed by the Eighth Circuit to justify Fourth Amendment protection for schoolchildren despite their otherwise diminished expectations of privacy.[116] It also mirrors the list of materials that the Eleventh Circuit used as a basis for asserting that "[f]ew places outside one's home justify a greater expectation of privacy than does the briefcase."[117] The fact that such items are digital rather than physical should not change their status as highly personal objects; after all, the Supreme Court recognized in *Katz* that intangibles are covered by the Fourth Amendment,[118] and courts have found digital files to be similarly covered.[119]

Although telephone conversations are fleeting, digital files are more persistent; however, the cases that have afforded digital files Fourth Amendment protection have generally involved files stored locally on a hard drive.[120] Should cloud computing change that equation? If backpacks serve as "homes away from home" for schoolchildren,[121] and briefcases serve the same function for working adults,[122] then is it not reasonable to consider a digital account containing the same types of materials, stored

111. *E.g.*, About Flickr, http://www.flickr.com/about (last visited Apr. 17, 2009); Getting Started with Picasa, http://picasa.google.com/support/bin/answer.py?answer=93183 (last visited Apr. 17, 2009).

112. *E.g.*, Yahoo! Address Book, http://address.yahoo.com (last visited Apr. 17, 2009).

113. *See, e.g.*, Gmail, 10 Reasons to Use Gmail, http://mail.google.com/mail/help/about.html (last visited Apr. 17, 2009).

114. *E.g.*, Blogger: About Us, The Story of Blogger, http://www.blogger.com/about (last visited Apr. 17, 2009); WordPress.Org, About WordPress, http://wordpress.org/about (last visited Apr. 17, 2009).

115. New Jersey v. T.L.O., 469 U.S. 325, 339 (1985).

116. Doe *ex rel.* Doe v. Little Rock Sch. Dist., 380 F.3d 349, 353 (8th Cir. 2004) (citing *T.L.O.*, 469 U.S. at 339).

117. United States v. Freire, 710 F.2d 1515, 1519 (11th Cir. 1983).

118. Katz v. United States, 389 U.S. 347, 353 (1967) (citing Silverman v. United States, 365 U.S. 505, 511 (1961)).

119. *E.g.*, United States v. Crist, No. 1:07-cr-211, 2008 WL 4682806, at *9 (M.D. Pa. Oct. 22, 2008).

120. *See, e.g.*, Trulock v. Freeh, 275 F.3d 391 (4th Cir. 2001); *Crist*, 2008 WL 4682806.

121. *Little Rock Sch. Dist.*, 380 F.3d at 353.

122. *Freire*, 710 F.2d at 1519.

in the cloud rather than on a computer hard drive, as serving that purpose as well?

Such an analogy is not so simple. Blogs and digital photo albums are often intentionally made public and placed on the Internet with the desire for others to access them, and with full knowledge of that public accessibility. The press routinely reports on what is being discussed in the "blogosphere."[123] At least one court has declared it "obvious that a claim to privacy is unavailable to someone who places information on an *indisputably, public medium*, such as the Internet, *without taking any measures to protect the information*."[124] The Internet is, after all, a mass-communications medium—a presumptively public space—while a briefcase or backpack is presumptively a private space. Under this presumption, it would seem unreasonable for one to place a diary, photo album, or other document online for any reason other than making it public.

But this no longer holds true in all instances as, for example, many blog-hosting sites have options for making blogs private.[125] Further, as connection speeds and broadband penetration increase across consumer markets, users are better able to upload content and interact with data in the Web 2.0 environment.[126] Wireless Internet and mobile-device networks allow people to access the cloud in far more places.[127] Increased speed

123. *E.g.*, Anahad O'Connor, *From Public and Blogosphere, Shock*, N.Y. TIMES, Mar. 10, 2008, http://www.nytimes.com/2008/03/10/nyregion/10cndcomments.html?_r=1.

124. United States v. Gines-Perez, 214 F. Supp. 2d 205, 225 (D.P.R. 2002), *vacated on other grounds*, 90 Fed. App'x 3 (1st Cir. 2004) (first emphasis added).

125. *See, e.g.*, Blogger Help, How Do I Control Who Can View My Blog?, http://help.blogger.com/bin/answer.py?hl=en&answer=42673 (last visited Apr. 17, 2009) (explaining that a blog hosted by Google's Blogger is "completely public" by default, but can be made private by restricting access to only those users with accounts approved by the blog creator); WordPress.com, Private Blogs, http://en.blog.wordpress.com/2006/08/04/private-blogs (last visited Apr. 17, 2009) (announcing new options for WordPress bloggers to make a private blog unlisted and limit access to only those with permission, in order to protect "more sensitive or private topics").

126. *See* Press Release, Scarborough Research, The Need for Internet Speed: Broadband Penetration Increased More than 300% Since 2002 (Apr. 15, 2008), [hereinafter Scarborough Research, Broadband Penetration Increased], *available at* http://www.reuters.com/article/pressRelease/idUS183986+15-Apr-2008+PRN20080415 (reporting an increase in adults with household broadband connections from twelve percent in 2002 to forty-nine percent in 2008, allowing users to "upload, download, post and interact with content in a Web 2.0 environment").

127. *See, e.g.*, Eric Benderoff, *This Year, Web Grew More Mobile than Ev-*

and efficiency make it more practical to store information in the cloud for purposes of easy access rather than just to make that content public.[128] Consequently, "anywhere access" has become a popular phrase associated with Web 2.0 and cloud-computing services.[129]

Because cloud computing is such a new phenomenon, court attention in this area has focused on e-mails rather than, for instance, photo albums and private blogs. The Ninth Circuit in *Quon* found "no meaningful distinction" between e-mails, letters, and text messages.[130] The court was dealing with text messages rather than e-mails, but agreed that a user maintains a reasonable expectation of privacy in the contents of a text message precisely because it is analogous to an e-mail or a letter.[131] Thus, the Ninth Circuit implicitly recognized that the same expectation of privacy covers e-mails, and the fact that e-mails are conveyed and stored on a public medium such as the Internet does not appear to affect that conclusion.

So far, the Ninth Circuit is the only circuit to have ruled on the issue of reasonable expectations of privacy in e-mail communications.[132] However, the *Quon* decision is lacking in certain areas, and due to the narrowness of its holding, it leaves certain questions unanswered. Although the court implied that the contents of an e-mail are protected, it did not decide whether there is a reasonable expectation of privacy in the inbox itself.[133] Such a narrow holding is equivalent to finding that a person has an expectation of privacy in the contents of a letter, but failing to address whether a similar expectation of privacy

er..., CHI. TRIB., Dec. 25, 2008, at 39 ("[Two thousand eight] was a year that saw the Web grow more critical as a mobile platform.").

128. Evidence suggests that users value the convenience and anywhere-access attributes of cloud computing even more than the ability to share files with others. Horrigan, Cloud Survey, *supra* note 9, at 5.

129. *See, e.g.*, Romano, *supra* note 81.

130. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 905 (9th Cir. 2008).

131. *Id.* at 905–06. Service providers can archive text-message content on their own servers in much the same way that e-mails are stored in the cloud. *See id.* at 895–96. *But see* Marcus R. Jones & Hugh H. Makes, *Traps in Electronic Communications*, 8 J. BUS. & SEC. L. 157, 162 (2008) (explaining that in most cases text messages are stored on the user's phone).

132. The Sixth Circuit actually made a similar ruling in 2007, but that opinion was later vacated. The court held that the issue of whether the government should be enjoined from conducting future ex parte searches was not ripe for adjudication. Warshak v. United States, 490 F.3d 455 (6th Cir. 2007), *vacated* 532 F.3d 521 (6th Cir. 2008).

133. *See Quon*, 529 F.3d 892.

could be found in the closed container in which the letter is placed. Although this holding is obviously positive for privacy advocates in the short term, in the long term it is too narrow to encompass the broader issue of cloud computing, which deals with far more types of content than e-mail.

The cloud is now used to store many of the same materials as a briefcase or backpack. Cloud computing has added an "anywhere-access" function to Internet usage which provides a reasonable justification for storing private materials in the cloud.[134] This "new" Internet is one in which society, at least in some instances, might be prepared to recognize a reasonable privacy interest.[135] However, the Internet remains in many ways a public medium, albeit with an increasing number of private corners. Bringing an object into public does not necessarily destroy reasonable expectations of privacy,[136] but more than mere intent to keep something private is required. Simply placing a personal photo album online and claiming to do so for purposes of private anywhere access will no more justify a reasonable expectation of privacy than would leaving a physical photo album on a park bench. Reasonable concealment efforts must also be present.[137]

B. VIRTUAL CONCEALMENT: INDIVIDUALS' SUBJECTIVELY REASONABLE PRIVACY EXPECTATIONS

A virtual container, like a physical one, does not receive Fourth Amendment protection merely because it contains objects deemed private. There must be some kind of privacy barrier between the contents and the public. An analysis of a person's reasonable efforts to conceal data online will have obvious practical differences from concealment of physical objects. An e-mail inbox or document storage account is not protected by opacity or physical locks. Digital data are instead concealed in the "invisible web"[138] behind unlisted links, password protection, and encryption.

134. *See, e.g.*, Romano, *supra* note 81.

135. *See, e.g.*, Horrigan, Cloud Survey, *supra* note 9, at 6–7 (finding that sixty-four percent of cloud-computing users in the United States would be either "somewhat" or "very" concerned if the service provider shared their files with law enforcement).

136. *See, e.g.*, Bond v. United States, 529 U.S. 334, 338–39 (2000).

137. *See, e.g.*, United States v. Meada, 408 F.3d 14, 23 (1st Cir. 2005).

138. *See generally* Alex Wright, *Exploring a 'Deep Web' That Google Can't Grasp*, N.Y. TIMES, Feb. 23, 2009, at B1 (describing material stored online that is invisible to common search engine methods); UC Berkeley Library, Invisible

Courts have implicitly recognized the existence of virtual containers in circumstances outside the cloud context. One court has held that running a hash—a method used to digitally "fingerprint" files on a computer and compare them to other known files—is the equivalent of a "search" for Fourth Amendment purposes.[139] In so deciding, the court recognized that a computer hard drive is composed of multiple "containers" which should be treated separately.[140]

In other contexts, courts have found that separate password-protected accounts or files on a computer should be recognized as separate areas for certain purposes.[141] When a computer is jointly used but each user has a separate password-protected account, courts have concluded that one user cannot consent to a search of the other user's account.[142] Courts essentially treat each file or account as a different container, dividing the computer into separate compartments for purposes of constitutional analysis, despite the fact that the wall dividing those compartments is virtual rather than physical.[143]

In *United States v. D'Andrea*, the court analogized a website to a "file cabinet or other physical container[] in which

or Deep Web: What It Is, Why It Exists, How to Find It, and Its Inherent Ambiguity, http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/InvisibleWeb.html (last visited Apr. 17, 2009) [hereinafter Invisible Web] ("The 'invisible web' is what you cannot find using [search engines and subject directories].").

139. United States v. Crist, No. 1:07-cr-211, 2008 WL 4682806, at *9 (M.D. Pa. Oct. 22, 2008). *But see* Posting of Orin Kerr, *supra* note 55 (arguing that using a hash to compare files to known images of child pornography is analogous to a constitutionally permissible drug-sniffing dog).

140. *Crist*, 2008 WL 4682806, at *10.

141. *See, e.g.*, Trulock v. Freeh, 275 F.3d 391, 398, 403 (4th Cir. 2001) (concluding that a live-in girlfriend could not consent to a police search of her boyfriend's computer files when the police were told that the computer was shared but that each had password-protected files inaccessible to the other); *see also* United States v. Andrus, 483 F.3d 711, 719–22 (10th Cir. 2007) (concluding that a father had apparent authority to consent to a police search of his adult son's password-protected computer, which the court categorized as a locked container). The court in *Andrus*, however, refused to presuppose that password protection is so common that a reasonable police officer should know that a computer is likely to be so protected. *Id.* at 721.

142. *See, e.g.*, *Trulock*, 275 F.3d at 398, 403.

143. The virtual-container analogy has been criticized in the offline context as a "fluctuating" concept, and one in which law enforcement officers argue that "they must be able to open *any* file to know what it is." G. Robert McLain, Jr., Note, United States v. Hill*: A New Rule, But No Clarity for the Rules Governing Computer Searches and Seizures*, 14 GEO. MASON L. REV. 1071, 1098, 1100 (2007) (emphasis added).

records can be stored."[144] But that language appeared in a footnote as a conclusion assumed without any explanation.[145] The website in *D'Andrea* was password protected, and the court cited Professor Warren LaFave, "a preeminent authority on the Fourth Amendment," for the proposition that a person using a password-protected website should be entitled to claim a reasonable expectation of privacy in the contents of the website.[146] Professor LaFave contends that "protections such [as] individual computer accounts, password protection, and perhaps encryption of data should be no less reasonable than reliance upon locks, bolts, and burglar alarms, even though each form of protection is penetrable."[147] The court seemed to presume that the password protection in the case at bar was *sufficient* to afford a reasonable expectation of privacy, though there is no indication as to whether password protection is *necessary* or, more generally, how a court is to determine what constitutes sufficient efforts to conceal a virtual container.

Even though unlocked physical containers, like the bag in *Bond v. United States*, may be afforded Fourth Amendment protections,[148] virtual methods of concealment such as encryption are more contentious. Professor Orin Kerr argues that this approach to determining whether an expectation of privacy is "reasonable" is rights-based[149]—an expectation is constitutionally "reasonable" or "legitimate" when it is backed by an enforceable, extraconstitutional right to enjoin the government's invasion of privacy.[150] Thus, the modern *Katz* test is not based upon how likely it is that something will remain private, but

144. United States v. D'Andrea, 497 F. Supp. 2d 117, 122 n.16 (D. Mass. 2007).

145. *Id.*

146. *Id.* at 121 (citing 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.6(f), at 721 (4th ed. 2004)).

147. LAFAVE, *supra* note 146, § 2.6(f), at 721 (quoting Randolph S. Sergent, Note, *A Fourth Amendment Model for Computer Networks and Data Privacy*, 81 VA. L. REV. 1181, 1200 (1995)). *But see* Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?"*, 33 CONN. L. REV. 503, 532 (2001) [hereinafter Kerr, *Cyberspace Encryption*] (arguing that historically, decrypting encrypted communications has been held not to violate a reasonable expectation of privacy, and that conclusion does not change in the Internet context).

148. *See* Bond v. United States, 529 U.S. 334, 338–39 (2000); *see also* United States v. Bosby, 675 F.2d 1174, 1180 (11th Cir. 1982) ("Absent exigent circumstances, closed containers such as a briefcase or pieces of personal luggage even if unlocked cannot be searched absent a warrant.").

149. Kerr, *Cyberspace Encryption*, *supra* note 147, at 507.

150. *Id.*

instead upon whether a person has the right to keep others out.[151] The government, Kerr concludes, is free to try to crack encrypted information, but "the fact that it will probably fail does not create Fourth Amendment protection."[152]

This interpretation of case law is not universal.[153] Furthermore, Kerr bases his argument on the premise that encryption is a flawed virtual analogy to a lock and key.[154] Hypothetically, if a briefcase is locked with a combination lock, the government could attempt to guess the combination until the briefcase unlocked; but because the briefcase is opaque, there is still a reasonable expectation of privacy in the unlocked container. In the context of virtual containers in the cloud, however, encryption is not simply a virtual lock and key; it is virtual *opacity*.[155]

But does it follow that an unlocked portion of the cloud—one not password protected at all—could also be protected? Can obscurity alone serve as virtual opacity? An unlisted link, like an unlisted telephone number, does not technically block access; it merely excludes a web address from search engine results.[156] In the case of Google accounts, the random string of numbers or letters used to protect the address can be rescrambled if an accountholder wishes to reclaim privacy,[157] similar to someone changing the lock on the front door of his house. In this regard, an unlisted link is not significantly different from a password-protected account, so long as it truly remains unlisted.[158] Such a web page is essentially relegated to the so-

151. *See id.* at 508.

152. *Id.* at 518.

153. *See, e.g.*, Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 532 n.135 (2005) (arguing that Kerr's assertions have grounding in "supportive dicta" but are nonetheless "inapposite or unpersuasive"); Sean J. Edgett, Note, *Double-Clicking on Fourth Amendment Protection: Encryption Creates a Reasonable Expectation of Privacy*, 30 PEPP. L. REV. 339, 355–61 (2003).

154. Kerr, *Cyberspace Encryption*, *supra* note 147, at 520–21.

155. *See* Edgett, *supra* note 153, at 365 ("Encryption makes a document invisible to outsiders . . . . Instead of using physical walls, it creates a digital wall . . . .").

156. *See, e.g.*, Picasa Album Privacy, *supra* note 91.

157. Google Video Privacy, *supra* note 89.

158. When Google initially provided an "unlisted" option for Picasa photo albums, the URL did not contain an authentication key, but instead simply included the name of the album in the address, making it relatively easy to guess. *See* Google Blogoscoped, Picasa Fixes Privacy Vulnerability, http://blogoscoped.com/archive/2006-10-07-n48.html (Oct. 7, 2006) (reporting that

called "invisible web."[159] This type of concealment via obscurity is harder to analogize to the physical world.

Although Professor LaFave and the *D'Andrea* court provide useful steps in the right direction, certain questions remain unanswered. The virtual-container theory is not universally recognized, nor is there any clear rule that recognizes which virtual-concealment methods satisfy the reasonableness requirement of *Katz*.[160] In addition, the role of third-party intermediaries, such as service providers, must be properly addressed.

C. THIRD-PARTY INTERMEDIARIES

Under *Katz*, the Court recognized that although a caller has a reasonable expectation of privacy in his telephone conversations vis-à-vis the outside world (including the police), the caller still assumes the risk that the other party to the conversation will reveal the contents of the call to others or the authorities.[161] When third-party intermediaries are involved, the third-party doctrine holds that certain transactional aspects of the communication may be lawfully obtained from the intermediary; thus, a telephone-service provider is considered a party to the numbers dialed,[162] and a bank is considered a party to the transactional records of its customers.[163] Courts have begun to address this issue in the online world, but there are reasons to question whether obtaining e-mail to/from addresses is the same as a pen register; and whether a password, unlisted URL, or other data accessible via the cloud are transactional or protected content.[164]

Courts have rightfully recognized that the recipient of online communications is a party to that communication. The dis-

Google added an authentication key to the web addresses of unlisted Picasa albums after facing criticism).

159. *See* Wright, *supra* note 138; Invisible Web, *supra* note 138. This could also bring into question websites with "noindex" meta tags, which are special tags that can be embedded within a web page's HTML code telling search engine robots not to index the page contents. HAROLD DAVIS, GOOGLE ADVERTISING TOOLS 61–62 (2006).

160. Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).

161. *Id.* at 363 n.* (White, J., concurring).

162. Smith v. Maryland, 442 U.S. 735, 744 (1979).

163. United States v. Miller, 425 U.S. 435, 442–43 (1976).

164. *See, e.g.*, Schuyler B. Sorosky, Note, United States v. Forrester*: An Unwarranted Narrowing of the Fourth Amendment*, 41 LOY. L.A. L. REV. 1121, 1138–39 (2008).

trict court in *D'Andrea* recognized this "well-settled" rule, finding that the defendants "took the risk that their right to privacy in the website's contents could be compromised" when they shared the website's password.[165] In *Quon*, the Ninth Circuit similarly recognized that the defendants had no reasonable expectation of privacy vis-à-vis each other;[166] however, the court found that the service provider itself was not a party to the content of the text messages, and thus could not be subpoenaed for those records.[167] The court's application of that rule to text messages implicitly applies to e-mails as well.

The only other federal appellate court decision to directly address the e-mail privacy issue as it pertains to third parties is *Warshak v. United States*, a Sixth Circuit case vacated on procedural grounds, in which the court similarly acknowledged that a court "must specifically identify the party with whom the communication is shared, as well as the parties from whom disclosure is shielded."[168] Although direct parties to an e-mail or other cloud communication are easily analogized to the callers in *Katz*, the status of the intermediary service providers have given courts more trouble.

The *Quon* case relied heavily upon another recent Ninth Circuit case, *United States v. Forrester*, for the proposition that e-mail users "'have no expectation of privacy in the to/from addresses of their messages . . . because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.'"[169] The court in *Forrester* analogized the to/from addresses on e-mails to the pen register, the search of which was

165. United States v. D'Andrea, 497 F. Supp. 2d 117, 123 (D. Mass. 2007). Orin Kerr has pointed out, however, that the court was wrong to assume that the password was voluntarily shared with the anonymous police informant; the password could have been obtained without the website owner's permission or knowledge, or the anonymous informant may not have been granted full access rights. Posting of Orin Kerr to The Volokh Conspiracy, http://volokh.com/posts/1185284749.shtml (July 24, 2007, 10:20).

166. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 906 (9th Cir. 2008).

167. *Id.* at 905–06.

168. Warshak v. United States, 490 F.3d 455, 470 (6th Cir. 2007), *vacated* 532 F.3d 521 (6th Cir. 2008). "[I]f the government in this case had received the content of Warshak's e-mails by subpoenaing the person with whom Warshak was e-mailing, a Fourth Amendment challenge brought by Warshak would fail, because he would not have maintained a reasonable expectation of privacy vis-à-vis his e-mailing partners." *Id.* at 471.

169. *Quon*, 529 F.3d at 905 (quoting United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (omission in original)).

held constitutionally valid in *Smith v. Maryland*.[170] There are potential problems with that direct analogy. In *Smith*, the Court distinguished numbers dialed from call content, finding that the former does not reveal who was on either end of the line or whether a conversation even took place.[171] Telephones—particularly public telephones—are routinely used by multiple people, and a pen register does not identify who made the call or who answered, it only identifies the numbers associated with either end. An e-mail account, on the other hand, is generally associated with only one user, and the address often includes the name of the person with whom it is associated. Obtaining to/from addresses goes beyond a pen register's level of intrusion by more precisely identifying the parties to the conversation.

The court's imprecise pen-register analogy aside, an e-mail address *is* in many ways akin to the to/from addresses on a standard letter; the addresses are conveyed to the e-mail service provider in order to complete the communication, and users should be reasonably aware of this. In *Quon*, the court made this analogy to the outside of an envelope.[172] Still, even commentators who agree with the court's finding in *Forrester* on Fourth Amendment grounds concede to the invasiveness of noncontent Internet surveillance.[173]

Even if it is proper to place to/from addresses outside the ambit of Fourth Amendment privacy protection, transactional information in general has become more revelatory and easier to obtain from the cloud,[174] and includes more than just e-mail addresses.[175] A web address, for example, might be considered transactional in nature due to the fact that an Internet browser must request that IP address to connect to the website.[176] Does

170. Smith v. Maryland, 442 U.S. 735, 742 (1979); *Forrester*, 512 F.3d at 505.

171. *Smith*, 442 U.S. at 741 ("'[Pen registers] do not hear sound. They disclose only the telephone numbers that have been dialed . . . .'" (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 167 (1977))).

172. *Quon*, 529 F.3d at 905 ("[I]ndividuals do not enjoy a reasonable expectation of privacy in what they write on the outside of an envelope.").

173. Posting of Orin Kerr to The Volokh Conspiracy, http://volokh.com/posts/1185384966.shtml (July 25, 2007, 13:36).

174. Dempsey, *supra* note 35, at 556 ("The rule that transactional information about the communications is unprotected had more limited implications when transactional data didn't reveal very much and was hard to analyze.").

175. *Forrester* also held that the IP addresses of websites a person has visited and the amount of data transmitted to or from an account are transactional and subject to the third-party doctrine. 512 F.3d at 510.

176. *See generally* 1 THE INTERNET ENCYCLOPEDIA 218–19 (Hossein Bidgoli

this mean that an unlisted link—authentication key and all—is subject to being subpoenaed from the cloud platform service provider without any Fourth Amendment problem? Furthermore, even a password-protected account requires a user to transmit the username and password to the service provider for authentication, so is the password itself considered transactional data to which the service provider is a party? Professor Kerr recently argued that the third-party doctrine acts as implied consent to search as opposed to the waiver of a reasonable expectation of privacy.[177] However, courts have maintained that a third party's limited rights of access do not eviscerate a reasonable expectation of privacy.[178] Therefore, even under a consent formulation, that consent is itself limited in scope.

This conforms with how recent courts have treated service providers with limited rights of access to communications content. In *Quon*, the court found the fact that the service provider *could have* accessed the message contents for its own purposes was not enough to destroy the users' reasonable expectations of privacy in those contents.[179] And, although not explicitly addressing the role of the service provider, the court in *D'Andrea* acknowledged that the government "can only compel disclosure of the specific information to which the subject of it has been granted access."[180] Because the informant in that case was not the service provider, the court did not address the issue of transactional data.[181] However, under the reasoning of the Ninth and Sixth Circuits, the contents of a protected website would be similarly shielded regardless of the service provider's ability to access the website's contents.[182]

ed., 2004) (explaining the process undertaken when a webpage is requested).

177. Kerr, *Third-Party Doctrine*, *supra* note 65, at 588.

178. *See e.g.*, United States v. Owens, 782 F.2d 146, 150 (10th Cir. 1986) (holding that luggage left in a motel room is still protected by the Fourth Amendment even if the checkout time has passed and the motel may legally enter by force and evict the hold-over guest).

179. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 905 (9th Cir. 2008) (citing United States v. Heckenkamp, 482 F.3d 1142, 1146–47 (9th Cir. 2007)); *see also* Warshak v. United States, 490 F.3d 455, 470 (6th Cir. 2007), *vacated*, 532 F.3d 521 (6th Cir. 2008) (arguing that if the third-party doctrine applied to every intermediary that has minimal access to content, then "letters would never be protected, by virtue of the Postal Service's ability to access them; [and] the contents of shared safe deposit boxes or storage lockers would never be protected, by virtue of the bank or storage company's ability to access them").

180. United States v. D'Andrea, 497 F. Supp. 2d 117, 122 (D. Mass. 2007).

181. *See id.* at 122–23 (treating the anonymous caller as a private party).

182. *Quon*, 529 F.3d at 905 (citing *Heckenkamp*, 482 F.3d at 1146–47);

It is not surprising that new technologies bring forth novel legal questions, and there is nothing new about courts analogizing to the past to deal with the present. So far courts have made some proper analogies—treating e-mails like letters, treating a password-protected website like a virtual container, and distinguishing between content and transactional data in the cloud. But these piecemeal solutions are not universally recognized, and do not fully address the complexities associated with cloud computing and societal expectations. It is unclear whether online content other than e-mails is protected, or whether other jurisdictions will follow the Ninth Circuit's approach to e-mails.[183] It is also unclear whether other courts will embrace the virtual-container theory, and, if they do embrace it, exactly what the contours of that theory will be. Finally, the line between content and transactional data in the cloud is far from settled. A new framework, built upon these early decisions, is therefore necessary.

III. A FOURTH AMENDMENT FRAMEWORK FOR THE DIGITAL CLOUD

With individuals and entities increasingly using the cloud to conduct business and store data, it is important to have a clear framework within which the government may conduct a search that meets constitutional requirements. First, courts must recognize that the Internet is evolving and that in some circumstances people place items in the cloud for private purposes. Society seems prepared to recognize that privacy interests in online data can be reasonable, thus satisfying one prong of Justice Harlan's *Katz* test.[184] Second, the virtual-container theory alluded to in *D'Andrea* should be universally recognized.[185] Under that theory, it should be acknowledged that virtual methods of concealment, such as encryption and password protection, satisfy an individual's subjectively reasonable expectation of privacy. Finally, the third-party doctrine must reasonably address society's expectations about its digital footprint. Courts should recognize that files stored online are not transactional because their contents are not intended or required to be viewed by a third party, and should create a prac-

Warshak, 490 F.3d at 470.

183. United States v. Forrester, 512 F.3d 500 (9th Cir. 2008).

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

185. *D'Andrea*, 497 F. Supp. 2d at 122 n.16.

tical exception for certain quasi-transactional data such as URLs and passwords in order to respect the legitimate safeguards of virtual content.

A. COURTS SHOULD RECOGNIZE SOCIETY'S REASONABLE EXPECTATION OF PRIVACY IN THE CLOUD AS THE COURT DID WITH THE TELEPHONE IN *KATZ*

The doctrinal basis exists to recognize that individuals can retain privacy interests in online objects, but that basis is limited. *Katz* recognized that people can have reasonable expectations of privacy in intangible objects,[186] which has come to include digital objects.[187] Furthermore, *Quon* supports the proposition that digital files, considered "highly personal" when in tangible form,[188] do not change in nature simply by being placed in the cloud.[189] But only one circuit has found "no meaningful difference" between e-mails and physical letters.[190] Helpful language from the Sixth Circuit's *Warshak* case was unfortunately vacated on procedural grounds.[191] More importantly, recognition of e-mail privacy does not make clear what protections will cover address books, calendars, photo albums, and other documents stored in the cloud.

Certainly in many ways the Internet remains, as one court put it, "an indisputably, public medium," but even that court qualified its statement with an acknowledgment that measures could be taken to protect information stored there.[192] The evolving, anywhere-access function of the Internet makes the cloud a public medium into which private items are increasingly—and reasonably—placed, interacted with, and stored. Just as a bag of personal items may be brought onto a public bus[193] or into a public school[194] and retain its privacy protection, it is reasona-

186. *Katz*, 389 U.S. at 353 (citing Silverman v. United States, 365 U.S. 505, 511 (1961)).

187. *E.g.*, United States v. Crist, No. 1:07-cr-211, 2008 WL 4682806, at *9 (M.D. Pa. Oct. 22, 2008).

188. *See* New Jersey v. T.L.O., 469 U.S. 325, 339 (1985).

189. *See* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 905 (9th Cir. 2008).

190. *See id.*

191. Warshak v. United States, 532 F.3d 521, 534 (6th Cir. 2008) (finding the issue to be unripe).

192. United States v. Gines-Perez, 214 F. Supp. 2d 205, 225 (D.P.R. 2002).

193. *See* Bond v. United States, 529 U.S. 334, 338–39 (2000).

194. Doe *ex rel.* Doe v. Little Rock Sch. Dist., 380 F.3d 349, 352 (8th Cir. 2004) (citing New Jersey v. T.L.O., 469 U.S. 325, 334–52 (1985)).

ble to treat personal items placed on the Internet in the same way. The cloud has become our "home . . . away from home."[195] Society's willingness to put such highly personal items in the cloud shows that it is prepared to recognize a reasonable expectation of privacy there.

In practice, this simply means that courts should acknowledge not only that technology is changing, but that our uses and expectations regarding those technologies mature over time as well. Early telephone users might have thought it absurd to expect privacy in a telegraph or a party line phone call,[196] yet *Katz* eventually recognized that phone calls could be private, in part because society had come to expect as much.[197] Similarly, before courts can even entertain whether encryption is a reasonable effort to conceal online or how the third-party doctrine should apply, they must first accept the premise that current Internet usage carries with it a reasonable societal expectation of privacy.

B. COURTS SHOULD ADOPT THE VIRTUAL-CONTAINER THEORY TO STANDARDIZE PRIVACY APPRAISALS IN THE CLOUD, AND RECOGNIZE VIRTUAL-CONCEALMENT EFFORTS

No matter to what extent society is prepared to recognize a privacy interest in cloud computing, reasonable concealment efforts are still necessary under the current Fourth Amendment analysis.[198] But there are no bags, backpacks, or briefcases in the cloud. Instead, there are folders and web pages which exist at various points on the spectrum from public to private. At least one court explicitly analogized a website to a container, rightfully assuming that the contents were concealed behind a password lock.[199] Similarly, other courts analogized intangible virtual folders and hard drive partitions to containers in the of-

195. *Id.* at 353.

196. *See, e.g.*, CLAUDE S. FISCHER, AMERICA CALLING: A SOCIAL HISTORY OF THE TELEPHONE TO 1940, at 52 (1992) ("In 1929 most residential customers had party lines.").

197. Katz v. United States, 389 U.S. 347, 358 (1967).

198. An improperly concealed item does not carry with it a reasonable expectation of privacy no matter how personal the item is. *See, e.g.*, United States v. Ross, 456 U.S. 798, 822–23 (1982) ("[T]he Fourth Amendment provides protection to the owner of every container that *conceals its contents from plain view*." (emphasis added)); United States v. Meada, 408 F.3d 14, 23 (1st Cir. 2005) (finding that a labeled container betrayed its contents and therefore the container did not provide a reasonable expectation of privacy).

199. United States v. D'Andrea, 497 F. Supp. 2d 117, 122 n.16 (D. Mass. 2007).

fline context.[200] This analogy does not change once the virtual container is uploaded into the cloud any more than a physical container fails to be considered a container once taken out into public.

Although the virtual-container theory has been criticized in the offline context,[201] the more ethereal and dynamic nature of the cloud requires a practical fiction. Still, the criticisms are not without merit—law enforcement needs the ability to seek a warrant for virtual containers in certain circumstances, which means the contours of such containers must be defined. Simply acknowledging that virtual containers exist does not necessarily grant one a reasonable expectation of privacy in its contents. A container is a possible means of concealment, but not every container conceals its contents.[202] Because literal opacity is not an option online, the only way to conceal virtual items in the cloud is through virtual barriers to entry, such as password protection or encryption. Historically, the decryption of encrypted messages by the government has been found not to raise Fourth Amendment concerns.[203] Thus, an encrypted letter sealed in an envelope would be covered by the Fourth Amendment, but the legal basis for its protection would be the envelope, not the encryption.

The folly of this distinction is magnified in the modern age for two reasons. First, modern encryption has become more complex, and in some instances nearly unbreakable,[204] yet the mere sealing an envelope or closing the zipper on a bag is considered a reasonable effort to conceal while encryption is not.[205] Some scholars would dismiss this assessment by pointing out that encryption is different because it is a false method of concealment, along the lines of speaking in an obscure language, and the Constitution cannot prohibit law enforcement from fi-

200. *See e.g.*, United States v. Crist, No. 1:07-cr-211, 2008 WL 4682806, at *9 (M.D. Pa. Oct. 22, 2008); *see also* Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001).

201. McLain, *supra* note 143, at 1100.

202. *E.g.*, *Meada*, 408 F.3d at 23.

203. *See* Kerr, *Cyberspace Encryption*, *supra* note 147, at 517.

204. *See* Pease, *supra* note 96.

205. Neither type of concealment is foolproof, but the fact that a form of protection is penetrable does not preclude the finding of a reasonable expectation of privacy. LAFAVE, *supra* note 146, § 2.6(f), at 721 (quoting Randolph S. Sergent, Note, *A Fourth Amendment Model for Computer Networks and Data Privacy*, 81 VA. L. REV. 1181, 1200 (1995)). *But see* Kerr, *Cyberspace Encryption*, *supra* note 147, at 508.

guring it out.[206] But encryption is far more effective than speaking in an obscure language or using an easily decipherable code.[207] Law enforcement could conceivably "figure out" the combination to a padlock more quickly and easily than it could decrypt modern encryption, but that does not eviscerate privacy interests in a physically locked container. Second, while a person encrypting a letter has the option of placing that letter into an envelope to garner Fourth Amendment privacy protection, one conducting business in the cloud does not have that luxury. Because opacity is not available in the digital context, encryption or password protection are among a limited number of privacy options.

Furthermore, a file does not necessarily even have to be uploaded into the cloud to be accessible from the cloud. By connecting a personal computer to the Internet, that hard drive and all of the virtual containers inside of it become a part of the cloud, and may be remotely accessible.[208] With an increasing number of households connected to the Internet,[209] the virtual threshold to the home is obscured. By recognizing that virtual containers exist and, when properly protected by virtual means such as encryption or password protection, maintain a reasonable expectation of privacy, the courts will prevent law enforcement from using a technological backdoor to avoid Fourth Amendment limitations.

Unlisted links raise another problem. Unlike a password, an unlisted link is concealed by practical obscurity within the "invisible web."[210] If a password is analogous to a lock[211] or opacity, and an obscure web address is analogous to an obscure

206. *See* Kerr, *Cyberspace Encryption*, *supra* note 147, at 515.

207. *See* Edgett, *supra* note 153, at 356–57 ("[E]ncryption does not work like an international language. There is only one code that can decipher the message . . . . If individuals are speaking a language unique to the two of them—an equivalent to encryption—then there should be a reasonable expectation of privacy." (citation omitted)).

208. *E.g.*, Remote Access Service Overview, http://www.remotepc.com/overview.htm (last visited Apr. 17, 2009). The British government is being criticized for a new policy that allows police to conduct "remote searching" of people's computers without a warrant. David Leppard, *Police to Step Up Hacking of Home PCs*, SUNDAY TIMES (London), Jan. 4, 2009, at 14.

209. Scarborough Research, Broadband Penetration Increased, *supra* note 126.

210. *See* Wright, *supra* note 138; Invisible Web, *supra* note 138.

211. *See, e.g.*, United States v. Andrus, 483 F.3d 711, 718 (10th Cir. 2007) ("Data on an entire computer may be protected by a password, with the password functioning as a lock . . . .").

physical address, then it would seem that the former is a reasonable effort to conceal and the latter is not. After all, the fact that someone lives at an obscure address does not prevent the police from tracking them down. But when an unlisted link contains an authentication key in its address, the analogy to the physical world loses its precision. The address and the lock and key become one and the same. If a person's obscure home was locked by electronic means, and the password to that lock happened to be the home's street address, the police could not use that knowledge to enter the home without a warrant. Just because the police *can* open a container does not mean the Constitution permits a search.[212]

Courts should universally recognize what the district court in *D'Andrea* recognized—virtual containers exist in the cloud. But they need to go a step further and also acknowledge the legitimacy of virtual concealment efforts—encryption, password protection, and the practical obscurity of unlisted links—as means of opacity in the cloud context. Under this rule, courts would make a case-by-case determination as to whether a user's reliance upon a password, encryption, or obscurity was a reasonable effort to conceal in a given situation. It is not a burden for law enforcement to determine whether a password is necessary to access a website, at which point it would need a warrant prior to accessing the account. Conversely, in the unlisted-link context, if an unlisted address appears on a public website as a hyperlink, law enforcement should be given discretion to treat such a virtual container as in plain view.

C. COURTS SHOULD TREAT CLOUD SERVICE PROVIDERS AS VIRTUAL LANDLORDS AND APPLY THE THIRD-PARTY DOCTRINE NARROWLY TO CLOUD CONTENT

Distinguishing between transactional and content data in the cloud can be difficult, but certain logical analogies should be followed by the court. Entering a search term into a search engine, for example, is the equivalent of asking the search provider a question—initiating a transaction—and a user assumes the risk that the service provider will reveal that information.[213] The to/from addresses on e-mails have also been consi-

212. *See, e.g.*, Garcia v. Dykstra, 260 F. App'x 887, 897–98 (6th Cir. 2008) (finding that plaintiffs retained a reasonable expectation of privacy in the contents of a locked storage unit even though the key was found by police on the ground near the padlock).

213. *See, e.g.*, Jayni Foley, Note, *Are Google Searches Private? An Original-*

dered transactional data, akin to an addressed envelope.[214] However, the contents of an e-mail have been properly classified as content data.[215] A service provider, even if it has the capability of accessing the contents of an e-mail, is not a party to the information.[216] Similarly, access to the content of a calendar, address book, photo album, text document, or private blog is not given to the service provider. Although the user might be interacting with a cloud-based word processor or spreadsheet, the content of those documents is not intended to be shared with the provider; the provider is merely providing a platform for using and storing the content via the cloud. Whatever minimal right the service provider reserves to access the contents of those files or containers, the service provider is not a party to the contents any more than a landlord is a party to what goes on behind his tenants' closed doors due to his limited right of entry.[217]

But while calendars, photo albums, and the like are more clearly content data as opposed to transactional, other types of data are less clear. The web address of a cloud container—even if it is unlisted—resides on the servers of the cloud service provider, and must be "dialed" by a user and authenticated by the provider before access is granted.[218] A password must similarly be authenticated.[219] Thus, the service provider has a copy of the keys to a user's cloud "storage unit," much like a landlord or storage locker owner has keys to a tenant's space, a bank has the keys to a safe deposit box, and a postal carrier has the keys

ist Interpretation of the Fourth Amendment in Online Communication Cases, 22 BERKELEY TECH. L.J. 447, 457 (2007) ("As the law currently stands, the broad 'assumption-of-risk' language in *Miller* and *Smith* provides the basis for arguments that search engine users lack an expectation of privacy in communications held by search engines and ISPs."); *see also* United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000).

214. *See* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 905 (9th Cir. 2008) (citing United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008)).

215. *Id.*

216. *Id.* (citing United States v. Heckenkamp, 482 F.3d 1142, 1146–47 (9th Cir. 2007)).

217. *E.g.*, Chapman v. United States, 365 U.S. 610, 616–18 (1961); *cf.* Stoner v. California, 376 U.S. 483, 489 (1964) (finding that a hotel proprietor lacks the authority to consent to a search of an occupied hotel room); United States v. Owens, 782 F.2d 146, 150 (10th Cir. 1986) (same).

218. *See* THE INTERNET ENCYCLOPEDIA, *supra* note 176, at 218–19.

219. *See* MATTHEW STREBE, NETWORK SECURITY JUMPSTART: COMPUTER AND NETWORK SECURITY BASICS 51 (2002) (explaining how password authentication works).

to a mailbox.[220] Yet that does not give law enforcement the authority to use those third parties as a means to enter a private space.[221]

The same rationale should apply to the cloud. In some circumstances, such as search engine queries, the third party is clearly an interested party to the communication. But when content data, passwords, or URLs are maintained by a service provider in a relationship more akin to that of landlord-tenant, such as private Google accounts, any such data that the provider is not directly interested in should not be understood to be open to search via consent or a waiver of Fourth Amendment protection.

CONCLUSION

The Internet is constantly evolving. The increased speed and mobility of Internet access, and the more widespread usage of Internet services and digital information, makes the online cloud more than a public medium—it is an anywhere-access point for private data. Companies and individuals turn to the cloud as a convenient and cheap alternative to traditional hard drive storage, and society expects its photo albums, address books, calendars, documents, and e-mails to maintain the same protections on a secure account in the cloud as they would if stored on a home computer. The increased availability and usage of virtual concealment tools, such as passwords, encryption, and unlisted links, make these expectations of privacy subjectively reasonable. Further, since users are not sharing this content with the service provider, but merely asking the provider to store it, the idea that the Constitution would permit law enforcement to subpoena from a service provider a document stored in an otherwise private account is rightly viewed as unreasonable.

One might argue that if a person wants to keep his papers and effects private, he should keep them at home or send them through the mail. But had the Supreme Court followed that line of reasoning forty years ago, people would not be able to place a private telephone call. By universally recognizing that digital content does not lose its highly personal status when it

220. *See* Posting of Daniel J. Solove to Concurring Opinions, http://www.concurringopinions.com/archives/2007/07/the_fourth_amen.html (July 9, 2007, 2:11).

221. *Quon*, 529 F.3d at 905 (citing *Heckenkamp*, 482 F.3d at 1146–47); *supra* note 179 and accompanying text.

is placed online, and by further recognizing that properly concealed virtual containers retain reasonable expectations of privacy, the courts will bring Fourth Amendment law up to speed with modern technology and societal expectations. Furthermore, by acknowledging that the relationship between a cloud service provider and a user is akin to a landlord-tenant relationship and is not entirely transactional, courts will further ensure that privacy concerns do not hamper the expansion of an efficient new way to store and interact with personal digital data.