Storing Documents in the Cloud: Toward an Evidentiary Privilege Protecting Papers and Effects Stored on the Internet

*Jacob M. Small**

Introduction

In June 1789, James Madison presented a proposal to the House of Representatives that, after winding its way through the legislative process, became the Bill of Rights: the first ten amendments to the United States Constitution.[1] Had he written the amendments today, he might have done so on a computer. But as it was 1789, he likely set quill to parchment. And when he penned the Fourth Amendment, he extended its protection to "persons, houses, papers, and effects,"[2] a phrase that clearly encompassed that parchment and quill.

But today, many documents are electronic. And increasingly, those electronic documents are stored, not on their owners' computers, but on those of third-party companies.[3] These companies offer so-called "cloud computing" services that allow users to produce, edit, and store documents on the companies' hardware.[4] The "cloud com-

* Associate Attorney, The Spiggle Law Firm in Arlington, Virginia; J.D., George Mason University, Civil Rights Law Journal. I wish to thank my wife Jennifer Small for her patience and support and my grandmother Ann Hunter for her advice and editorial expertise.

1 *Preface*, 12 Papers of James Madison 185 (Charles F. Hobson et al. eds., The University Press of Virginia 1979); Herman Ames, The Proposed Amendments to the Constitution of the United States During the First Century of its History, 184 (Lenox Hill Publ'g & Distrib. Co. 1970).

2 U.S. Const. amend. IV.

3 John B. Horrigan, *Cloud Computing Gains in Currency: Online Americans Increasingly Access Data and Applications Stored in Cyberspace*, Pew Research Center (Sept. 12, 2008), http://pewinternet.org/~/media//Files/Reports/2008/PIP_Cloud.Memo.pdf.pdf ("Some 69% of online Americans use webmail services, store data online, or use software applications whose functionality is located on the web.") (last visited February 23, 2013).

4 Timothy D. Martin, *Hey! You! Get Off of My Cloud: Defining and Protecting the Metes and Bounds of Privacy, Security, and Property in Cloud Computing*, 92 J. Pat. & Trademark Off. Soc'y 283, 287 (2010) ("Rather than storing and accessing information on [their] desktop computer, [cloud computing users'] data and software exist on remote servers and are accessible wherever [they] happen to be.") (quoting Brad Smith, Senior Vice President and General Counsel, Microsoft, Keynote Address at the Brookings Institution: Cloud Computing for Business and

puting" services offer clients—businesses or individuals—several advantages over local storage.[5] For example, clients of cloud computing services may have the ability to access their data from anywhere with a mobile device,[6] have multiple authors edit the same document,[7] and lease computing services and storage capacity on an as-needed basis.[8] Unsurprisingly, the percentage of users who store data in the cloud is expected to grow rapidly over the coming years.[9]

Storing data on a company's servers (cloud-based data storage) is not without risks.[10] Companies such as Google have privacy policies that allow them to scan the data's contents to better target their clients' advertising at users.[11] At least one company has lost large quantities of users' data.[12] However, this Article focuses on another risk: the risk that the government might compel a service provider to produce copies of a person's documents without a warrant based upon

---

Society (Jan. 20, 2010), available at http://www.microsoft.com/presspass/presskits/cloudpolicy/docs/20100120_transcript.pdf).

[5] *See* Michael Armbrust et al., *Above the Clouds: A Berkeley View of Cloud Computing* 4, UC BERKELEY RELIABLE ADAPTIVE DISTRIB. SYS. LAB. (2009), http://d1smfj0g31qzek.cloudfront.net/abovetheclouds.pdf ("The advantages of [Cloud Computing] to both end users and service providers are well understood.").

[6] *See, e.g.*, *Getting Started with Evernote*, EVERNOTE (Jan. 8, 2011), http://www.evernote.com/about/learn_more/.

[7] *See, e.g.*, *Google Docs: Campaign Speech*, YOUTUBE (Jan. 8, 2011), http://www.youtube.com/watch?v=jo_o5mjUSio (demonstrating how multiple authors can edit the same document using Google Docs) (last visited Feb. 23, 2013).

[8] Roger Smith, *Computing in the Cloud*, 52 RESEARCH TECH. MGMT. 65, 65-67 (Sept./Oct. 2009).

[9] Janna Quitney Anderson & Lee Rainie, *The Future of Cloud Computing*, PEW RESEARCH CENTER (2010), http://www.pewinternet.org/~/media//Files/Reports/2010/PIP_Future_of_the_Internet_cloud_computing.pdf [hereinafter *Pew Report*] ("A solid majority of technology experts and stakeholders participating in the fourth Future of the Internet survey expect that by 2020 most people will access software applications online and share and access information through the use of remote server networks, rather than depending primarily on tools and information housed on their individual, personal computers.") (last visited Feb. 23, 2013).

[10] *See generally Privacy Policy*, GOOGLE: POLICIES & PRINCIPLES (Jan. 8, 2011), http://www.google.com/privacy/privacy-policy.html (last visited Feb. 23, 2013); Jon Stokes, *T-Mobile and Microsoft/Danger Data Loss is Bad for the Cloud*, ARS TECHNICA (Oct. 12, 2009), http://arstechnica.com/business/news/2009/10/t-mobile-microsoftdanger-data-loss-is-bad-for-the-cloud.ars (last visited Feb. 23, 2013).

[11] *See Privacy Policy*, GOOGLE: POLICIES & PRINCIPLES (Jan. 8, 2011), http://www.google.com/privacy/privacy-policy.html (specifying that all of Google, Inc.'s services may collect data about a user's interaction with those services in order to "[p]rovide, maintain, protect, and improve" those services, including advertising services).

[12] Jon Stokes, *T-Mobile and Microsoft/Danger Data Loss is Bad for the Cloud*, ARS TECHNICA (Oct. 12, 2009), http://arstechnica.com/business/news/2009/10/t-mobile-microsoftdanger-data-loss-is-bad-for-the-cloud.ars.

probable cause, and that such a compelled production could be used against the user in a criminal trial.[13] This risk exists because of the Supreme Court's rulings in a series of Fourth Amendment cases from the 1970s.[14]

In *Couch v. United States*, *United States v. Miller*, and *Smith v. Maryland*, the Supreme Court established that individuals do not have a reasonable expectation of privacy; therefore, the Fourth Amendment does not protect the information they share with third-party companies.[15] Congress has since enacted the Stored Communications Act (SCA), which protects electronic documents shared with certain third parties.[16] However, when it comes to requiring the government to show evidence prior to conducting a search, the SCA offers less protection than the Fourth Amendment.[17] In general, the government has a lower burden to satisfy in obtaining court orders compelling ex parte production of documents, when the documents are electronic and stored on a third-party's server.[18] Using this lower standard means a dilution of Fourth Amendment protections if the government seizes the "papers and effects" that, once stored in homes, are now stored in the cloud.

This Article reviews the statutory and constitutional landscape relevant to searches and seizures of documents stored in the cloud. It then argues that current law provides insufficient protection for the types of property that the Fourth Amendment was intended to protect, and that the appropriate response is the creation of an evidentiary privilege between online document storage providers and end users. Part I reviews constitutional and statutory search and seizure law and discusses modern trends in cloud computing. Part II analyzes the relevant decisions and academic discourse, illustrating that, under

---

13 *See* Achal Oza, *Amend the ECPA: Fourth Amendment Protection Erodes as E-mails Get Dusty*, 88 B.U. L. REV. 1043, 1044-45 (2008).

14 Smith v. Maryland, 422 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976); Couch v. United States, 409 U.S. 322 (1973).

15 *See* discussion *infra* Part I.C.2.

16 18 U.S.C. §§ 2701-2711 (2006).

17 *See* discussion *infra* Part I.D.

18 *Compare* U.S. CONST. amend IV ("[N]o [w]arrants shall issue, but upon probable cause, supported by [o]ath or affirmation . . ."), *with* 18 U.S.C. § 2703(d) ("A court order for disclosure . . . shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.").

current law, documents stored in the cloud are accessible by the government upon a minimal factual showing. Part III presents discussion of the continuing need for a third-party doctrine while arguing that the Supreme Court should recognize an evidentiary privilege between cloud-based service providers and their clients.

I. BACKGROUND

Cloud computing services have arrived amidst a legal landscape that is unprepared to accommodate their unique characteristics.[19] Before the advent of the personal computer and the proliferation of the Internet, people did not have electronic documents nor were third-party companies offering electronic document management solutions. Thus, the Fourth Amendment has existed, for the most part, in a world where papers and effects could only mean physical items. This Part discusses the nature of cloud-based document storage and examines the legal landscape that the government will encounter as it attempts to compel production of documents stored in the cloud.

A. *An Introduction to Cloud-Based Document Storage*

Google, Inc. CEO Eric Schmidt has been credited with coining the term "cloud computing."[20] In an address at the Search Engine Strategies Conference in August of 2006,[21] Schmidt used the term to refer to software applications that were hosted on remote servers, as opposed to local machines.[22] Since then, use of the term has become ubiquitous.[23] The National Institute of Standards and Technology has even authored a definition of cloud computing, calling it "a model for enabling ubiquitous, convenient, on-demand network access to a

---

[19] *Cf.* 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, 1212 (2004) [hereinafter Kerr, *User's Guide to the SCA*] ("[The Internet is] almost 'custom designed' to frustrate claims of strong Fourth Amendment protection in remotely stored files under current Fourth Amendment Doctrine." (quoting Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 812-13 (2003)).

[20] *See, e.g.*, Richard Oppenheimer, *A Match Made in Heaven*, 17 SEARCHER 14, 14 (July 2009).

[21] Interview with Eric Schmidt, CEO, Google, Inc. (Aug. 9, 2006), *available at* http://www.google.com/press/podium/ses2006.html.

[22] *Id.*

[23] John Viega, *Cloud Computing and the Common Man*, 42 COMPUTER 106, 106 (Aug. 2009) ("Cloud computing is one of the biggest technology buzzwords these days.").

shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[24]

Although the definition sounds complicated, the premise behind cloud computing is relatively simple: Cloud computing is a different way for people to use their computers.[25] Until recently, when people needed to accomplish a task on a computer, they installed specialized software on that computer.[26] Under the cloud computing paradigm, however, the software exists on an Internet server.[27] Users can access the software on their local machines via a Web browser or specialized client programs, but the software that does the work, and the data and documents being accessed, exist on an Internet server, or "in the cloud."[28]

The potential advantages of this approach are numerous, and it would be impossible to highlight them all in this Article. Certain advantages, however, may have implications for Fourth Amendment applications. Particularly, cloud-based storage might replace several types of common physical articles, like photographs, financial records, books, and daily planners. Papers and effects, which used to mean physical objects in a desk drawer or on a shelf, are becoming digital records stored in the cloud.

Cloud-based storage solutions for photographs offer storage with added functionality. Google's Picasa service, for example, allows users to store photographs online, edit the images, order prints, share the images via e-mail or social networking sites, and access the images from any device with a Web browser.[29] Competitors like Flickr[30] and Photobucket[31] offer similar functionality. Even modern cameras, in lieu of transferring images directly to a hard drive, can be set up to

---

[24] NAT'L INST. OF STANDARDS & TECH., THE NIST DEFINITION OF CLOUD COMPUTING (Sept. 2011).

[25] *See* Horrigan, *supra* note 3.

[26] *See id*.

[27] *See id*.

[28] *See id*. at 3-4.

[29] *See Welcome to Picasa and Picasa Web Albums!*, GOOGLE, http://support.google.com/picasa/answer/157000?hl=en&ref_topic=1689652 (last visited Feb. 23, 2013).

[30] *See Welcome to the Flickr Tour*, FLICKR , http://www.flickr.com/tour (last visited Feb. 23, 2013).

[31] *See About Photobucket*, PHOTOBUCKET, http://beta.photobucket.com/about (last visited Feb. 23, 2013).

upload images directly to a user's chosen image hosting site, with no wires involved.[32] With these advantages, it is easy to understand why someone might elect to store all of their personal photographs online.

Similar advantages exist for users who need to create and edit text documents, spreadsheets, or presentations. Google Drive is a cloud-based service that hosts the document as well as the software suite.[33] Users only need a Web browser on a laptop, tablet computer, or mobile phone to access, edit, print, or present their documents.[34] They also have the ability to work collaboratively with colleagues, as Google Drive supports multiple users editing the same document concurrently.[35] Microsoft offers a similar service, called SkyDrive, which also offers cloud-based storage of documents.[36] Thus, people who elect to use these cloud-based office software suites may never house actual copies of documents on their own computers.

There are similar services for financial records,[37] notes,[38] personal calendars,[39] and eBooks.[40] The value proposition for users is clear: If a physical object's value derives from its content, it can most likely be stored online, providing users access anywhere, from any device. A developing trend is also becoming clear: Users are migrating to these services.[41] As they do, however, they may be migrating their papers

---

[32] Cameras equipped with Eye-Fi memory cards use wireless networks to automatically upload images to image hosting sites. *See Eye-Fi Features*, EYE-FI, http://www.eye.fi/features (last visited Feb. 23, 2013).

[33] *See Google Drive Apps*, GOOGLE, https://www.google.com/intl/en_US/drive/start/apps.html (last visited Feb. 23, 2013).

[34] *See Google Drive Home*, GOOGLE, https://www.google.com/intl/en_US/drive/start/index.html (last visited Feb. 23, 2013).

[35] *Id.*

[36] *See* Omar Shahine, *SkyDrive: Designing Personal Cloud Storage for Billions of People*, WINDOWS (Nov. 22, 2011), http://blogs.windows.com/windows_live/b/windowslive/archive/2011/11/22/skydrive-designing-personal-cloud-storage-for-billions-of-people.aspx (last visited Feb. 23, 2013).

[37] *See How Mint Works*, MINT, http://www.mint.com/how-it-works/ (last visited Jan. 26, 2013).

[38] *See About Evernote*, EVERNOTE, http://www.evernote.com/about/learn_more/ (last visited Jan. 26, 2013).

[39] *See Welcome to Google Calendar*, GOOGLE, http://www.google.com/intl/en/googlecalendar/about.html (last visited Jan. 26, 2013).

[40] Amazon's Kindle Store manages customers' purchases by allowing them to move copies of purchased eBooks from one device to another. *See New to Kindle? Start Here*, AMAZON, http://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=200505460 (last visited Jan. 26, 2013).

[41] *See* Horrigan, *supra* note 3; *Pew Report*, *supra* note 9.

and effects out from under the Fourth Amendment's umbrella of protection.

B. Katz v. United States *and Reasonable Expectations of Privacy*

Any discussion of modern Fourth Amendment law starts with the seminal 1967 case, *Katz v. United States*.[42] In *Katz*, the Supreme Court considered whether the defendant's Fourth Amendment rights were violated when police listened to his telephone call by attaching an electronic listening device to the telephone booth he used.[43] Precedent was not on the defendant's side, because almost thirty years prior to *Katz*, in *Olmstead v. United States*, the Court had held that an electronic wiretap did not amount to a search and seizure.[44] The Court in *Olmstead* had held that the Fourth Amendment only applied to searches and seizures of physical property.[45] The Court in *Katz*, however, changed course, explicitly overruling *Olmstead* and holding that "the Fourth Amendment protects people, not places."[46]

The Court concluded that the police had violated the defendant's Fourth Amendment rights by invading his privacy without a warrant.[47] It held that all searches, absent prior approval by a magistrate, are per se unreasonable.[48] As to what privacy interests are protected, such that invasions of them qualify as searches under the Fourth Amendment, Justice Harlan wrote in a concurring opinion that, "there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[49]

Katz extended Fourth Amendment protection to the information conveyed in an electronic communication, and outside of the bounds

---

[42] *See* Katz v. United States, 389 U.S. 347 (1967).

[43] *Id.* at 354.

[44] Olmstead v. United States, 277 U.S. 438, 466-68 (1928).

[45] *Id.* at 466; *see also id*. at 463 ("The well-known historical purpose of the Fourth Amendment, directed against general warrants and writs of assistance, was to prevent the use of governmental force to search a man's house, his person, his papers, and his effects, and to prevent their seizure against his will.").

[46] *Katz*, 389 U.S. at 351-53.

[47] *Id.* at 353.

[48] *Id.* at 357.

[49] *Id.* at 361 (Harlan, J., concurring).

of the amendment's explicit text.[50] For that reason, it has been called the "lodestar" of Fourth Amendment cases concerning electronic surveillance.[51] It is the two-part test in Justice Harlan's concurrence, however, that has been applied consistently to determine if police activity intrudes upon a protected privacy interest.[52] This Article is concerned with a specific application of Justice Harlan's second prong: whether a subjective expectation of privacy in documents stored on the Internet is one that society is prepared to recognize as reasonable.

C. *Third Parties, the Assumption of Risk, and Business Records*

In answering the question, "Is a particular expectation of privacy reasonable," the Supreme Court has developed a coherent doctrine that applies when persons share information with third parties: the so-called "third-party doctrine."[53] Applying the third-party doctrine in the landmark cases discussed below, the Supreme Court established that individuals have no legitimate expectation of privacy when they share information with others.[54] Pursuant to this rule, some electronic communications have come to be seen as unprotected by the Fourth Amendment because they are disclosures to third parties."[55]

---

[50] *See* David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2211-12 (2009) ("Although the Fourth Amendment refers only to 'persons, houses, papers, and effects,' *Katz* extended protection to privacy interests in intangible communications.") (internal citation omitted).

[51] Smith v. Maryland, 442 U.S. 735, 739 (1979).

[52] Beginning with Rakas v. Illinois, the Court has cited Justice Harlan's test to define when a "search" occurs. *See, e.g.*, Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978); *accord* Smith, 442 U.S. at 740.

[53] *See, e.g.*, Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563-65 (2009) [hereinafter Kerr, *Third-Party Doctrine*]; Stephen E. Henderson, *Nothing New Under The Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 518-21 (2005); Matthew D. Lawless, Comment, *The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection*, 2007 UCLA J.L. & TECH. 1, 8-26 (2007).

[54] Henderson, *supra* note 53 at 521.

[55] *See* ORIN S. KERR, DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING EVIDENCE IN CRIMINAL INVESTIGATIONS 6-10 (Computer Crime and Intellectual Prop. Section ed., Office of Legal Educ. 3rd ed. 2009); *see also* Henderson, *supra* note 53 at 521 (2005); *see generally* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE DIGITAL AGE (Jack M. Balkin & Beth Simone Noveck, eds., NYU Press 2006) (2004).

1. The Third-Party Doctrine

The origins of the third-party doctrine have been attributed to cases dealing with the government's use of undercover agents.[56] In one such case, *Hoffa v. United States*, the Supreme Court laid the doctrine's groundwork.[57] The defendant, Jimmy Hoffa, after being convicted of attempting to bribe jurors, sought to have his conviction thrown out because the government had placed an informant in his attaché.[58] Hoffa argued that the informant's failure to disclose that he was reporting to federal agents violated his Fourth Amendment rights.[59] The Court disagreed and held that Hoffa's "misplaced confidence that [the informant] would not reveal his wrongdoing" did not implicate Fourth Amendment rights.[60] It stated, "The risk of being overheard by an eavesdropper or betrayed by an informer . . . . is the kind of risk we necessarily assume whenever we speak."[61]

The Court elaborated its basis for deciding *Hoffa* in 1969 in *United States v. White*.[62] As in *Hoffa*, the petitioner in *White* had been convicted based upon evidence gathered by a government informant.[63] But the informant in *White* was also wearing an audio recording device.[64] Government agents heard the petitioner's conversations with the informant as they occurred, and they testified regarding the substance of those conversations at trial.[65]

The Supreme Court allowed the testimony.[66] The Court cited *Hoffa*, left intact by *Katz*, for the proposition 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."[67] It stated that a criminal "must realize and risk that his companions may be reporting to the police" and that "if he has no doubts, or allays them, or risks what doubt he has, the risk is his."[68] Similarly citing

---

56 *See* Kerr, *Third-Party Doctrine*, *supra* note 53, at 567-68.
57 Hoffa v. United States, 385 U.S. 293 (1966).
58 *Id.* at 295-96.
59 *Id.* at 300.
60 *Id.* at 302-03.
61 *Id.* at 303 (quoting Lopez v. U.S. 373 U.S. 427, 465 (1963)).
62 United States v. White, 401 U.S. 745, 749-52 (1971).
63 *Id.* at 746-47.
64 *Id.*
65 *Id.*
66 *Id.* at 752.
67 *Id*. at 749 (quoting Hoffa v. U.S. 385 U.S. 293, 302 (1966)).
68 United States v. White, 401 U.S. 745, 752 (1971).

Hoffa, the Court stated that there is no constitutional violation when an informer testifies in open court as to conversations with the accused.[69]

2. The Court Applies the Third-Party Doctrine to Business Records

In a series of cases in the 1970s, the Supreme Court established that persons who communicate information to businesses cannot rely on Fourth Amendment principles to protect that information from compelled production.[70] By 1979, when the Court decided the last of these cases, *Smith v. Maryland*, it had enshrined as law the principle that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[71]

Couch v. United States, the first of these cases, dealt with an Internal Revenue Service subpoena of taxpayer documents in an accountant's possession.[72] The petitioner argued that production of the documents was a violation of her Fifth Amendment right against self-incrimination.[73] The petitioner claimed that, because she owned the documents, a Fifth Amendment privilege ought to protect them from compelled production.[74] Under this same reasoning, she made a Fourth Amendment claim.[75] The Court addressed the Fourth Amendment argument with only one paragraph.[76] It was enough space to hold that, because an accountant has the responsibility to disclose clients' documents when filing tax returns, the petitioner had no reasonable expectation of privacy in documents she had shared with her accountant.[77]

In 1976, in *United States v. Miller*, the Court expanded its holding in *Couch* by refusing to recognize a reasonable expectation of privacy in a person's bank account records.[78] The Court considered whether a

---

69 *Id.* at 751 (citing Hoffa v. United States, 385 U.S. 293, 300-303 (1966)).

70 *See* Smith v. Maryland, 442 U.S. 735, 745 (1979); United States v. Miller, 425 U.S. 435, 443-44 (1976); Couch v. United States; 409 U.S. 322, 329 (1973).

71 *Smith*, 442 U.S. at 743-44.

72 *Couch*, 409 U.S. at 323.

73 *See id.* at 325.

74 *See id.*

75 *See id.* at 325 n.6, 335-36.

76 *Id.* at 335-36.

77 *Id.*

78 *See* United States v. Miller, 425 U.S. 435, 440 (1976) (ruling that a person's bank records are the bank's business records, not the person's private papers).

subpoena of those records, combined with a statutory recordkeeping requirement, was the functional equivalent of a search and seizure of a depositor's private papers.[79] Addressing the respondent's argument that the records were "merely copies of personal records that were made available to the banks for a limited purpose and in which [the respondent had] a reasonable expectation of privacy," the Court looked at "the nature of the particular documents sought to be protected in order to determine whether there [was] a legitimate 'expectation of privacy' concerning their contents."[80] The records in question were checks, deposit slips, and financial statements.[81] The Court noted that the information in these documents was voluntarily disclosed to the bank and its employees.[82] The Court, citing *White*, said, "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[83] It then held that, even assuming that the bank, in keeping records and complying with a subpoena, was acting as a government agent, no Fourth Amendment rights were violated when the government compelled information that was conveyed to a third party such as the bank.[84]

The Court next applied the doctrine to electronic communications in *Smith v. Maryland*.[85] There, the petitioner had been convicted of robbery.[86] After the robbery occurred, the victim received threatening phone calls from a caller who identified himself as the person who had robbed her.[87] To verify that the petitioner was the perpetrator, the police requested that the telephone company install a pen register to record the numbers the petitioner dialed.[88] After the pen register was installed, the petitioner called the victim again, giving the police evidence that he was the robber.[89]

The petitioner sought to have the fruits of the pen register excluded, claiming a reasonable expectation of privacy in the numbers

---

79 *Id.* at 441-42.
80 *Id.* at 442.
81 *Id.* at 438.
82 *Id.* at 442.
83 *Id.* at 443 (citing U.S. v. White, 401 U.S. 745, 751-52 (1971)).
84 United States v. Miller, 425 U.S. 435, 443-44 (1976) (citations omitted).
85 Smith v. Maryland, 442 U.S. 735 (1979).
86 *Id.* at 737-38.
87 *Id.* at 737.
88 *Id.*
89 *Id.*

he dialed from his own home telephone.[90] The Court rejected the argument, claiming that it was "too much to believe" that people expected that the numbers they dialed would remain private.[91] Telephone subscribers know that the numbers they dial are communicated to the telephone company because they see those numbers on their phone bill and they know that pen registers can be used to identify harassing callers.[92] Because telephone customers know that the numbers they dial are communicated to telephone companies, and because there is no legitimate expectation of privacy in information turned over to a third party, the Court held that use of a pen register without a warrant was not a violation of the Fourth Amendment.[93]

Taken together, *Couch*, *Miller*, and *Smith* are often cited as support for the proposition that the third-party doctrine applies to a business's records of a person's electronic communications.[94] Assuming that proposition is correct, cloud-based document storage seems to fall squarely within the third-party doctrine. This Article addresses the application and effect of the doctrine on cloud-based document storage described in Part II.A.

D. *The SCA: A Statutory Replacement for the Fourth Amendment*

Despite the third-party doctrine, government officials must meet a minimum process requirement to compel production of certain electronic records. This requirement stems from the Electronic Communications Privacy Act (ECPA) and the Stored Communications Act (SCA), both of which were enacted in 1986.[95] Congress enacted the

---

[90] *Id.* at 737, 741-43.

[91] Smith v. Maryland, 442 U.S. 735, 742-43 (1979).

[92] *Id.*

[93] *Id.* at 738, 743-46.

[94] *See, e.g.*, Guest v. Leis, 255 F.3d 325, 335-36 (6th Cir. 2001) (ruling that subscriber information, disclosed to system operators over the a computer network, lacks Fourth Amendment protection); Kerr, *Third-Party Doctrine*, *supra* note 53, at 573 ("Internet services are third-party services, raising the prospect that the Fourth Amendment may apply only modestly to internet communications."); Amanda Yellon, Comment, *The Fourth Amendment's New Frontier: Judicial Reasoning Applying the Fourth Amendment to Electronic Communications*, 4 J. BUS. & TECH. L. 411, 433 (2009) ("Under the Court's third party doctrine, the e-mail user has assumed the risk 'in revealing his affairs to another, that the information will be conveyed by that person to the Government.'") (quoting United States v. Miller, 425 U.S. 435, 442-43 (1976)); Lawless, *supra* note 53, at 33-34 (asserting that internet search records fall within the third-party doctrine's scope).

[95] *See* 18 U.S.C. §§ 3121-3127 (2006); 18 U.S.C. §§ 2701-2712 (2006).

ECPA as an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968[96] with the intent to to modernize the nation's privacy protections regarding electronic communications.[97]

In furtherance of that goal, the SCA prohibits electronic communication service providers and remote computing service providers from disclosing a subscriber's communications, with certain exceptions.[98] This prohibition extends to disclosure to the government, except when required by a warrant or when the subscriber has a good faith belief that disclosure is necessary to prevent a dangerous situation.[99]

The SCA also establishes that governmental entities may compel production of the contents of electronic communications.[100] Under § 2703 of the SCA, the government must satisfy different standards to compel disclosure of different types of communications.[101] The types of production that are relevant to this Article, however, are limited.

The SCA differentiates between types of communications service providers.[102] The statute refers to both electronic communications service (ECS) providers and remote computing service (RCS) providers.[103] Identifying the protections that the SCA creates for a particular communication starts with identifying the classification of the provider that facilitates that communication.[104]

This Article considers only RCS providers for two reasons. First, cloud computing service providers fit nicely within the SCA's definition of an RCS provider.[105] Second, this Article argues for a limited evidentiary privilege only between cloud-based storage providers and users.[106] To the extent that a person utilizes a cloud-based document storage service for communication with third parties other than the service provider, the proposed privilege would not apply. Because

---

96 Omnibus Crime Control and Safe Streets (Federal Wiretapping) Act of 1968, 18 U.S.C. §§ 2511-2522; *see* S. REP. No. 99-541, at 1 (1986).

97 *See* S. REP. No. 99-541, at 1.

98 18 U.S.C. § 2702 (2006).

99 18 U.S.C. § 2702(b)(8) (2006).

100 18 U.S.C. § 2703 (2006).

101 *Id.*; Kerr, *User's Guide to the SCA*, *supra* note 19, at 1218-19.

102 Kerr, *User's Guide to the SCA*, *supra* note 19, at 1213-14.

103 *Id.* at 1214.

104 *Id.* at 1213.

105 *See* 18 U.S.C. § 2711(2) (2006) (defining RCS as "the provision to the public of computer storage or processing services by means of an electronic communications system").

106 *See infra* Part III.

ECS explicitly involves communication from one party to another,[107] ECS appears to fall clearly outside of the scope of both the proposed privilege and the scope of this Article.

The SCA establishes that the government may compel an RCS provider to produce the contents of an electronic communication[108] if the government obtains a warrant,[109] an administrative subpoena,[110] or a court order.[111] Of those three methods, this Article examines only the court order described in 18 U.S.C. § 2703(b)(1)(B)(ii).[112]

To procure such an order, the government must show "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication . . . are relevant and material to an ongoing criminal investigation.[113] The "specific and articulable" language is the language the Supreme Court used in *Terry v. Ohio* to describe the threshold factual evidence necessary to satisfy the Fourth Amendment's requirement that a seizure be reasonable, not the Fourth Amendment's probable cause requirement.[114]

The specific and articulable facts threshold is lower than probable cause—the threshold required by the Fourth Amendment[115]—and some commentators have described it as far lower than the probable cause requirement.[116] This Article examines the implication of court

---

107 *See* 18 U.S.C. § 2510(15) (2006) (ECS includes "any service which provides to users thereof the ability to send or receive wire or electronic communications").

108 For the remainder of this comment, the term "electronic communication" will have the definition assigned to it in 18 U.S.C. § 2510(12) (" 'electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce . . ."). Electronic communications between a user and the computers of a cloud-based document storage provider (but not between the user and any third party) fall within this definition.

109 18 U.S.C. § 2703(b)(1)(A) (2006).

110 18 U.S.C. § 2703(b)(1)(B)(i) (2006).

111 18 U.S.C. § 2703(b)(1)(B)(ii) (2006).

112 *See id.* This Article will only focus on court orders because warrants can only be procured with a showing of probable cause before a neutral magistrate, and administrative subpoenas are outside of the scope of this Article.

113 18 U.S.C. § 2703(d) (2006).

114 *See* Terry v. Ohio, 392 U.S. 1, 21-22 (1968).

115 U.S. CONST. amend IV.

116 *See, e.g.*, Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 816 (2003) ("[T]he statutory protections fall considerably short of the traditional rules."); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1150 (2002) [hereinafter Solove, *Digital Dossiers*] ("As warrants supported by probable cause are replaced

orders supported by less than probable cause, applied to cloud-based document storage.

II. ANALYSIS

Before further discussing the limited evidentiary privilege's relationship to documents stored online, it is necessary to first examine general Fourth Amendment doctrine in the context of cloud-based document storage. Section A examines how Fourth Amendment cases concerning email affect the application of the third-party doctrine to cloud-based document storage. Although some commentators have disparaged the third-party doctrine,[117] Section B examines some arguments that have been made in its favor, as a means of ruling out the wholesale abandonment of the doctrine. Section C briefly discusses the similarities between some documents that are stored online and traditional papers and effects.

A. *Application of the Third-Party Doctrine to Cloud-Based Document Storage*

The third-party doctrine broadly stands for the proposition that a person has no legitimate expectation of privacy in information he shares with a third person.[118] *Smith*, *Miller*, and *Couch* established that the third-party doctrine prevents some legitimate expectations of privacy even when the third party is a business—such as a bank or telephone company—and the information it holds is presumed private.[119] The implication of the doctrine seems to be that where a person transmits electronic communications over a third person's servers, the government may approach the third person to gain access to the documents without implicating the Fourth Amendment.[120]

Two United States Circuit Courts, however, have argued that e-mail communications fall outside of the scope of the third-party doc-

---

by subpoenas and court orders supported by 'articulable facts' that are 'relevant' to an investigation, the role of the judge in the process is diminished to nothing more than a decorative seal of approval.").

117 *See* Kerr, *Third-Party Doctrine*, *supra* note 53, at 563 n.5.

118 *See* discussion *supra* Parts I.C.1-2.

119 *See* discussion *supra* Part I.C.2.

120 *See* Derek Constantine, *Cloud Computing: The Next Great Technological Innovation, The Death of Online Privacy, or Both?*, 28 GA. St. U. L. Rev. 499, 513-16 (2012) (discussing the application of the third-party doctrine to cloud computing).

trine.[121] Both courts considered the similarities between e-mail and postal mail.[122] In *United States v. Warshak*, the Sixth Circuit Court of Appeals analogized the Supreme Court's dicta in *Katz*—where the Court mentioned the "vital role that the public telephone has come to play in private communications"—to the modern prevalence of e-mail.[123] Following this reasoning, the Sixth Circuit refused to abandon Fourth Amendment protection for e-mail, arguing, "As some forms of communication begin to diminish, the Fourth Amendment must recognize and protect nascent ones that arise."[124] It held that the Fourth Amendment required the government to procure a search warrant before compelling an e-mail service provider to turn over the contents of a subscriber's e-mail.[125] It also held that, to the extent that the SCA allows otherwise, the SCA is unconstitutional.[126] The analogy between e-mail and regular mail brings the oft-cited content-envelope distinction into focus.[127] The *Warshak* court analogized e-mail to postal mail, calling e-mail the "technological scion" of postal mail.[128] Under this analogy, the text in the body of the e-mail might be protected, but not other information, like the recipient's e-mail address.[129]

It is not automatically clear, however, that the content-envelope distinction, or even the analogy with postal mail, is relevant to cloud-based document storage. Some documents that are stored on Internet servers are not communications, and instead are personal documents such as spreadsheets, pictures, contracts, and books. These documents are shared with the cloud-based storage provider for storage purposes, giving the user access to the documents through his mobile phone, laptop, or iPod.[130] Although the documents are communicated

---

121 *See* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010); *see also* United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2007).

122 *Warshak*, 631 F.3d at 285-86; *Forrester*, 512 F.3d at 511.

123 *Warshak*, 631 F.3d at 284 (quoting Katz v. United States, 389 U.S. 347, 352 (1967)).

124 *Id.* at 286.

125 *Id.* at 288.

126 *Id.*

127 *See generally*, Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2112 (2009) (describing longstanding Supreme Court Fourth Amendment precedent as recognizing a distinction between information that is exposed on the outside of a mailed package, for which there is no reasonable expectation of privacy, and the contents of the package, for which there is a reasonable expectation of privacy).

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

129 *See* Tokson, *supra* note 127, at 2126-27.

130 *See supra* Part I.A.

to the provider, the provider in this case is the recipient, not an intermediary.[131]

In the case of a compelled production pursuant to § 2703(b)(1)(B)(ii) of the SCA, the recipient of the communication, the cloud-based storage provider, is presented with a court order, not an intermediary party.[132] Even in the case of letter mail, once the recipient receives the mail, the sender loses, pursuant to the third-party doctrine, all reasonable expectations of privacy in the letter's contents.[133] The sender cannot vicariously enforce the recipient's Fourth Amendment right to demand a warrant.[134] Thus, it seems that a bar to the normal operation of the third-party doctrine is a prerequisite of Fourth Amendment protection for cloud-based document storage.

B. *The Third-Party Doctrine Serves Critical Functions in Fourth Amendment Law*

This Article does not argue for the abandonment of the third-party doctrine. Instead, it recognizes that, although the third-party doctrine is an important part of Fourth Amendment doctrine, it may lead to unreasonable results when applied to modern Internet storage services.[135]

In 2009, Professor Orin Kerr penned a defense of the third-party doctrine.[136] Kerr recognized that the doctrine is technologically neutral because it corrects a substitution effect whereby criminals use third parties to hide previously public acts, and that it preserves clarity in Fourth Amendment rules.[137] Kerr also addressed some of the doc-

---

131 *See supra* Part I.A.

132 *See* 18 U.S.C. § 2703(b)(1) (2006) ("A governmental entity may require *a provider of remote computing service* to disclose the contents of any wire or electronic communication to which this paragraph is made applicable . . . .") (emphasis added), *invalidated by Warshak*, 631 F.3d 286 (2010).

133 *See* Kerr, *Third-Party Doctrine*, *supra* note 53, at 582 ("The sender has Fourth Amendment rights in the letter during transmission, but once it arrives at its destination, those rights disappear." (citing United States v. Villarreal, 963 F.2d 770, 774 (5th Cir. 1992))).

134 Rakas v. Illinois, 439 U.S. 128, 133-34 (1978) (quoting Alderman v. United States, 394 U.S. 165, 174 (1969)).

135 The unreasonable result is the decreasing ability of the Fourth Amendment to protect individual's papers and effects from warrantless government search and seizure. *See* discussion *infra* Part II.C.

136 *See* Kerr, *Third-Party Doctrine*, *supra* note 53, at 561.

137 *Id.* at 564-65.

trine's critics, claiming that problems with the doctrine are more about form than substance.[138] Kerr then argued that critics often overlook the many alternatives to Fourth Amendment protections of privacy, such as statutory protections and common law privileges.[139]

Kerr's argument carries force. It is true that the third-party doctrine is technologically neutral, although this can be seen as both a cost and a benefit.[140] Kerr writes, "Just as the Fourth Amendment should protect that which technology exposes, so should the Fourth Amendment permit access to that which technology hides."[141] This argument recognizes that more of what people do is being done on the Internet. To the extent that the third-party doctrine ignores this fact, however, the net result may be that an increasing amount of private life loses Fourth Amendment protections.

Kerr addressed the opposite of this effect when he argued that criminals may use third parties to hide what would otherwise be public acts.[142] This substitution effect increases as technological advances allow criminals to commit more of their criminal acts in private.[143] Kerr argued that the third party doctrine allows the police to cancel out the substitution effect by gleaning information from the third party.[144]

A number of scholars have leveled criticism at the third-party doctrine.[145] Kerr addresses some of these criticisms by admitting that, as the Supreme Court has explained it, the third-party doctrine makes little sense.[146] The Court has held that government searches of third parties fail to meet *Katz*'s objective test.[147] According to Kerr, the appropriate way to view the rule is as failure to meet *Katz*'s subjective test.[148] Viewing the doctrine in this light, Kerr argues that the third-party doctrine raises the issue, "When does a person's choice to dis-

138 *Id.* at 565, 588-90.

139 *Id.* at 595-600.

140 *See id.* at 580 (quoting Olmstead v. United States, 277 U.S. 438, 474 (Brandeis, J., dissenting), *overruled by* Katz v. United States, 398 U.S. 347 (1967)).

141 *Id.*

142 *See* Kerr, *Third-Party Doctrine*, *supra* note 53, at 576.

143 *See id.* at 580.

144 *See id.* at 580-81.

145 *See id.* at 563 n.5.

146 *See id.* at 588.

147 *See* United States v. White, 401 U.S. 745, 752-53 (1971) (holding that society will not recognize a subjective expectation of privacy held in information that is shared with third parties).

148 *See* Kerr, *The Third-Party Doctrine*, *supra* note 53, at 588-89.

close information to a third party constitute consent to a search?"[149] Framing the doctrine in these terms, however, is arguably just as suspect as the Court's application in *Katz* and the business records cases. A disclosure to a third person cannot reasonably be seen as consent to a search conducted by the government. The thrust of Kerr's point, however, may be that an individual who shares information is not consenting to a governmental search, but that he is consenting to share his right to exclude. The first party no longer has exclusive possession of the information, meaning that he no longer has the power to maintain its privacy.[150]

Of course, the information may be protected by statute or privilege, and Kerr devotes a section to discussing substitutes for the Fourth Amendment.[151] This Article has already examined the protections afforded electronic documents by the SCA.[152] Additionally, communications with some third parties, such as accountants and lawyers, may be privileged, and thus protected from compelled disclosure.[153] This Article argues in Part III that the Supreme Court should recognize such a privilege in electronic documents that are shared with cloud-based document storage services.

Kerr's defense of third-party doctrine has elicited its own criticism.[154] The purpose of this Section, however, is not to parse the entire landscape of the discourse, but to show that the third-party doctrine is arguably a necessary doctrine. If the doctrine is to survive, however, it should not do so at the expense of constitutional protection for an individual's digital papers and effects.

---

149 *Id.* at 588.

150 *See id.* at 590; Rakas v. Illinois, 439 U.S. 128, 133-34 (1978) (holding that "Fourth Amendment rights are personal rights which, like some other constitutional rights, may not be vicariously asserted.") (quoting Alderman v. United States, 394 U.S. 165, 174 (1969)).

151 *See* Kerr, *Third-Party Doctrine*, *supra* note 53, at 595-99 (naming statutory protections, common law privileges, and rights of the third parties themselves as substitutes for the Fourth Amendment).

152 *See supra* Part I.D.

153 *See* Kerr, *Third-Party Doctrine*, *supra* note 53, at 596-98.

154 *See*, Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 BERKELEY TECH. L.J. 1199-1201 (2009); Erin Murphy, *The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239-41 (2009).

C. *Cloud-Based Document Storage Includes Several Types of Documents that Intuitively Appear to Be a Person's Papers and Effects*

This Section briefly discusses potential effects of the third-party doctrine on types of documents that intuitively seem like they would fall under the Fourth Amendment's protection of a person's papers and effects. This Article has already outlined many of the current uses for cloud-based document storage.[155] Users of these services are apt to keep fewer physical copies of documents in their homes and keep more documents in cloud-based document storage providers' servers.[156]

The many types of documents that are subject to this transfer include: photographs, records, books, magazines, multimedia, personal planners, and more. These types of documents are inherently like those that people normally keep in their homes or businesses. People have bookshelves, photo albums, filing cabinets, drawers, and safes primarily to store these types of documents. It is worth noting that, while these documents are of a kind that people might intuitively call their papers and effects, certain items cannot be stored online.[157]

A person cannot store physical objects in the cloud. If a criminal has physical evidence on his clothing, a weapon that he used in a crime, or a shoe sole that carries a telltale pattern, he cannot transfer these objects to a computer server. The things that are used as evidence in many crimes will be where they have always been: In the physical world. Of course, it would be naive to think that no evidence of crime will be stored in cloud-based document storage, but many of the documents that are migrating onto the Internet are personal effects.

If society begins to store these documents primarily on the Internet—their photographs, calendars, diaries, and so on—and if the third-party doctrine precludes Fourth Amendment protection for these documents, the results will be absurd: The types of objects that are generally less likely to be evidence in a crime, and more likely to

---

155 *See supra* Part I.A.

156 *See* Horrigan, *supra* note 3, at 1-2 (asserting that based on the survey research that "[s]ome 69% of online Americans use webmail services, store data online" because they prefer its ease and convenience, ability to access their data from whatever computer they are using, and sharing information in cyberspace).

157 *See id*. at 4-5.

be personal and sensitive, will become easier for the government to search and seize. At the same time, physical evidence, generally more likely to be relevant to a criminal investigation, will continue to be subject to the Fourth Amendment requirement of a warrant, authorized by a neutral magistrate and supported by probable cause.

III. ARGUMENT

Cloud-based document storage is by all accounts becoming widely adopted.[158] Throughout the history of Fourth Amendment jurisprudence, scholars and judges have argued that the Fourth Amendment must recognize when the government's ability to take advantage of technology outpaces constitutionally protected privacy interests.[159] This Part argues that the flexibility of the Fourth Amendment should allow courts to create an evidentiary privilege protecting cloud-based document storage. However, because the Federal Rules of Evidence enacted by Congress allow for the creation of new privileges, this Article's recommendation should find support from even those who would prefer that courts abstain from novel creations of law.

This Part assumes at the outset that the Fourth Amendment is flexible enough to protect privacy interests by recognizing changes in technology. Section A argues, generally, that the Fourth Amendment compels an exemption to the third-party doctrine for certain types of cloud-based document storage. Part B argues, specifically, that the result of such an exemption resembles a limited evidentiary privilege.

---

158 *See id*. at 1-2.

159 *See*, Kyllo v. United States, 533 U.S. 27, 34-36, 40 (2001) (classifying as a search the viewing of a private home's outer walls with a camera capable of seeing heat energy emanating from within the home, even though the police did not enter the curtilage or home); Katz v. United States, 389 U.S. 347, 352 (1967) (refusing to apply the Fourth Amendment so narrowly as to ignore the "vital role" the public telephone played in society); Olmstead v. United States, 277 U.S. 438, 473-74 (1928) (Brandeis, J., dissenting), *overruled by* Katz v. United States, 389 U.S. 347 (1967) ("In the application of a Constitution . . . our contemplation cannot be only of what has been but of what may be . . . . Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court . . . ."); United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010) ("[E]mail requires strong protection under the Fourth Amendment; otherwise, the Fourth Amendment would prove an ineffective guardian of private communication . . . ."); Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1011-12 (2010) (arguing that application of the Fourth Amendment to the Internet may require the creation of new rules in order to serve the same functions as the old rules).

Part C concludes by acknowledging another potential solution, a statutorily created privilege, and explains why such a privilege is inferior.

A. *The Fourth Amendment Compels the Protection of Some Documents that a Person Stores Online*

The Fourth Amendment, and the doctrines that arise in its applications, must be flexible enough to serve their intended function in the modern world.[160] The primary function of the Fourth Amendment is to protect individuals' privacy and security from unreasonable invasion by the government.[161] That protection is strongest in the home,[162] and it should apply with equal force when people store in the cloud the documents that used to be stored in their home.

A person's home is more than just a place or a dwelling house. People keep their belongings in their homes. When a person installs a safe in his home, or locks his door when he leaves, it is his belongings that he intends to keep safe. A person's belongings, furthermore, are not always physical objects.

The pictures on a person's camera belong to him, as do the medical records he has scanned into his computer. But those documents are less secure and less useful in his home than they could be in a virtual home that he leases from a cloud-based document storage company.[163] Thus, the physical home, which the Fourth Amendment endeavors to protect above all else, is not where the "rational maximizer" would choose to keep those belongings. The Internet server, which provides remote access and backup systems to protect against file loss,[164] is arguably a better home for a person's most important documents. The Fourth Amendment must be flexible enough to allow

---

160 *See* Lopez v. United States, 373 U.S. 427, 464 (1963) (citing Ohio v. Price, 364 U.S. 263, 272 (1960)).

161 *See* United States v. Warshak, 631 F.3d 266, 283-84 (citing Camara v. Mun. Ct. of S.F., 387 U.S. 523, 528 (1967), Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 613-14 (1989)).

162 *See* Kyllo v. United States, 533 U.S. 27, 31 (2001) (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)) ("'At the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'").

163 *See* Martin, *supra* note 4, at 294 (listing advantages and benefits of cloud-computing such as enhanced security, maintenance, possibilities of user cooperation and collaboration).

164 *See Any File, Anywhere*, MICROSOFT, http://windows.microsoft.com/en-US/skydrive/any-file-anywhere (last visited Feb. 13, 2013).

courts to recognize the increasing role that the Internet is playing in securing a person's papers and effects.[165]

The test for whether a Fourth Amendment violation has occurred has two parts.[166] First, has the person exhibited a subjective expectation of privacy with regard to the thing searched?[167] Second, is that expectation of privacy one that society is prepared to recognize as reasonable?[168]

Regarding the first, subjective inquiry, documents stored with cloud-based document storage companies are often protected by passwords.[169] This alone is a manifestation of an expectation of privacy.[170] Regarding the objective inquiry, the third-party doctrine normally precludes as unreasonable any expectation of privacy in information that is shared with a third person.[171] This is a case, however, of the exception swallowing the rule. The third-party doctrine, as an exception to the Fourth Amendment, will eat away at the ability of the Fourth Amendment to protect individuals' papers and effects.[172]

The fact that documents have been shared with a third party does not always preclude constitutional protection. Relationships protected by privilege allow for communication between parties without the intendant application of the third-party doctrine.[173] Courts should recognize such a privilege for cloud-based document storage.

---

165 *See* Lopez v. United States, 373 U.S. 427, 464 (1963) (citing Ohio v. Price, 364 U.S. 263, 272 (1960)).

166 *See Warshak*, 631 F.3d at 284 (citing California v. Ciraolo, 476 U.S. 207, 284 (1986)).

167 *Id.*

168 *Id.*

169 David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2217 (2009).

170 *See* United States v. Buckner, 473 F.3d 551, 554 (5th Cir. 2007) (quoting Trulock v. Freeh, 275 F.3d 371, 403 (4th Cir. 2001) ("By using a password, [the Plaintiff-Appellant] affirmatively intended to exclude . . . others from his personal files." Thus, he had a reasonable expectation of privacy in the password-protected computer files.)).

171 *See supra* Parts I.C.1-2.

172 *Cf.* Solove, *Digital Dossiers*, *supra* note 116, at 1150 ("The current statutory regime that has attempted to fill the void created by the judicial evisceration of the Fourth Amendment is inadequate because it results in the de facto watering down of the warrant and probable cause requirements of the Fourth Amendment.").

173 *See* Kerr, *The Third-Party Doctrine*, *supra* note 53, at 595-96.

B. *Courts Should Recognize an Evidentiary Privilege Existing Between Cloud-Based Document Storage Providers and Users*

Communications between an attorney and his client are privileged.[174] Thus, the disclosure, by the client and to the attorney, does not fall within the scope of the third-party doctrine.[175] Such a privilege should be recognized as existing between a cloud-based document storage provider and a user. The privilege model, applied to cloud-based document storage, would accomplish the goal of protecting a person's private, cloud-stored documents while preserving the integrity and purpose of the third-party doctrine in most cases.

The recognition of new privileges is not unprecedented.[176] Federal Rule of Evidence 501, which allows for the adoption of new privileges,[177] states that "The common law—as interpreted by United States courts in the light of reason and experience—governs a claim of privilege unless any of [the United States Constitution, a federal statute, or rules prescribed by the Supreme Court] provides otherwise."[178] Evidentiary privileges are generally disfavored:

> [T]he public . . . has a right to every man's evidence. When we come to examine the various claims of exemption, we start with the primary assumption that there is a general duty to give what testimony one is capable of giving, and that any exemptions which may exist are distinctly exceptional, being so many derogations from a positive general rule.[179]

For the same reason, privileges are construed narrowly.[180] Moreover, narrow construction is desirable for a privilege protecting cloud-based document storage. The privilege should only apply where:

---

174 *See, e.g.*, Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).

175 *See* Kerr, *The Third-Party Doctrine*, *supra* note 53, at 597 ("As a practical matter, the privilege trumps the third-party doctrine.").

176 *See, e.g.*, Jaffee v. Redmond, 518 U.S. 1, 15 (1996) (recognizing a psychotherapist-patient privilege).

177 *Jaffee*, 518 U.S. at 8.

178 FED. R. EVID. 501.

179 United States v. Bryan, 339 U.S. 323, 332(1950) (*quoting* 8 J. WIGMORE, EVIDENCE § 2192 (3d ed.)).

180 *See Jaffe*, 518 U.S. at 19 (Scalia, J., dissenting) (citing United States v. Zolin, 491 U.S. 554, 568-570 (1989)); Trammel v. United States, 445 U.S. 40, 50 (1980)) ("Adherence to [Wigmore's] principle has caused us . . . . to construe narrowly the scope of existing privileges.").

1) a sufficient level of privacy has been maintained,
2) the documents have not been shared with a party outside of the privileged relationship,
3) the contract establishing the relationship is consistent with a subjective expectation that the documents will be private, and
4) the user, not the provider, is asserting the privilege.

Before courts will recognize a privilege, the privilege must further a "public good transcending the normally predominant principle of utilizing all rational means for ascertaining truth."[181] Protecting cloud-based document storage furthers such a public good: The preservation of Fourth Amendment protections for individuals' papers and effects. The privilege will accomplish the narrow goal of extending constitutional protection to documents that clearly should receive such protection while preserving the important third-party doctrine.

An alternative to a judicially recognized privilege is a statutorily created privilege. That alternative has flaws, however. Section C examines some hypothetical benefits of the judicially recognized privilege over a statutorily created one.

C. *A Judicially Recognized Privilege Protecting Cloud-Based Document Storage Is Preferable to a Statutorily Created One*

Before comparing the judicially created privilege and a statutorily created privilege, it is worthwhile to remember that the courts' authorization to create new privileges is statutorily derived.[182] Thus, the creation of a new privilege, under Rule 501, is not judicial action without congressional approval. Additionally, there are benefits to judicial creation of a privilege for cloud-based document storage.

First, and most importantly, protection for cloud-based document storage is arguably constitutionally mandated.[183] Judicial recognition of the privilege would solve the problem of too little protection for documents stored online by recognizing that certain online documents are constitutionally protected. A statutory remedy would leave open

---

181 *See Jaffee*, 518 U.S. at 9 (internal citations omitted).
182 FED. R. EVID. 501.
183 *See supra* Part III.A.

important questions about the application of the Fourth Amendment to cloud-based document storage.

Second, a court, in determining whether to apply the privilege, has the authority not to recognize a judicially created privilege when it does not further a "public good transcending the normally predominant principle of utilizing all rational means for ascertaining truth."[184] Courts should have the flexibility to identify proper applications of the privilege, and the common law provides that.[185] With so many potential providers of cloud-based document storage services, and the fast pace at which these services evolve, flexibility is an asset for judges seeking to enforce the privilege.

Finally, a statute creating the privilege is likely to become outdated before Congress is able to revise it. The SCA is an example of this predicament. The SCA was first enacted in 1986[186] and modern critics claim that it no longer fits the way society uses computer networks.[187] A judicially created privilege, however, can be applied "by United States courts in the light of reason and experience."[188]

CONCLUSION

Certain documents, those stored online by users of cloud-based document storage companies, are analogous to documents stored in safe locations in a person's home or office. These documents are deserving of the full protection of the Fourth Amendment, including the requirement that the government attain a warrant based upon probable clause prior to conducting a search. Currently, because of the third-party doctrine, the application of the Fourth Amendment to these documents is unclear. The SCA establishes a minimum process requirement before the government can search documents stored online, but the requirement falls far short of the Fourth Amendment.

To correct this, either Congress or the courts can act. The courts can recognize a privilege under Rule 501 of the Federal Rules of Evidence that applies between cloud-based document storage providers

---

184 *Jaffee*, 518 U.S. at 9 (internal citations omitted).

185 Elisha E. Weiner, *Price and Privilege: While Litigation Financing Offers Hope to Plaintiffs with Limited Resources, and Exchange of Confidential Information with the Financer May Waive the Attorney-Client Privilege*, 35 L.A. LAW. 20, 23 (2012).

186 18 U.S.C.A. § 2701 (2002).

187 *See, e.g.*, Kerr, *User's Guide to the SCA*, *supra* note 19, at 1229-31.

188 FED. R. EVID. 501 advisory committee notes.

and users. Alternatively, Congress can act to create such a privilege. Either of these options would ensure that users had a reasonable expectation of privacy, but the judicially created privilege would be flexible enough to only be applied where needed.

Regardless of the mechanism used, cloud-based document storage should receive Fourth Amendment protection, despite the fact that it requires, by its nature, communications occurring between two or more parties. Society long ago solved the problem of protecting important communications from compelled disclosure—it developed the law of privilege. Certain documents, certain papers and effects, are important enough to receive that protection. Cloud-based document storage is important enough to be privileged.