Up in the Air: Clarifying Cloud Storage Protections

ERIK C. SHALLMAN*

INTRODUCTION

Imagine you possess some handwritten documents that you would like to keep from prying eyes. You purchase a fireproof safe and install it in your den. Only you and the safe manufacturer know the code to the safe, so you feel comfortable locking away the documents and going about your business. You know that even if law enforcement officers somehow coerced the manufacturer into giving them the code, they could not simply sneak into your home and open the safe because the Fourth Amendment requires the officers to obtain a warrant based on probable cause before searching your home.¹

Eventually, you have too many files to fit in your safe, let alone your den. You contract with a storage company to store the documents in a warehouse accessible only to you. You trade away the security of keeping the documents in your home for the comfort of an empty living room. But still, the documents are in a closed container, and you know the police must get a warrant to search your storage unit.²

As time goes by, you embrace the digital world and no longer use handwritten ledgers. Instead, you store all of your documents as text, spreadsheet, or image files on your laptop’s hard drive.³ For good measure, you scan your old documents into the computer and get rid of the storage unit. The entirety of your document collection now lives inside a laptop in your den. Your information is back in your home—a location historically given the most protection by the Fourth Amendment.⁴ Absent a showing of probable cause, the contents of your house are safe from the prying eyes of

---

¹ U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

² See United States v. Johnson, 584 F.3d 995, 1001 (10th Cir. 2009) (“People generally have a reasonable expectation of privacy in a storage unit, because storage units are secure areas that ‘command a high degree of privacy.’” (quoting United States v. Salinas-Cano, 959 F.2d 861, 864 (10th Cir. 1992)).


⁴ Kyllo v. United States, 533 U.S. 27, 31 (2001) (“With few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no.”).
As it happens, a mishap occurs, and you lose some of the data stored on your hard drive. Perhaps the cause is a stray cup of coffee, or a trip over a power cord, or simply a manufacturing defect. Whatever the cause, you suddenly realize that because you store your documents on a single hard drive, the mishap could have cost you your entire document library. Further, even if you were to back up your data to an external hard drive at home, there would still be a risk that a fire, earthquake, or other natural disaster would destroy your data. Fortunately, the technology sector recognized this risk, and multiple companies now provide “cloud storage” solutions. These companies store and backup personal files on remote servers, often giving you the ability to synchronize both personal and work-related files across multiple computers and devices. Individual consumers often use these cloud-based services, but businesses increasingly utilize the cloud for document sharing and to streamline group projects.

You decide it is time to adopt the cloud, so you download and install Dropbox, a popular cloud storage service. Every time you save a document to the Dropbox folder on your laptop, the file is automatically, safely, and securely copied and whisked off into the cloud. Dropbox’s corporate servers retain a copy of all your files that are readily accessible from any Internet-connected computer.

You feel secure. You presume Dropbox’s servers are similar to your old third-party storage unit, so you believe your documents are safe from both destruction and the government. But you might be wrong. Under

5. See id.
10. Id.
current law, police officers may be able to access your cloud-stored documents without a warrant because of the Third-Party Doctrine. A broad reading of this doctrine suggests that information voluntarily revealed to a third party retains no Fourth Amendment protection. Thus, if the Third-Party Doctrine applies to cloud storage, knowingly sharing your data with Dropbox gives Dropbox the right to convey that data to the government without implicating the Fourth Amendment. In other words, the Third-Party Doctrine may allow police access to your cloud-stored data without a warrant.

Hopefully, this strikes you as wrong—nonsensical even. Cloud-stored documents contain the same content as other documents the Fourth Amendment protects from government interception, yet they may lose protection the moment we press "save." Thirty years ago, we kept letters and documents in a lockbox. Twenty years ago, we stored that same information in local computer files. Today, we store those documents in the cloud. Society is quickly becoming paperless. As this shift occurs, will the Fourth Amendment slowly lose its teeth? In the landmark case _Katz v. United States_, the Supreme Court made it clear that the Fourth Amendment protects people and not places. If this remains true, it should not matter where your documents are stored. The Fourth Amendment should continue to protect our documents, regardless of where we store them—the shift to cloud-based storage should not mean a forfeit of traditional constitutional protections.

As the United States increasingly relies on the cloud for data storage, the question of how much protection cloud-stored documents receive is becoming more pressing. The government already accesses private data stored in the cloud for both domestic law enforcement and national...
security purposes. Currently, it is unclear what protections apply to cloud storage, but a reasonable reading of the applicable cases and statutes indicates that minimal protections apply. This lack of strong protection is inconsistent with how society views and uses cloud storage and frustrates Congress’s purpose in enacting these statutes.

Part I of this Article explains why Fourth Amendment protections do not clearly apply to cloud storage by evaluating current judicial interpretations of the Fourth Amendment. Part II focuses on the Electronic Communications Privacy Act of 1986 (ECPA) and demonstrates that ECPA offers cloud-stored documents only limited protection against unwarranted government access. Part III argues that Congress should reform current laws to explicitly protect cloud storage and describes three critical amendments present in proposed ECPA reform bills. Part III then suggests two additional amendments to ensure unambiguous protection for cloud-stored documents. This Article concludes that although Congress is on the right track with its pending ECPA reform bills, incorporating this Article’s proposed amendments would embrace cloud technology and better protect cloud-stored information.

I. THE FOURTH AMENDMENT DOES NOT CLEARLY PROTECT CLOUD-STORED CONTENT

The Fourth Amendment is the most obvious and powerful tool for protecting private information from unjustified government inspection. It gives individuals the right “to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” To comply with this right, the government must procure a warrant based “upon probable cause” before performing a search. The Fourth Amendment only comes into play when the government performs a “search”—a term without clear

---

19. See generally The NSA Files, GUARDIAN, http://www.theguardian.com/world/the-nsa-files (last visited Apr. 14, 2014) (detailing Edward Snowden’s revelations relating to the National Security Agency’s warrantless access of information stored with major technology companies). While the national security context presents important questions, this Article only focuses on domestic law enforcement access to cloud-stored documents.

20. Courts may not provide constitutional protections to cloud storage under current Fourth Amendment precedent, see infra Part 0, and while Congress passed legislation in the mid-1980s to extend Fourth Amendment-like protections to electronic communications, only the weakest of protections likely apply to cloud storage. See infra Part 0.

21. S. REP. No. 99-541, at 3 (1986) (“[I]nformation is processed for the benefit of the user but often it is maintained for approximately 3 months to ensure system integrity. For the person or business whose records are involved, the privacy or proprietary interest in that information should not change. Nevertheless, because it is subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection. Thus, the information may be open to possible wrongful use and public disclosure by law enforcement authorities as well as unauthorized private parties.”) (internal citation omitted).


23. U.S. CONST. amend. IV.

24. Id.
The modern interpretation of the Fourth Amendment comes from \textit{Katz}, a case in which the Court considered whether a search occurred when police placed a recording device on the outside of a public telephone booth to intercept the defendant’s private conversations.\textsuperscript{27} Firmly rejecting the concept of constitutionally protected areas, the Court held that “the Fourth Amendment protects people, not places.”\textsuperscript{28} The majority opinion recognized that “what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.”\textsuperscript{29} Justice Harlan’s concurrence provides the lasting “reasonable expectation of privacy” test that courts use to determine whether a search has occurred.\textsuperscript{30} Under this test, a person has a reasonable expectation of privacy where (1) that person exhibits an actual, subjective expectation of privacy, and (2) that expectation is one that society recognizes as reasonable.\textsuperscript{31}

An analysis of Fourth Amendment precedent does not clearly reveal whether the Fourth Amendment protects cloud-stored content. Protection depends on whether both the individual user expects the stored information to remain private (subjective expectation of privacy), and whether society generally expects the information to remain private (objective expectation of privacy). Courts have come down on both sides as to whether users maintain a reasonable expectation of privacy in electronic data stored with third parties, but no court has directly decided this issue with respect to cloud storage. The lack of judicial guidance, as well as the difficulty of applying older precedent to modern technology, complicates the expectation of privacy analysis for cloud storage.

A. REASONABLE EXPECTATION OF PRIVACY IN CLOUD STORAGE

Courts have extended the meaning of “papers”\textsuperscript{32} under the Fourth Amendment to include more than just tangible sheets of pulp. The \textit{Katz} Court, for instance, provided Fourth Amendment protection to the intangible content of a telephone conversation.\textsuperscript{33} Courts have granted

\begin{itemize}
\item \textsuperscript{25} See, e.g., United States v. Jones, 132 S. Ct. 945, 949 (2012) (holding that the government’s installation of a GPS device on the defendant’s car was a search within the Fourth Amendment); Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (holding that installing and using a pen register was not a search); United States v. Miller, 96 U.S. 435, 446 (1976) (holding that government subpoenas for bank records were not searches); Katz v. United States, 389 U.S. 347, 359 (1967) (holding that attaching a listening device to the outside of a public telephone booth constituted a search); Olmstead v. United States, 277 U.S. 438 (1928) (holding that attaching a wiretap to telephone wires outside the home and without trespass did not constitute a search).
\item \textsuperscript{26} See supra note 25.
\item \textsuperscript{27} \textit{Katz}, 389 U.S. at 348.
\item \textsuperscript{28} \textit{Id.} at 350–51.
\item \textsuperscript{29} \textit{Id.} at 351.
\item \textsuperscript{30} \textit{Id.} at 361 (Harlan, J., concurring).
\item \textsuperscript{31} \textit{Id.} (Harlan, J., concurring).
\item \textsuperscript{32} U.S. CONST. amend. IV (“The right of the people to be secure in their persons, houses, papers, and effects . . . .” (emphasis added)).
\item \textsuperscript{33} \textit{Katz}, 389 U.S. at 354–59.
\end{itemize}
protection to the intangible files on personal computers, finding hard drives analogous to closed containers—items in which an owner historically maintained a reasonable expectation of privacy even in a public area.\textsuperscript{34} Courts have also found briefcases, backpacks, purses, and even lockers to be closed containers and thus worthy of protection.\textsuperscript{35}

Cloud storage, however, differs from a computer sitting in a home or in a backpack in one notable way: with cloud storage, the user does not own the computer storing the documents. The user essentially rents space on a company's server. But this difference does not necessarily obviate the Fourth Amendment—after all, the renter of an apartment retains a reasonable expectation of privacy in her rented quarters.\textsuperscript{36}

Because users do not physically live in the space they rent on the cloud, the best analogy between the cloud and physical world is to analogize cloud users to renters of storage units. And it has been established that renters of storage units maintain a reasonable expectation of privacy in their units:

People generally have a reasonable expectation of privacy in a storage unit, because storage units are secure areas that "command a high degree of privacy." And an individual can have a recognized privacy expectation in a storage space even when he or she is not the lessee of the unit.\textsuperscript{37}

Storage units retain Fourth Amendment protection even though the owner or landlord maintains the right to access the property for limited purposes.\textsuperscript{38} Cloud storage providers also retain limited access rights: the provider can access cloud-stored content to store, retrieve, and back up files. One commentator argues that cloud service providers are essentially "virtual landlords," such that even though providers have the virtual keys to their users' virtual storage units, the users retain a reasonable expectation of privacy in their cloud-stored documents.\textsuperscript{39}

In 2010, the Sixth Circuit concluded that a user has a reasonable

\begin{itemize}
  \item \textsuperscript{34} See Trulock v. Freeh, 275 F.3d 391, 410 (4th Cir. 2001) (Michael, J., concurring in part and dissenting in part) ("Courts have not hesitated to apply established Fourth Amendment principles to computers and computer files, often drawing analogies between computers and physical storage units such as file cabinets and closed containers."); United States v. Reyes, 922 F. Supp. 818, 832–33 (S.D.N.Y. 1996) (finding that although officers properly seized a pager, the authority to possess is distinct from the authority to examine the contents of the pager’s memory); United States v. Chan, 830 F. Supp. 531, 535 (N.D. Cal. 1993) (finding that the defendant had a reasonable expectation of privacy in the contents of a pager’s memory).
  \item \textsuperscript{35} United States v. Freire, 710 F.2d 1515, 1519 (11th Cir. 1983) (finding a privacy interest in a briefcase); Doe ex rel. Doe v. Little Rock Sch. Dist., 380 F.3d 349, 353 (8th Cir. 2004) (finding an expectation of privacy in students' backpacks); Murdock v. State, 664 P.2d 589, 598 (Alaska Ct. App. 1983) ("The petitioners had a reasonable expectation of privacy in the property stored [in a 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.").
  \item \textsuperscript{36} See Chapman v. United States, 365 U.S. 610, 615–18 (1961) (finding that a leaseholder maintains an expectation of privacy in rented property despite consent of the landlord for a search).
  \item \textsuperscript{37} United States v. Johnson, 584 F.3d 995, 1001 (10th Cir. 2009) (internal citations omitted).
  \item \textsuperscript{38} See id.
  \item \textsuperscript{39} David A. Couillard, Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing, 93 MINN. L. REV. 2205, 2236 (2009).
\end{itemize}
expectation of privacy in the contents of his emails. In *United States v. Warshak*, the defendant was indicted for mail, wire, and bank fraud. After the indictment, the government compelled the defendant’s Internet service provider (ISP) to turn over thousands of his emails. Applying the reasonable expectation of privacy test from *Katz*, the court first concluded that the defendant exhibited a subjective expectation of privacy in his emails because of their “sensitive and sometimes damning substance.” The court then held that society recognizes the defendant’s expectation as reasonable.

The court found email to be fundamentally similar to letters and other traditional forms of communication, stating that “it would defy common sense” to protect email under a lesser Fourth Amendment standard. The court rejected the government’s argument that the ISP’s contractual right to access the defendant’s emails destroyed any expectation of privacy for two reasons. First, the court determined that the mere ability of a third party to access the contents of a communication does not itself extinguish the right to privacy. A mail handler could rip open a letter or a telephone company could tap into a phone line, but the Fourth Amendment still protects letters and telephone conversations. Second, the court found that a limited contractual right to access the contents of communications does not end the reasonableness inquiry. At the time *Katz* was decided, telephone companies contractually reserved the right to monitor telephone conversations to protect against improper or illegal use, but this right did not extinguish a user’s expectation of privacy. The *Warshak* court found the defendant’s agreement with his ISP, which stated that the ISP “may access” the defendant’s information in certain circumstances, similar to that between the phone companies and their customers. The court noted that “control over the [emails] and ability to access them under certain limited

40. *United States v. Warshak* (Warshak III), 631 F.3d 266, 288 (6th Cir. 2010). Previously, a Sixth Circuit panel heard the issue in 2007 and found a reasonable expectation of privacy in email. Warshak v. United States (Warshak I), 490 F.3d 455, 473 (6th Cir. 2007) (“We have little difficulty agreeing with the district court that individuals maintain a reasonable expectation of privacy in e-mails that are stored with, or sent or received through, a commercial ISP.”). But an en banc rehearing reversed the panel’s decision without reaching the merits. Warshak v. United States (Warshak II), 532 F.3d 521, 533–34 (6th Cir. 2008) (rejecting Warshak’s claim for ripeness).
41. *Warshak III*, 631 F.3d 266 (6th Cir. 2010).
42. *Id.* at 281 (author refers to this case generally in the text as *Warshak*).
43. *Id*.
44. *Id.* at 284.
45. *Id*.
46. *Id.* at 285–86.
47. *Id.* at 286.
48. *Id*.
49. *Id.* at 287.
50. *Id*.
51. *Id*.
52. *Id*. The court did not, however, say that a service agreement could never destroy an expectation of privacy in email. Perhaps a contractual right to “audit, inspect, and monitor” would be enough to overcome the expectation of privacy. *Id.* (quoting *Warshak I*, 490 F.3d at 472–73).
circumstances [is] not [] enough to overcome an expectation of privacy.”

Warshak’s reasoning can be extended to cloud storage. Cloud-stored documents are similar to traditionally protected papers in the home, just as emails are similar to traditionally protected letters. Further, Warshak held that the email provider’s limited right to access the emails was not enough to destroy the reasonable expectation of privacy, and cloud storage providers retain similar limited rights to access stored documents. The Warshak court would likely find that a user maintains a reasonable expectation of privacy in cloud-stored documents.

Despite the weight of the Warshak opinion, few courts outside of the Sixth Circuit have applied its holding. Most courts dismiss the idea that users have a reasonable expectation of privacy in stored email, at least when the recipient has already opened the email. Courts in the Eleventh and Second Circuit have found that voluntarily delivering messages to third parties destroys a user’s right to privacy in the transmitted information.

Part of the courts’ reasoning in these cases relied on the Third-Party Doctrine. The courts determined that users lost their expectation of privacy in the content of their emails upon voluntarily sending the email to a recipient. But unlike email, cloud-stored documents are usually not intended for a third-party recipient; users typically store documents for their own later retrieval. Applying the reasoning of the Eleventh and Second Circuits to cloud storage, the expectation of privacy for cloud users is not reduced when users do not intend to deliver the documents to anyone else.

Until more appellate courts or the Supreme Court squarely decide that users have a reasonable expectation of privacy in email or other electronic communications, there is no guarantee that the Fourth Amendment applies to cloud storage. After Warshak, users in the Sixth Circuit enjoy a

---

53. Id. at 287 (quoting Warshak 1, 490 F.3d at 473). The Warshak court’s holding provides a strong basis for finding a Fourth Amendment privacy right in email stored in the cloud. Even so, other courts have almost summarily dismissed the idea that users have a reasonable expectation of privacy in stored email, at least when the user has already opened the email. Courts in the Eleventh and Second Circuit have found that voluntarily delivering messages to third parties destroys a user’s right to privacy in the transmitted information. See Rehberg v. Paulk, 598 F.3d 1268, 1282 (11th Cir. 2010) (“[Plaintiff’s] voluntary delivery of emails to third parties constituted a voluntary relinquishment of the right to privacy in that information.”). On rehearing, a panel overturned Rehberg and decided the case without reaching the constitutional question. Rehberg v. Paulk, 611 F.3d 828, 846 (11th Cir. 2010) (“[W]e now question whether it would be prudent in this case and on this limited factual record to establish broad precedent as to the reasonable privacy expectation in email content. Moreover, because this is a qualified immunity case, we need not reach the underlying constitutional issue. Instead, we can resolve this case narrowly . . . .”); see also United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) (“[Individuals] may not, however, enjoy such an expectation of privacy in transmissions over the Internet or e-mail that have already arrived at the recipient.”).

54. The Fifth Circuit has applied Warshak to determine that some cell site location information constitutes a business record and is not subject to a reasonable expectation of privacy. In re Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 611 (5th Cir. 2013).

55. See Rehberg, 598 F.3d at 1282; Lifshitz, 369 F.3d at 190.

56. Lifshitz, 369 F.3d at 190 (holding that there was no expectation of privacy in emails that had already been received).

57. In some cases documents are stored in shared folders that multiple users can access. In these circumstances, the Second Circuit’s reasoning may apply.
reasonable expectation of privacy in their email and presumably enjoy that expectation in their cloud-stored documents as well. But two other circuits disagree with Warshak as to what constitutes a reasonable expectation of privacy in electronic communications, and it is unclear which side the remaining circuits will take.

B. THE THIRD-PARTY DOCTRINE MAY DESTROY FOURTH AMENDMENT PROTECTION OF CLOUD STORAGE

Even where individuals have a subjective expectation of privacy and act accordingly, the Third-Party Doctrine may defeat Fourth Amendment protections. The Third-Party Doctrine finds its roots in the Supreme Court case United States v. Miller. Miller, the defendant, a bootlegger who made whiskey with an unregistered still, failed to pay the appropriate federal taxes on his proceeds. The Bureau of Alcohol, Tobacco, and Firearms (ATF), tipped off by an informant, seized Miller's distillery equipment. The ATF then served Miller's two banks with grand jury subpoenas, requesting records of Miller's accounts, and the banks complied. Miller argued that the subpoenas were technically deficient and the ATF had seized the bank documents illegally. The district court denied Miller's argument, but the court of appeals reversed, finding the ATF had violated Miller's Fourth Amendment right against unreasonable search and seizure due to the "compulsory production of a man's private papers to establish a criminal charge against him."

The Supreme Court disagreed with the court of appeals for two reasons. First, the Court refused to classify any of the seized documents as "private papers." Instead, the Court determined the documents were the banks' business records because the banks, rather than being neutral observers, were parties to the transactions depicted in the records. Further, the Court found that Miller neither owned nor possessed the records and they were not "confidential communications." The documents were deposit slips and personal checks that were exposed to the banks' employees in the ordinary course of business. Since the records were integral to the banks' business, the Court determined they could not

58. The Sixth Circuit did determine that there is no expectation of privacy in files uploaded to a public peer-to-peer network because the files were made publically available. United States v. Conner, 521 Fed. App'x 493, 497–98 (6th Cir. 2013). However, users do not make personal cloud-stored documents accessible to the public and likely retain their reasonable expectation of privacy under Conner.
60. Id. at 436.
61. Id. at 437.
62. Id.
63. Id. at 438–39.
64. Id. (internal quotation omitted).
65. Id. at 440.
66. Id. at 440–41.
67. Id.
68. Id.
be Miller's personal papers and could not receive Fourth Amendment protection. 69

Second, the Court found no legitimate expectation of privacy in the contents of the records because Miller had assumed the risk of exposing his information to the bank. 70 Relying on Katz's reasoning that "'what a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection,"'71 the Court determined Miller lost any expectation of privacy he might have had in the documents when he voluntarily conveyed the information contained in them to the banks, noting that "'[t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.'"72 The Court stated that the Fourth Amendment does not apply "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."73 In other words, regardless of what Miller may have believed about the privacy of his documents, he destroyed his expectation of privacy when he revealed his information to the bank.

In 1979, Smith v. Maryland74 expanded both the Miller ruling and the Third-Party Doctrine.75 In Smith, the government requested that the defendant's telephone company install a pen register to intercept and record all outgoing numbers dialed by the defendant's home phone.76 Unlike Katz, the government did not intercept content from the calls: the pen register merely recorded telephone numbers as they were dialed.77 The Court held that there is no reasonable expectation of privacy in numbers dialed, reasoning that the average telephone subscriber understands she must reveal the numbers she dials to the telephone company so the company can connect the call.78 Further, because the subscriber receives a bill that shows what long-distance numbers were called, she must realize that the telephone company is capable of recording the numbers she dials.79 By knowingly and voluntarily conveying her dialing information to the telephone company, the Court determined she loses any expectation of privacy in those numbers.80

This expansion of the Third-Party Doctrine seems to include

69. Id.
70. Id. at 442-43.
71. Id. at 442 (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).
72. Id. at 443.
73. Id.
74. 442 U.S. 735 (1979).
75. Id.
76. Id. at 737.
77. Id.
78. Id. at 742.
79. Id. at 742-43.
80. Id. at 743. Since Smith, Congress has statutorily expanded the range of what a pen register can record to include dialing, routing, addressing, and signaling information. See 18 U.S.C § 3127(3) (2012).
electronic communications since virtually all electronic communications must pass through a third-party intermediary. Even so, arguments that the Thirty-Party Doctrine should not apply to electronic communications have made some headway in the courts. The following section provides two arguments against the Third-Party Doctrine and applies them to cloud storage.

1. Electronic Communications as Business Records

In *Miller*, the Court stressed that the bank records were also business records.\(^\text{81}\) Such business records did not trigger the Fourth Amendment when the government compelled their disclosure because the bank itself was a party to the transaction and the records sought were “exposed to [the banks’] employees in the ordinary course of business.”\(^\text{82}\)

Professors Patricia Bellia and Susan Freiwald argue that, under *Miller*, emails stored with a third party should be considered “confidential communications” rather than business records.\(^\text{83}\) Unlike bank records, the content of email is not generally exposed to the service provider or its employees in the ordinary course of business. Email is more akin to a piece of luggage left in the care of a third party or a package sent through a delivery service than to a record voluntarily disclosed to a third party.\(^\text{84}\) Bellia and Freiwald further contend that a service provider, unlike a bank, is a true third-party intermediary because users do not direct the content of email at the service provider.\(^\text{85}\) Thus, content not directed at the service provider cannot be a business record under *Miller* because it is not exposed to service provider employees in the ordinary course of business.\(^\text{86}\)

Similar to email, cloud-stored documents are also more like confidential communications than business records. First, the storage provider is not an interested party in a transaction with the user. Although the provider requires some basic information in order to store the documents properly, such as when the file was saved or where it came from, storage providers are generally indifferent to the content of the documents they store. Second, storage providers simply store the documents and do not regularly expose them to employees. Individuals do not direct cloud-stored documents at their providers, just as they do not direct emails to their providers. If email is analogous to handing an envelope to a service provider for delivery, then cloud storage is akin to handing a package to a service provider for storage. In either case, the service provider acts solely as an intermediary, never viewing the content

\(^\text{82.}\) *Id.* at 442.
\(^\text{84.}\) *Id.*
\(^\text{85.}\) See *id.* Bellia and Freiwald recognize the possibility that some email may actually be a record of a transaction between the service provider and the user. *Id.* at 149 n.112. For example, email sent directly by a user to a service provider would be considered a record.
\(^\text{86.}\) *Id.*
of the envelope or package.

Cloud storage providers do, however, maintain a high level of control over the documents, which suggests a more transactional relationship than that involving email and opens up the possibility that cloud-stored documents could be viewed as business records. Though cloud storage most closely resembles placing documents in a physical storage unit owned by a third-party company, notable differences exist in the processes of storing physical and digital documents. Typically, the lessee of a physical storage unit has the key and controls access. The owner’s ability to enter is limited and incidental to business operations unrelated to the storage itself. With cloud storage, however, the service provider, rather than the user, places the documents in storage. The service provider holds onto the “keys” to the server. When a user, let’s call her Alice, saves a document in her Dropbox folder, she essentially asks Dropbox to copy the file and move it securely into her space on its server. Instead of taking her package directly to her unit and locking it away, Alice now hands her package over to the security guard at the front desk, who goes back into a warehouse, finds the bin labeled “Alice,” and places the package inside.

Despite the high level of control cloud storage providers retain over documents stored in the cloud, Warshak supports the argument that cloud-stored documents are not business records. The nature of the relationship between users and providers is more like that between a lessee and a physical storage provider than between a bank and a bank customer. Unlike a bank, the cloud storage provider is not an interested party to the transaction. When a bank customer writes a check, the check itself is an instruction directed to a bank employee to transfer money from one account to another. Cloud storage users do not direct their documents at the provider. Even considering the holding in Miller and the differences between stored email and cloud-stored documents, Warshak’s reasoning suggests that cloud-stored documents are not business records.

2. Assuming the Risk of Third-Party Access to Electronic Communications

In reaching its holding in Miller—that an individual does not have a Fourth Amendment privacy interest in personal bank records—the Supreme Court also relied on an assumption of risk theory, a theory that resulted from cases involving government informants. Various scholars have argued that courts misapply this precedent and misunderstand human nature. They argue that an assumption of risk can only occur when more than one option exists and an individual knowingly and voluntarily decides to select one option over the other. Yet in certain situations, such as

87. Miller, 425 U.S. at 443.
89. See Bellia & Freiwald, supra note 83, at 156.
banking, individuals lack options: "[O]ne could not easily engage in modern society without banking." Thus, an individual should not be expected to assume the risk that information he turns over to a bank may be revealed to the government because he does not have the option of not banking. If we take the view that choosing to use a bank is an assumption of risk, despite banking being a modern necessity, we run the risk that choosing to use any modern technology will deprive users of Fourth Amendment protections.

Presumably, cloud storage users do not intend to convey all of their information to service providers, but the question remains as to exactly what information users actually and knowingly convey to third parties in the cloud storage context. In a typical transaction, one party generally conveys all the content of the transaction to the other. With a letter or a package, the third-party carrier is only privy to the address or routing information listed on the outside of the parcel. The sender intends to convey the content of the parcel only to the recipient. What one intends to convey, however, is a far cry from what one actually conveys.

In the area of digital information, emails are the digital equivalents of letters and packages. Users might expect ISPs to have access to the routing or address information of the email, but they do not intend to share the content of their emails with the providers. Cloud storage is similar—the average individual does not store documents in Dropbox or Google Drive with the intent for these companies to read the stored content.

Cloud storage users may assume that providers have minimal access to their stored content, but in fact these providers retain a high level of access. Cloud providers require users to accept Terms of Service before

90. Id.

91. The Fifth Circuit rejected the ubiquity argument in the case of cell phones. See In re Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 613 (5th Cir. 2013) ("Their use of their [cell] phones, moreover, is entirely voluntary. The Government does not require a member of the public to own or carry a phone. As the days of monopoly phone companies are past, the Government does not require him to obtain his cell phone service from a particular service provider that keeps historical cell site records for its subscribers, either." (internal citation omitted)). However, at least one district court judge agrees that the increased prevalence of cell phones results in an increased expectation of privacy:

It is now safe to assume that the vast majority of people reading this opinion have at least one cell phone within arm's reach (in addition to other mobile devices). In fact, some undoubtedly will be reading this opinion on their cellphones. Cell phones have also morphed into multi-purpose devices. They are now maps and music players. They are cameras. They are even lighters that people hold up at rock concerts. They are ubiquitous as well. Count the phones at the bus stop, in a restaurant, or around the table at a work meeting or any given occasion. Thirty-four years ago, none of those phones would have been there. Thirty-four years ago, city streets were lined with pay phones. Thirty-four years ago, when people wanted to send "text messages," they wrote letters and attached postage stamps. Klayman v. Obama, 957 F. Supp. 2d 1, 34-35 (D.D.C. 2013) (internal footnotes omitted).

Put simply, people in 2013 have an entirely different relationship with phones than they did thirty-four years ago. As a result, people make calls and send text messages now that they would not (really, could not) have made or sent back when Smith was decided—for example, every phone call today between two people trying to locate one another in a public place... Whereas some may assume that these cultural changes will force people to "reconcile themselves" to an "inevitable" "diminution of privacy that new technology entails," I think it is more likely that these trends have resulted in a greater expectation of privacy and a recognition that society views that expectation as reasonable.

Id. at 36 (quoting United States v. Jones, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring)).
offering their services. They also maintain Privacy Policies describing how they will use and store user data. Most of these policies describe at least one instance in which the service provider can or does access and analyze the information stored. For example, Dropbox’s Terms of Service states:

When you use our Services, you provide us with things like your files, content, email messages, contacts and so on (“Your Stuff”). Your Stuff is yours. These Terms don’t give us any rights to Your Stuff except for the limited rights that enable us to offer the Services.

We need your permission to do things like hosting Your Stuff, backing it up, and sharing it when you ask us to. Our Services also provide you with features like photo thumbnails, document previews, email organization, easy sorting, editing, sharing and searching. These and other features may require our systems to access, store and scan Your Stuff. You give us permission to do those things, and this permission extends to trusted third parties we work with.

In other words, a Dropbox user agrees that Dropbox and its “trusted third parties” can “access, store and scan” anything stored on the service.

In its Privacy Policy, Dropbox makes it clear that “[Dropbox] may disclose your information to third parties if [it] determine[s] that such disclosure is reasonably necessary to (a) comply with the law; (b) protect any person from death or serious bodily injury; (c) prevent fraud or abuse of Dropbox or [its] users; or (d) protect Dropbox’s property rights.” Assuming a Dropbox user actually reads the Terms of Service, she would have to conclude that she has conveyed a significant amount of her data’s content to Dropbox.

Analyzing cloud storage under Warshak suggests that users do not assume the risk that cloud storage providers will access their information.

---


94. Id.

95. Such information includes:
Services. When you use our Services, we store, process and transmit your files (including stuff like your photos, structured data and emails) and information related to them (for example, location tags in photos). If you give us access to your contacts, we’ll store those contacts on our servers for you to use. This will make it easy for you to do things like share your stuff, send emails, and invite others to use the Services.


96. This is not a good assumption. According to a survey by The Guardian, “just 7% of Britons read the online terms and conditions when signing up for products and services.” Rebecca Smithers, Terms and Conditions: Not Reading the Small Print Can Mean Big Problems, THE GUARDIAN (May 11, 2011), http://www.theguardian.com/money/2011/may/11/terms-conditions-small-print-big-problems. One study found that users would spend approximately 201 hours per year if they actually read the online privacy policies they agreed to. Aleecia M. McDonald & Lorrie Faith Cranor, The Cost of Reading Privacy Policies, 4 I/S: J.L. & POL’Y FOR INFO. SOC’Y 543, 565 (2009).

97. Google’s Terms of Service are even clearer: “Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored.” Google Terms of Service, GOOGLE, http://www.google.com/policies/terms/ (last visited Apr. 19, 2014).
By contractual agreement, most cloud services affirmatively retain the right to access and analyze content stored with them. Under *Miller*, then, users may lose Fourth Amendment protection in their documents as soon as they save them with a third-party cloud storage provider.98 *Warshak*, however, found that absent "an intention to ‘audit, inspect, and monitor,’” a limited right of access will not overcome an expectation of privacy, and consequently rejected applying the Third-Party Doctrine to email.99 The cloud storage policies discussed above admittedly retain more rights than the policy in *Warshak*, but still do not show an actual intention of the service provider to inspect every document.

In 2012, the Supreme Court decided *United States v. Jones*,100 a case that lends support to *Warshak*'s treatment of the Third-Party Doctrine. The Supreme Court also hinted it may be open to limiting the doctrine. In *Jones*, the Court was asked to decide whether attaching a GPS monitoring device to an individual’s vehicle and tracking that vehicle’s movement on public streets constituted a search under the Fourth Amendment.101 The majority found that a search occurred because the “[g]overnment physically occupied the private property for the purpose of obtaining information.”102 In two concurrences, five of the justices struggled with the majority’s view.

Justice Alito’s concurrence, joined by three other justices, rejected the majority’s trespass-based reasoning, and instead applied the reasonable expectation of privacy test.103 Justice Alito found that lengthy GPS monitoring for ordinary offenses clearly violated the Fourth Amendment.104 Justice Alito also suggested that the evolving state of technology will continue to alter the average person’s privacy expectations as she becomes used to more pervasive technologies.105 In her solo concurrence, Justice Sotomayor stated:

More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information

---

98. United States v. Miller, 425 U.S. 435, 443 (1976) (“[The Fourth Amendment does not prohibit the obtaining of information revealed to a third party . . . even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.”).


100. 132 S. Ct. 945 (2012).

101. Id. at 948.

102. Id. at 949.

103. Id. at 962 (Alito, J., concurring).

104. Id. at 964 (Alito, J., concurring) (“I conclude that the lengthy monitoring that occurred in this case constituted a search under the Fourth Amendment.”).

105. Id. at 963 (Alito, J., concurring) (“Perhaps most significant, cell phones and other wireless devices now permit wireless carriers to track and record the location of users . . . . For older phones, the accuracy of the location information depends on the density of the tower network, but new ‘smart phones,’ which are equipped with a GPS device, permit more precise tracking. For example, when a user activates the GPS on such a phone, a provider is able to monitor the phone’s location and speed of movement and can then report back real-time traffic conditions after combining (‘crowdsourcing’) the speed of all such phones on any particular road. Similarly, phone-location-tracking services are offered as ‘social’ tools, allowing consumers to find (or to avoid) others who enroll in these services. The availability and use of these and other new devices will continue to shape the average person’s expectations about the privacy of his or her daily movements.” (internal citations omitted)).
voluntarily disclosed to third parties. This approach is ill suited to the
digital age, in which people reveal a great deal of information about
themselves to third parties in the course of carrying out mundane tasks.
People disclose the phone numbers that they dial or text to their cellular
providers; the URLs that they visit and the e-mail addresses with which
they correspond to their Internet service providers; and the books,
groceries, and medications they purchase to online retailers. . . . I would
not assume that all information voluntarily disclosed to some member
of the public for a limited purpose is, for that reason alone, disentitled to
Fourth Amendment protection.\(^{106}\)

Ultimately, Jones's characterization of the Third-Party Doctrine
remains dicta because, while all of the justices agreed that a search
occurred, they could not agree on how or why. Justice Sotomayor's
concurrence calls into question the Third-Party Doctrine entirely, and
Justice Alito's concurrence seems to challenge the assumption of the risk
argument. All five of the concurring justices found a reasonable
expectation of privacy in Jones’s location data despite the argument that
Jones permitted others to see his public movements and assumed the risk
that law enforcement agents would use a GPS device to track those
movements. This suggests that at least some members of the Court are open
to significantly curtailing the Third-Party Doctrine.

Jones does not, however, overturn Miller or Smith. The Third-Party
Doctrine remains good law, although courts are not united on its post-Jones
application.\(^{107}\) Further, it is unclear how broadly lower courts will read
Miller and Smith and whether other jurisdictions are willing to extend
Warshak's line of reasoning to email, other electronic communications, and
cloud storage.

C. NO CLEAR APPLICATION OF FOURTH AMENDMENT TO CLOUD STORAGE

Given that judicial application of the Fourth Amendment to electronic
communications has not been uniform, it is unclear whether courts would
consider cloud storage to fall under its protections. Warshak and Jones
strongly indicate that the legal landscape may be shifting away from a strict
interpretation of the Third-Party Doctrine, but absent wider adoption of
Warshak or a decision from the Supreme Court explicitly addressing the
Fourth Amendment's application to electronic communications, the extent
of this shift is unknown.

Ultimately, this confusion means individuals cannot rely on the courts

\(^{106}\) Id. at 957 (Sotomayor, J., concurring) (internal citations omitted).

\(^{107}\) Compare Klayman v. Obama, 957 F. Supp. 2d 1, 31 (D.D.C. 2013) ("When do present-day
circumstances—the evolutions in the Government's surveillance capabilities, citizens' phone habits,
and the relationship between the NSA and telecom companies—become so thoroughy unlike those
considered by the Supreme Court thirty-four years ago that a precedent like Smith simply does not
apply? The answer, unfortunately for the Government, is now."); with ACLU v. Clapper, 959 F. Supp.
2d 724, 752 (S.D.N.Y. 2013) ("But the Supreme Court did not overrule Smith. And the Supreme Court
has instructed lower courts not to predict whether it would overrule a precedent even if its reasoning has
been supplanted by later cases. . . . Clear precedent applies because Smith held that a subscriber has no
legitimate expectation of privacy in telephony metadata created by third parties. Inferior courts are
bound by that precedent." (internal citations omitted)).
to provide strong constitutional protections for cloud storage anytime soon. Since cloud storage requires protection from government interception, and no such protection is forthcoming from the courts, Congress should pass new legislation to provide cloud storage with necessary protections against unjustified government monitoring. In 1986, Congress responded to the need to protect electronic communications by enacting ECPA, but the advancements of modern electronic communications have left that 28-year-old law in the dust.

II. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OFFERS CLOUD STORAGE LITTLE PROTECTION

With ECPA, Congress created a complex framework for protecting electronic communications. Congress amended ECPA twice, but the protections most applicable to cloud storage have remained essentially unchanged. Congress crafted ECPA before the World Wide Web existed, and courts now struggle to apply its statutory scheme to today’s rapidly advancing technology. Certain ECPA provisions do not apply to cloud storage at all, and those that do apply likely provide only low levels of protection.

A. THE PEN REGISTER ACT ONLY PROTECTS A NARROW CATEGORY OF INFORMATION

Title III of ECPA, the Pen Register Act, protects dialing, routing, addressing, and signaling information from real-time government interception. When enacted, ECPA limited the information that pen registers could collect to telephone dialing information. Not until the USA PATRIOT Act did Congress expand the definition of “collectible information” to include other routing, addressing, and signaling information.


110. Title I of ECPA punishes anyone who “intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication.” 18 U.S.C. § 2511(1)(a) (2012). The government must intercept the content in real time in order for this provision to apply. Title III of ECPA concerns pen register and trap and trace devices. 18 U.S.C. § 3121(a) (2012). Both pen registers and trap and trace devices are used to intercept dialing, routing, addressing, or signaling information in real time. In cloud storage applications, the information protected by Titles I and III are already created and stored by the service provider. The government need merely request the information—there is no need for real time interception, so Titles I and III are largely inapplicable to cloud storage.


113. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept
Yet even under this expanded definition, the type of information the Pen Register Act seeks to protect is information about who is contacting whom and how the communication gets from Person A to Person B. In contrast, an electronically stored document does not have the same attributes as a traditional communication. Rather, it has metadata, or data that describes characteristics of the document, pertaining directly to the contents of the file: the author, the date of creation, etc. The only addressing or routing information generated for cloud-stored documents is when and from where the user sent the document to the service provider.

Since cloud-stored documents lack the addressing attributes of traditional communications, the Pen Register Act arguably protects only a narrow aspect of cloud-stored documents. It will protect only information such as how and when the document was sent to the cloud storage provider. Other metadata attributes of cloud-stored documents likely fall outside this category, and cloud storage users must rely on other sections of ECPA to protect content information.

B. THE STORED COMMUNICATIONS ACT DOES NOT ADEQUATELY PROTECT CLOUD STORAGE

Congress designed Title II of ECPA, the Stored Communications Act (SCA), to protect electronic communications held in storage.114 The SCA is a complex statute that offers varying levels of protection to electronic communications depending on the circumstances under which the communications are stored.115 Due to vague and outdated terms, it is unclear whether the SCA, which only protects "electronic communications,"116 applies to cloud storage. The following section examines this issue, concluding that the SCA likely applies to cloud storage. Assuming the SCA does apply, the section then applies three SCA provisions to cloud-stored documents.

The SCA applies to the contents and records of "electronic communications" held in storage.117 The term "communication" traditionally refers to the mutual transfer of information from one party to another, such as through conversations, letters, or emails. The SCA's definition of electronic communication is broader, including "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. . . ."118 This definition leaves open

---

117. Id.
the possibility of a one-sided communication, as there is no requirement that the transfer actually be received by anyone. A document sent by a user to be stored with a cloud service provider is certainly a “signal, writing, . . . or intelligence of any nature” that is “transmitted . . . by wire, radio, electromagnetic, photoelectronic or photooptical system,” even though the document was never meant to be communicated to, or received by, another party.

A literal reading of the SCA’s language reveals that the definition of electronic communication is broad enough to encompass cloud storage. It is possible that Congress did not include a requirement that the document be intended for another person because it is implicit in the plain meaning of the term “communication.” Absent such a requirement, however, the definition could be interpreted to allow the SCA to apply to cloud storage.

1. 18 U.S.C. § 2703(a): Contents in Electronic Storage

Section 2703(a) applies to contents of an electronic communication held by an electronic communications service (ECS), which is simply any service that allows users to send or receive electronic communications. The statute describes such communications as those “in electronic storage in an electronic communications system,” where an “electronic communications system” is “any wire, radio, electromagnetic, photooptical or photoelectronic facilit[y] for the transmission of wire or electronic communications, and any computer facilit[y] or related electronic equipment for the electronic storage of such communications.” If the content has been in storage for 180 days or less, the government must procure a search warrant to access the information. If the content has been in storage for more than 180 days, the government need only obtain a subpoena or court order to access the information.

In ascertaining whether § 2703(a) applies to cloud storage, the first question is whether a cloud service provider is considered an ECS. If we assume that a document stored on the cloud is an electronic communication under the SCA, a cloud service provider would, by definition, be a service allowing a user to send or receive the communication. However, the core mission of a traditional ECS is to allow a user to send or receive communications or to provide the infrastructure by which online information travels. A cloud service provider does not necessarily

119. Id. There are some cases where cloud documents are actually intended to be received by other parties, such as with shared access folders, where multiple users can access an online folder.
120. 18 U.S.C. § 2703(a) (2012).
125. See id. (allowing the government to use an administrative subpoena or court order to compel disclosure of electronic communications held in storage for more than 180 days).
126. In re Doubleclick Privacy Litig., 154 F. Supp. 2d 497, 511 n.20 (S.D.N.Y. 2001) (“Examples of providers in the Internet world would include ISPs such as America Online, Juno and UUNET, as well as, perhaps, the telecommunications companies whose cables and phone lines carry
provide that infrastructure, and a user's ability to send or receive communications is only incidental to the purpose of storing and retrieving the documents. Yet, cloud service providers allow users to send or receive documents over their networks, making it likely that they would fit under the SCA's definition of an ECS.

If we assume a cloud service provider is an ECS, the next step is to determine whether a cloud-stored document is held in "electronic storage." Electronic storage is: (1) "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof," and (2) "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." Once a document reaches the cloud, it is no longer in temporary or intermediate storage under the first definition of storage. Rather, the service provider stores the document for later retrieval by the user. As the purpose of cloud storage is to provide backups that can be retrieved from any device, cloud-stored documents fall under the plain meaning of the second definition of electronic storage.

This conclusion is bolstered by the Ninth Circuit's analysis in *Theofel v. Farey-Jones*. In *Theofel*, the court found that a message is held in electronic storage when an ISP stores it on a server in case a user wants to download another copy. Under this view, cloud storage clearly meets the second definition of electronic storage. *Theofel*, however, is only controlling in the Ninth Circuit. In other jurisdictions, electronic storage must be incident to the transmission of the communication—any storage after the transmission is complete does not count. In these jurisdictions, cloud-stored documents would not be considered in electronic storage because the storage is not incident to the transmission.

Continuing the analysis, if we assume both that a cloud service provider is an ECS and a cloud-stored document is an electronic communication, the last step is to determine whether the document has been in storage for more or less than 180 days. This time limit reflects Congress's assumption that short-term storage implicates the Fourth Amendment while long-term storage indicates user abandonment. While this assumption may have been accurate when Congress enacted the SCA in 1986, it no longer reflects modern-day use of technology. Decreasing

---

128. 359 F.3d 1066 (9th Cir. 2003).
129. Id at 1075.
131. See Susan Freiwald & Sylvain Mëtëlle, Reforming Surveillance Law: The Swiss Model, 28 BERKELEY TECH. L.J. 1261, 1311–12 (2013) ("The 180-day cutoff for the mandatory warrant reflects Congress' view in 1986 that emails stored a relatively short time were likely protected by the Fourth Amendment, while those stored longer than 180 days could be seen to be abandoned by the user and therefore the business records of the storing company.")
storage costs and the increasing volume of electronic communications mean that users will store important emails or communications for longer periods of time, perhaps even years, without considering them to be abandoned. Cloud storage is similar to modern email in this respect. Cloud storage saves documents for an indefinite period of time to allow for later retrieval. The purpose is to store documents, not to view and dispose of them. Yet, under § 2703(a), after 180 days a document loses its warrant protection.

Whether § 2703(a) applies depends first on whether a cloud storage provider can be characterized as an ECS, which is questionable because the provider’s ultimate purpose is to store documents, not transmit them. Even if the provider is an ECS, cloud-stored documents may only be considered in electronic storage within the Ninth Circuit. Other jurisdictions have a narrower view of electronic storage that may not cover cloud storage. To the extent that § 2703(a) applies, the government would be required to seek a warrant only for documents that have been stored in the cloud for 180 days or less and could compel service providers to produce older documents by satisfying a lesser standard.

2. 18 U.S.C. § 2703(b): Contents Held By a Remote Computing Service

The alternative to defining a cloud service provider as an ECS is to treat it as a Remote Computing Service (RCS). Section 2703(b) allows the government to acquire the content of any electronic communication from a RCS provided the communication is held or maintained (1) on behalf of a user’s electronic transmission, and (2) solely for the purpose of providing storage or computer processing services to such user. If these elements are met, the government may acquire the content by obtaining either a warrant or an order based on § 2703(d) (a “D order”), the latter of which also requires the government to provide notice to the content owner. In providing notice, however, the government may take advantage of certain delayed notice tools.

Section 2703(b) applies only if a cloud service provider meets the definition of a RCS. A RCS provides “computer storage or processing services by means of an electronic communications system . . . to the public.” Cloud storage service providers can be classified as RCSs since they back up documents for later retrieval. Classifying backup providers as

134. *Id.* § 2703(b)(1)(a)–(b) (2012). A D order is a mechanism by which the government can procure a court order for disclosure of the contents of electronic communication if it “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.” *Id.* § 2703(d).
RCSs is consistent with Congress’s understanding of remote computing at the time the SCA was passed, as well as with subsequent judicial interpretation. Further, cloud storage meets the requirement that such services be offered to the public. A service is offered to the public when it is available to any member of the general population who complies with the requisite procedures and pays any requisite fees. Most cloud storage providers meet this definition, as they offer free and paid services to the public at large.

If cloud service providers operate as RCSs, then documents in cloud storage clearly meet the other two elements of § 2703(b): (1) the service provider holds the documents on behalf of the user, and (2) the user sends the documents electronically to the service provider. Service providers only retain documents to provide its cloud storage service.

This analysis concludes that because cloud service providers are likely RCSs, the government can use § 2703(b) to access cloud-stored documents. Using § 2703(b), then, the government could either meet the general warrant requirement by showing probable cause or use the lower D order standard. The D order standard requires only that the government provide “specific and articulable facts showing that there are reasonable grounds to believe that the contents . . . sought, are relevant and material to an ongoing criminal investigation.”

If the government wants to obtain a D order, it must provide notice to the user, but the government can apply for a delay of notice by showing that notification could have an “adverse result.” Such adverse results are enumerated in § 2705(a)(2), and include: (1) physically endangering an individual, (2) possible flight from prosecution, (3) potential evidence tampering, (4) intimidating potential witnesses, and (5) otherwise seriously jeopardizing the investigation or delaying the trial. Given that any notice could potentially result in flight, destruction of evidence, or otherwise jeopardize an investigation, it would not require very imaginative arguments to show that notification would have an adverse result.

The government’s ability to delay notice collapses the distinction between the warrant and the D order—the only difference left is the standard that the government must meet to compel service providers to disclose content. After meeting the “adverse result” requirement for

138. See Steve Jackson Games, Inc. v. United States Secret Service, 816 F. Supp. 432, 442–43 (W.D. Tex. 1993) (finding that an online bulletin board system was an RCS because it “provided services to the public whereby its users could store public and private electronic communications”).
139. See SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, supra note 130, at 119.
140. See supra note 7.
141. Note that whether a cloud service provider is classified as an RCS has no bearing on whether that provider is also classified as an ECS. See supra Part II.B.1. Thus, it is possible that a provider could be considered both an ECS and an RCS, and thus subject to both 18 U.S.C. § 2703(a) and (b).
142. Id. § 2703(d).
144. Id. § 2705(a)(2)(A)–(E).
delayed notice, the government can utilize the D order’s lower specific and articulable facts standard.

The result is that under § 2703(b), the government may access the contents of cloud-stored documents by using a specific and articulable facts standard and often may delay notification to the target user. In other words, the SCA allows the retrieval of content of electronic communications held by RCSs, affording less protection than that provided by a warrant requirement.


Section 2703(c) allows the government to require an ECS or RCS to disclose records and other information pertaining to a user of the service. Depending on the types of records or information the government seeks, § 2703(c) provides different levels of protection. If the government seeks basic subscriber information (such as name, address, or length of service), it needs only to obtain an administrative subpoena. For other subscriber information, not including content, the government must procure a warrant or use a D order.

Section 2703(c) is consistent with the understanding that non-content information is less protected than content. In the cloud storage context, non-content information could conceivably include file names, file sizes, file types, storage date, last access date, document versions, deleted documents, or other metadata. The government could use this wealth of information to build a rich picture of the user’s habits, or even to reveal something about the content of the document. File names are often descriptive and, when coupled with the file type and storage date, may provide information concerning the “substance, purport, or meaning” of the document. Under current judicial interpretation, this information is acquirable under § 2703(c) even though in the aggregate it may provide information about content.

C. ECPA IS INSUFFICIENT TO PROTECT CLOUD STORAGE

ECPA’s initial purpose was to balance privacy interests with

---

146. Id. § 2703(c)(1)(E).
147. Id. § 2703(c)(1)(A)-(B). The government may also access content if it has the consent of the subscriber. Id. § 2703(c)(1)(C).
148. 18 U.S.C. § 2510(8) (2012). For example, a file named “guest_list_house_party_Apr_20.xlsx” that is updated consistently is likely to contain a list of guests expected to attend a house party on April 20. Because this is the user’s document, one can infer that the party will be occurring at the user’s house on April 20.
149. See United States v. Perrine, 518 F.3d 1196, 1204–05 (10th Cir. 2008) (“Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment’s privacy expectation.”); United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (“[E]-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit 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.”).
legitimate law enforcement needs and to provide Fourth Amendment-like safeguards for stored electronic communications. But as it pertains to cloud storage, it appears that this purpose is not met. First, it is unclear whether cloud storage is considered an electronic communication. Second, even if it is, the nature of cloud storage means that the government can often access the contents of users’ files under a reasonable and articulable suspicion standard—much lower than the probable cause standard of a warrant.

Applying a lower standard makes no sense, as documents held in cloud storage can be just as revealing as the information stored in emails, and perhaps even more so. Letters, financial documents, reports, and personal documentation can all be stored in the cloud. Allowing the government to access such documents with merely a court order contravenes the traditional protections that have been afforded to such documents.

Further, cloud-stored documents losing protection after being stored for 180 days is inconsistent with how users expect cloud storage to operate. As online storage becomes more ubiquitous and less expensive, users may store documents for longer periods of time. This is not indicative of abandonment, but simply a result of the increased utility and availability of technology. It would be unreasonable to suggest that documents stored in a home office for six months suddenly lose their Fourth Amendment protection—why should documents stored online be any different?

Fortunately, Congress can amend ECPA, and there are a number of proposed bills that seek to simplify and strengthen protections for electronic communications.

III. NECESSARY ECPA REFORM

The call for ECPA reform is not new, but Congress has yet to amend the statute. Still, there are a number of proposed bills on the table, and all of these bills aim to simplify the SCA and expand protections for the content of electronic communications. This section identifies three critical amendments in the proposed bills that would increase protections for electronic communications and suggests two additional amendments that would aid in applying the SCA specifically to cloud storage.

---

150. See S. REP. NO. 99-541, at 1–3 (1986); Kerr, supra note 115, at 6.


A. THREE CRITICAL ECPA AMENDMENTS TO PROTECT CLOUD STORAGE

The proposed bills seeking to reform ECPA would update the SCA to simplify its application and bring its protections to modern electronic communications.

1. Remove Disparate Treatment of Information Stored with an ECS or RCS

Almost every proposed ECPA reform bill recognizes the need to harmonize the treatment of information held by different types of service providers. These bills do not completely remove the distinction between ECSs and RCSs, but they do treat them equally for purposes of government access. The proposed bills ensure a universal level of protection for electronic communications and eliminate the need to distinguish between an ECS and RCS.

Universal treatment of service providers is an important change because the ECS-RCS distinction determines what level of protection is afforded to electronic communications. Some service providers do not fall clearly into one category or the other and may be simultaneously subject to different standards. Further, providing different levels of protection based solely on what kind of entity is handling or processing a communication creates inconsistencies. If the content of a communication should be protected, it should be protected regardless of whether the service provider simply provides a conduit for the communication (ECS) or stores the communication on its servers (RCS). Treating all service providers the same creates the common-sense result that a given type of information is equally protected in all circumstances.

Eliminating this distinction also improves protections for cloud storage. Since cloud storage providers arguably operate as RCSs, with a correspondingly lower level of protection, removing this distinction increases the protections afforded to cloud storage by treating cloud storage providers the same as ECSs.

2. Require a Warrant for All Content Information

Most proposed bills incorporate a warrant standard for accessing content information, essentially codifying Warshak. When introducing the Electronic Communications Privacy Act Amendments Act of 2013, Senator Leahy explained that "[t]oday, we use our email accounts as digital filing cabinets, where we store many of the personal documents and sensitive information that the Fourth Amendment was meant to protect. This bill takes an essential step toward ensuring that the private life of


Americans remains private."

Requiring a warrant to access stored content recognizes that the cyber-difference of online storage is not sufficient to eradicate privacy rights. This requirement is a substantial change, as the SCA currently allows the government to obtain content information without a warrant in two ways: (1) from an ECS when the communication has been in storage more than 180 days, and (2) from an RCS.\(^\text{156}\) Given that content information is particularly sensitive and is generally subject to higher protections, the government should be required to meet the probable cause standard and obtain a warrant to access such information.

The warrant requirement would also increase protections for cloud-stored documents. Since cloud storage service providers are most likely classified as RCSs, the government can easily obtain cloud-stored documents without a warrant under the current SCA.\(^\text{157}\) The addition of a warrant requirement for all content would protect cloud-stored documents in more circumstances and is consistent with the understanding that content information should be highly protected.

3. Eliminate the 180-Day Standard

Eliminating the 180-day distinction is a common fixture of ECPA reform efforts.\(^\text{158}\) The 180-day rule is "outdated" and no longer reflects the reality of how most users interact with the Internet.\(^\text{159}\) Recognizing that privacy protections should not be obviated by the mere passage of time brings the law into alignment with modern practices.

The SCA currently provides different legal standards depending on whether a communication has been stored for more or less than 180 days.\(^\text{160}\) Data that was originally protected by a warrant requirement loses its protection and can be acquired by a lesser standard once it has been stored for more than 180 days.\(^\text{161}\) This standard was developed based on an understanding of the way email worked in 1986\(^\text{162}\) and does not currently reflect the way that email or cloud storage works. Current users are more likely to leave important emails in storage because there is no cost to doing so—there is no need or incentive to delete emails with modern email services. The 180-day standard is no longer workable because it does not

---


161. Id.

162. See Freiwald & Métille, supra note 131, at 1311–12.
take into account the fact that users treat email and other electronic communications like permanent filing cabinets.

Removing the 180-day standard is even more important for cloud storage because the purpose of cloud storage is to store documents for long-term access. Users store documents without worrying about how long they will be stored, but under the current SCA as soon as a document is stored with an ECS for more than 180 days the government can compel its disclosure without a warrant. Cloud-stored documents receive an appropriate level of protection by dropping the 180-day standard.

B. TWO SUGGESTED ECPA AMENDMENTS TO CLARIFY SCA APPLICATION TO CLOUD STORAGE

The proposed ECPA reform bills eliminate most of the confusion and difficulty of applying the SCA to modern electronic communications. However, these bills still do not directly address a few key differences between cloud storage and traditional communications. The following sections suggest two further amendments to more clearly place cloud storage under the SCA.

1. Explicitly Include Cloud Storage in the SCA’s Protections

Although the current definition of electronic communication is fairly broad, it does not clearly encompass cloud storage. Cloud-stored documents are not “communications” in the strictest sense of the word because they are generally not transmitted with the intent that they be received by anyone else. ECPA’s definition of electronic communication does not include a requirement that transmissions be sent with an intent that they be received, but it is possible courts could interpret “communication” to exclude cloud storage from any of the SCA’s protections.

The proposed bills do not specifically expand the definition of electronic communication. Instead, the bills alter the meaning of electronic storage. Essentially, these bills state that the government “may require the disclosure . . . of the contents of a wire or electronic communication that is in electronic storage with or otherwise stored, held, or maintained by the provider only if the governmental entity obtains a warrant . . . ." This clarifies when electronic communications are subject to protection, but does not clarify what counts as an electronic communication. Although cloud-stored documents are clearly stored by a provider, the bills refer only to “the contents of . . . electronic communication[s] . . . held . . . by the provider.” Cloud-stored documents would already need to be considered electronic communications before the expanded definition of storage would provide any additional support.

There are at least two methods to amend the SCA to ensure that its

163. See supra Part II.B.
164. See id.
166. Id.
protections extend to cloud storage. First, Congress could change the
definition of electronic communication to include cloud storage. A possible
addition that would clearly include cloud storage could be:

\[
\ldots \text{any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature, or any electronically stored sign, signal, writing, image, sound, data, or intelligence of any kind transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photoptical system...}
\]

This would clarify that the SCA would apply not just to transfers but
also to electronic documents held in storage that have been transferred by
some electronic system.

Second, Congress could create a new definition for “electronically
stored documents” and amend the SCA to include that phrase in addition
to wire and electronic communications. A workable definition of
“electronically stored documents” could be:

\[
\ldots \text{any sign, signal, writing, image, sound, data, or intelligence of any kind held in storage by a computer facility or related electronic equipment.}
\]

With this definition in place, any section of the SCA that protects the
contents of electronic communications would also protect electronically
stored documents. By amending the SCA to include such definitions,
Congress would clearly protect documents held in cloud storage.

2. Clarify the Type of Non-Content Data the Government Can Procure
Without a Warrant

The SCA currently allows the government to procure non-content
records about subscribers with less than a warrant.\(^ 167\) While this is
acceptable for some records, such as generic subscriber information that
can be characterized as legitimate business records, it raises concerns when
the records are more indicative of content, such as file names or file types.

The information enumerated in § 2703(c)(2) relates mostly to the
business relationship between the user and the service provider, which, as
legitimate business records, should not be subject to a warrant
requirement.\(^ 168\) However, § 2703(c)(1) further allows the government to
collect a “record or other information pertaining to a subscriber.”\(^ 169\) This
type of information may reach beyond traditional business records and into
the metadata of cloud-stored documents. Granted, the government must
procure a warrant or D order to retrieve such records, but a D order requires
only a showing of specific and articulable facts.

The proposed ECPA reform bills seem to address this issue by
amending § 2703(1) to be “subject to paragraph (2),”\(^ 170\) potentially limiting
the government’s access of non-content information to those types of information enumerated in § 2703(2). The amendments, however, do not change the “record or other information pertaining to a subscriber” language, which leaves open the possibility that the government can compel providers to disclose other non-content information.\footnote{Id. 2014[171]} To the extent that the government can use § 2703(1) to access metadata attributes of cloud-stored documents that are indicative of content, it should be subject to the higher warrant standard.

To properly protect such metadata, Congress should amend ECPA to clarify that only the records enumerated in § 2703(2) are available with a D order or other valid subpoena. Other non-content information or records should be subject to a warrant requirement. This would allow the government to access legitimate business records with a lower standard while still protecting users’ privacy interests in metadata that reveal content.

CONCLUSION

Society increasingly relies on cloud storage. Individuals are transferring more and more documents containing private information from home offices and personal computers to the cloud. The only substantial difference between these cloud-stored documents and the documents stored in a home office is their location. While such documents used to be under the robust protection of the Fourth Amendment, judicial application of the Third-Party Doctrine makes it unclear whether electronic communications are afforded Fourth Amendment protection. Congress addressed the issue of electronic communications by enacting ECPA in 1986, but the evolution of technology makes the provisions of ECPA confusing to interpret and difficult to apply, particularly in the context of cloud storage. Congress should amend ECPA to more clearly protect cloud storage.

There are a number of pending bills that seek to reform ECPA. These bills include amendments that clarify the SCA’s application and increase protections for modern electronic communications. The three critical amendments that these bills include are: (1) eliminating the distinction between an ECS and an RCS, (2) requiring a warrant for all content information, and (3) eliminating the 180-day rule. This Article suggests that in addition to these amendments, Congress should guarantee the SCA’s application to cloud storage by amending the SCA to (1) include cloud storage in the definition of “electronic communication,” and (2) require a warrant for non-content attributes of cloud-stored documents that reveal content.

Improved technology has informed and transformed virtually every part of our lives, and the courts have constantly struggled to apply our rigid constitutional framework. The Constitution’s Fourth Amendment protects
our papers, but our modern “papers” are stored in the cloud. It is important for these “papers” to be protected even while the courts continue to define the contours of Fourth Amendment application to modern electronic communications. Congress is on the right track with the pending ECPA reform bills, and incorporating this Article’s proposed amendments would embrace cloud technology and better protect cloud-stored information.