Self-storage Units and Cloud Computing: Conceptual and Practical Problems with the Stored Communications Act and Its Bar on ISP Disclosures to Private Litigants

JEFFREY PAUL DE SOUSA*

TABLE OF CONTENTS

INTRODUCTION .......................................... 248

I. HOW THE SCA WORKS ................................ 249

II. PROBLEMS WITH THE SCA’S APPLICATION IN CIVIL LITIGATION .... 251
   A. THE SCA’S DISTINCTION BETWEEN E-DISCOVERY AND TRADITIONAL DISCOVERY MAKES LITTLE SENSE .......................... 252
      1. The Standards for Both Types of Discovery Are Essentially Identical ......................................................... 252
      2. The Storage Unit Analogy ............................................ 254
         a. A Distinction Without a Difference ............................ 254
         b. Civil Discovery of Storage Units .............................. 257
         c. Criminal Discovery of Storage Units ....................... 259
   B. THE SCA’S FOCUS ON PRIVATE, CIVIL LITIGANTS IS OVERBROAD 260
      1. Fourth Amendment-Like Protections ............................ 260
      2. General Internet Privacy Protections .......................... 263
   C. THE SCA DOES NOT EFFECTIVELY PREVENT PARTIES FROM DISCOVERING ESI ...................................................... 264
      1. Courts May Simply Require Parties to Reformulate Subpoenas as Direct Production Requests ........................... 264
      2. Courts Have Adopted Other Routes Around the SCA, or Simply Ignored It ..................................................... 266

III. PROPOSED SOLUTION: AMEND THE SCA ............................ 268

CONCLUSION ............................................ 269

* Georgetown University Law Center, J.D. 2013. © 2013, Jeffrey Paul DeSousa. The author would like to thank Professor Gronvall, Professor Hitsky, and the Journal editors for their help on this project, as well as his family for their help more generally.
INTRODUCTION

The Stored Communications Act (SCA),1 passed by Congress in 1986 as part of the Electronic Communications Privacy Act,2 has proven to be a controversial piece of legislation. Although other articles have focused on the SCA’s outdated terminology, confusing language, and nonsensical provisions, this Note criticizes the SCA’s prohibition of certain disclosures by Internet service providers (ISPs) in the context of civil litigation between private parties.3

The SCA’s prohibition of third-party disclosure—even when the requesting party is armed with a court order or subpoena—poses several problems. First, it draws a distinction—where none should exist—between e-discovery4 and traditional discovery.5 If a civil litigant sought to subpoena a third party for information contained in the “real world,” rather than in the digital sphere, the courts would allow it. Yet courts have applied the SCA to prohibit requesting parties from subpoenaing third parties, such as cloud computing providers, to acquire the same information that would be discoverable were the information stored in the real world. This is a problem.

To demonstrate the point, this Note relies on an analogy—a self-storage unit.6 The courts have typically held that the contents of a storage unit are discoverable, even when the only route to accessing those contents was through a third-party subpoena. To the extent that the SCA treats the discovery of electronically stored information (ESI) differently than the law treats the discovery of the contents of the storage unit, it runs afoul of common sense.

Second, not only does it make little sense for the SCA to prevent discovery of material stored in the online equivalent of a storage unit, but the SCA is overbroad in its focus on private civil litigants.7 The purpose of the SCA is to ensure that individuals enjoy Fourth Amendment-like protections for their ESI, even if courts do not extend the Constitution to reach that ESI. For example, Congress wanted to prevent law enforcement from acquiring ESI without a warrant by requesting that information from an ISP with access to it, such as an e-mail provider. But when the government is not a party to the litigation—either as the prosecutor or in a civil-enforcement action—Congress’s original concern is not implicated and the SCA need not, and should not, apply. To the extent that the SCA may address other concerns, such as general Internet privacy, it is

---

3. This Note focuses only on the SCA as it applies to civil, private litigants. The SCA rightly applies to the government, even when it seeks discovery in the civil, rather than criminal, context.
5. See infra section II.A.
6. See infra section II.A.2.
7. See infra section II.B.
similarly overbroad when it governs civil litigation.

Third, even if preventing ISPs from disclosing information to private litigants was a laudable goal, the SCA fails on its own terms. That is because, although the SCA bars direct disclosure from an ISP to a requesting party, courts nevertheless allow discovery of the requested information. They merely do so through the backwards channel of Rule 34 requests for documents. This has harmful side effects. By forcing requesting parties to get ESI through production requests, instead of subpoenas, courts increase the likelihood that discovery disputes will be heavily litigated, simultaneously increasing the expense and time devoted to e-discovery—a field that is proving expensive and time consuming enough as it is. And in some instances, courts have either ignored the SCA entirely or manufactured bizarre solutions to the SCA’s bar on third-party disclosure, increasing the complexity of civil discovery and occasionally permitting more, not less, discovery of ESI.

This Note proceeds in three Parts. Part I briefly discusses how the SCA’s prohibition on ISP disclosures works. Part II takes a closer look at the three problems with the SCA identified above: its invalid distinction, overbreadth, and ineffectiveness. Part III proposes a solution: Congress should amend the SCA to include a subpoena exception allowing ISPs to disclose ESI to private litigants.

I. HOW THE SCA WORKS

The SCA has a number of provisions that protect the privacy of Internet users. For the purposes of this Note, two of those provisions are relevant because they prohibit ISPs from disclosing a user’s ESI to private litigants. First, SCA § 2702(a)(1) states that “a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service.” Second, § 2702(a)(2) further provides that “a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service . . . solely for the purpose of providing storage or computer processing services.”

8. See infra section II.C.
10. See 18 U.S.C. § 2701 (2006) (establishing criminal penalties for a person or entity that accesses without authorization, or exceeds authorization, a facility providing electronic communication services); id. § 2702 (prohibiting ISP disclosure of user data except in enumerated circumstances); see also id. § 2703 (establishing situations in which an ISP is required to make disclosures to a governmental entity, sometimes requiring a warrant and sometimes requiring less than a warrant).
11. Id. § 2702(a)(1).
12. Id. § 2702(a)(2).
The terms “electronic communication service”\textsuperscript{13} and “remote computing service”\textsuperscript{14} have been criticized because they insert needless confusion into the SCA\textsuperscript{15}. Courts and commentators generally agree, however, that those terms cover ISPs that provide the services in the following, noncomprehensive list: e-mail, social networking, and cloud-based storage. For instance, the SCA covers e-mail providers such as Hotmail\textsuperscript{16}, Gmail, AOL\textsuperscript{17} and Yahoo!; social-networking sites like Facebook and MySpace\textsuperscript{18}; and cloud service providers such as Google Drive, Dropbox, and Microsoft’s SkyDrive\textsuperscript{19}. The amount of private information (and potential evidence) stored by these ISPs is enormous\textsuperscript{20};
SCA § 2702 is therefore an impediment to a significant amount of desirable e-discovery. Although there are exceptions to the SCA’s bar on ISP disclosures, there is no exception that permits them to disclose ESI to a private party in civil litigation, even when that party is armed with a court order or subpoena. To enforce these provisions of the SCA, Congress created a civil cause of action under § 2707. An aggrieved party may recover actual and punitive damages from any “person or entity”—other than the United States—in violation of the SCA, along with litigation costs. The SCA also authorizes “such preliminary and other equitable or declaratory relief as may be appropriate.”

II. PROBLEMS WITH THE SCA’S APPLICATION IN CIVIL LITIGATION

This Part discusses three flaws with the SCA that warrant amending it. First, the SCA draws an unnecessary distinction between e-discovery and traditional discovery when it prevents third-party subpoenas of ESI. This is illustrated by an analogy to a real world self-storage unit. But that is not to say that there are no distinctions between e-discovery and traditional discovery: it is only to say that those distinctions should not matter for the particular aspect of the SCA, § 2702, which bars ISPs from disclosing ESI to private, civil litigants. Second, the SCA’s bar on these subpoenas does not further the SCA’s goals—either its attempt to create Fourth Amendment-like protections for ESI or to create

received by federal government agencies each year. The amount of stored information continues to grow exponentially.” (citations omitted)).

21. See In re Subpoena Duces Tecum to AOL, LLC, 550 F. Supp. 2d at 611 (“[T]his Court holds that State Farm’s subpoena may not be enforced consistent with the plain language of the Privacy Act because the exceptions enumerated in § 2702(b) do not include civil discovery subpoenas.”); FTC v. Netscape Commc’ns Corp., 196 F.R.D. 559, 561 (N.D. Cal. 2000) (“There is no reason for the court to believe that Congress could not have specifically included discovery subpoenas in the statute had it meant to.”); O’Grady v. Superior Court, 44 Cal. Rptr. 3d 72, 85 (Cal. Ct. App. 2006) (“A subpoena is not enforceable if compliance would violate the SCA. Any disclosure violates the SCA unless it falls within an enumerated exception to [the] general prohibition.”). The government, on the other hand, can get ESI with a subpoena (or less) in certain circumstances. See 18 U.S.C. § 2703.

22. See 18 U.S.C. § 2707(a) (“Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.”). The Ninth Circuit discussed the civil cause of action in Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2003), amended by 359 F.3d 1066 (9th Cir. 2004). The SCA also criminalizes conduct not relevant to this Note. See 18 U.S.C. § 2701(a)–(b) (making it a crime to “intentionally access[] without authorization a facility through which an electronic communication service is provided” or “intentionally exceed[] an authorization to access that facility,” and attaching penalties including fines and imprisonment).


24. Id. § 2707(b)(1).

25. The Fourth Amendment states: “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.” U.S. CONST. amend. IV.
general Internet privacy protections. Third, even assuming these other problems were not present, the SCA’s bar on ISP disclosures is ineffective.

A. THE SCA’S DISTINCTION BETWEEN E-DISCOVERY AND TRADITIONAL DISCOVERY MAKES LITTLE SENSE

Conceptually, there is no difference between e-discovery and traditional discovery that would justify the SCA’s bar on ISP disclosures to private litigants.26 After all, why should it matter whether a “smoking gun” document exists in hard copy or as a PDF?27 And why should it matter whether the document is stored in a company’s self-storage unit or in the company’s Google Drive account? Either way, if the document is relevant and nonprivileged, a requesting party should be permitted to access it.

But when courts and commentators manufacture a distinction between the hard copy and the digital versions of that document, they make e-discovery needlessly complex and risk formulating bad policy. To the extent that “digital is different,”29 it is not so different that the SCA’s bar on ISP disclosures should stand in the face of a subpoena. This Part advances two arguments for this proposition: (1) the standards of e-discovery and traditional discovery are otherwise identical and (2) any distinctions that do exist cannot survive scrutiny when we consider that ESI stored in the cloud is no different from information contained in a storage unit.

1. The Standards for Both Types of Discovery Are Essentially Identical

The standard governing the scope of e-discovery is the same standard that governs traditional discovery: relevance.30 Rule 26(b)(1) states that: “Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party’s claim or defense—including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter.”31

---

26. This is not so different from a point recently made by the Ninth Circuit that “[t]he government’s surveillance of e-mail addresses... may be technologically sophisticated, but it is conceptually indistinguishable from government surveillance of physical mail.” United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2007) (emphasis added).

27. A Portable Document Format (PDF) is a type of electronic document.


30. See Fed. R. Civ. P. 26. In 2006, the Advisory Committee amended the Federal Rules to reflect the changing nature of civil discovery and the emergence of e-discovery as a prominent discovery issue. See Fed. R. Civ. P. 26 advisory committee notes. Specifically, the Rules now contain the term “electronically stored information,” which is used in both Rules 26 and 34.

31. It goes on to state, “For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action. Relevant information need not be admissible at the trial if the
Applying this standard, courts have permitted discovery of relevant ESI contained on litigants’ social-networking pages and in cloud-based e-mail.32

Likewise, other discovery standards apply equally to both e-discovery and traditional discovery. For instance, the duty to preserve requires a potential litigant to preserve all forms of relevant evidence33 and attaches when litigation becomes reasonably foreseeable.34 A party may seek sanctions for spoliation of evidence under identical circumstances.35 And the same privilege and work-product protections apply to ESI as they do any other form of evidence.36 Although Rule 26 identifies some distinctions between ESI and other types of evidence discussed below,37 those distinctions are not significant enough to justify the different treatment that the SCA has afforded ESI and real world evidence.
2. The Storage Unit Analogy

Storage of ESI in the cloud or on a company’s in-house servers is no different from storage of traditional forms of information in a storage unit. A storage unit is an empty room that can be rented from a storage facility company such as Simply Storage or Extra Space Storage, for purposes of storing physical items. To rent a unit, an individual signs a contract with the storage facility that typically runs on a monthly basis.

Once the individual has rented the storage unit, he can use it to store any materials he pleases, within the bounds of the contract. Storage units are often used by people who are moving houses or apartments and require temporary storage for their possessions. But storage units may also be used by individuals or corporations for any reason that a person might wish to store materials in a safe, secure environment.

The storage unit is a useful analogy to storage of ESI for three reasons. First, there is no difference between a storage unit in the real world and digital storage of ESI, either functionally or conceptually. Second, courts permit private civil litigants to obtain discovery of material contained in storage units, whereas the SCA bars similar discovery of ESI. Third, courts have recognized a Fourth Amendment right in storage units, which should also apply to cloud storage. Because there is no rational justification for a distinction between ESI and physical evidence, the SCA is flawed.

a. A Distinction Without a Difference. The only distinction between a real world storage unit and a server farm belonging to a cloud computing service provider is that the former’s storage space is physical, rather than digital. But this is a distinction without a difference, because the content stored in those spaces—that is, the ideas conveyed by the hard copy or ESI materials—is the same. For instance, the meaning of a document does not change whether it is stored as a PDF on a server or printed in paper form. The content, or substance,
of the document remains unchanged when it gets printed, and it is the content that matters.44

The cloud, just like a storage unit, is merely a method of storing data. Now, the particular storage method that an individual or a corporation uses to store its data may have practical effects in litigation.45 The difference between physical and digital storage should not govern whether the data is discoverable. Rather, that determination should be made—as discussed above—based on the same factors that have governed since the genesis of Rule 26: material is discoverable if it is relevant and nonprivileged.

Arguably, the cloud is different from a storage unit because it has an almost unlimited storage capacity, whereas the storage unit is limited by its square footage. Although this is beyond dispute, it should not matter: the physical data and materials contained in a storage unit may reveal information about a person or corporation that is every bit as personal and intimate as the ESI contained in the cloud. A storage unit can contain address and appointment books, diaries and journals, family photographs, business records, and any number of revealing pieces of information. A storage unit may also contain information that the cloud cannot because the storage unit permits storage of uniquely physical materials—for instance, a piece of valuable jewelry that may be the subject of civil litigation.

The situation is no different for a company that chooses to store its hardcopy business files in a storage unit. A storage unit can accommodate thousands of pages of sensitive documents, ranging from those containing confidential intellectual property to those containing other business secrets. If the only distinction between the cloud and a storage unit is that the cloud has greater storage capacity, that distinction is inconsequential because it ignores that the files stored in hardcopy can be every bit as critical—and as private—as those stored as ESI.

Of course, there are certain differences between discovery and e-discovery. The drafters of the Federal Rules recognized that e-discovery is different in four ways: First, a litigant may possess vast quantities of ESI, whereas physical forms of evidence have inherent quantity limitations;46 second, ESI includes information “not contained within its four corners,” that is, metadata;47 third,
ESI is more durable and may persist even after it is “deleted” from a hard drive; and fourth, e-discovery may involve costly retrieval, restoration, or translation before it is useable.

But none of these distinctions suggests that ESI should not be discoverable in the general case or that ISPs should be prohibited from disclosing ESI. They do suggest that courts should account for special ESI considerations, such as cost and proportionality, when making discovery rulings. That is why Rule 26(b)(2)(B) provides for an exception to e-discovery in certain circumstances, for instance, when a producing party successfully argues that the ESI is “not reasonably accessible because of undue burden or cost.” The courts have held that this exception applies when, for example, ESI is contained on backup tapes and the cost of recovery is disproportionate to the likely importance of the material.

Is this exception for e-discovery really any different from the conventional exception Rule 26 provides for overly burdensome traditional discovery? Rule 26(b)(2)(C)(i) states that the court must limit discovery when “the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive,” and Rule 26(b)(2)(C)(iii) requires limitations when “the burden or expense of the proposed discovery outweighs its likely benefit, considering the


48. Payne, supra note 46, at 856 (citing Scheindlin, supra note 46, at 3, and Moore et al., supra note 47, § 37A.03[3]) (explaining that “[d]eleted electronic documents remain recoverable on a computer’s hard drive until a new file overwrites it” and “[r]etrieval of deleted documents may require extensive time and money”).

49. Id. (citing Scheindlin, supra note 46, at 3). Another difference, not noted by the drafters, is the relative ease of uploading files to the cloud as opposed to the potentially burdensome requirement of physically depositing items in a storage unit. Although this observation is invariably true, the relevant inquiry is whether the space to be searched can possibly contain sensitive information. To this end, a storage unit can easily contain private information, especially in the event that a person is using a storage unit to store the contents of a home during a move. It is hard to imagine a more sensitive collection of items and information than the contents of a person’s home, which otherwise would remain strictly private.


52. See, e.g., Hagemeyer N. Am., Inc. v. Gateway Data Scis. Corp., 222 F.R.D. 594, 603 (E.D. Wis. 2004) (holding that producing party would produce a sample of its backup tapes, at which point the court would determine whether production was so disproportionate to the benefit that costs should be shifted to the requesting party).


needs of the case, the amount in controversy, the parties’ resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues.\textsuperscript{55} These provisions apply equally to e-discovery and traditional discovery. The “burden or expense” language of Rule 26(b)(2)(C)(iii) sounds remarkably similar to Rule 26(b)(2)(B)’s “not reasonably accessible because of undue burden or cost” language.\textsuperscript{56} So although Rule 26 at first blush appears to treat e-discovery and traditional discovery differently in limited regards, those distinctions are not so meaningful as to justify the SCA’s bar on ISP disclosures.

Ultimately, a person who rented a storage unit to store the contents of his home while he moved houses would surely think that those contents were extremely personal and worthy of privacy protection. As a result, there is no unique characteristic of ESI that warrants its receipt of greater privacy protections than the physical material held in a storage unit.

\textbf{b. Civil Discovery of Storage Units.} As discussed below, courts have permitted civil discovery of data and documents within storage units in response to both direct requests for production under Rule 34\textsuperscript{57} as well as third-party subpoenas under Rule 45. It goes without saying that a requesting party may make a direct production request for material contained within the producing party’s storage unit. In such a case, the storage unit is within the producing party’s control, and the court will expect the producing party to comply with the Rule 34 request to the extent that the requested material is discoverable.

Yet a Rule 34 request may not be the most efficient way of obtaining information for a couple of reasons. For one, a producing party may be unwilling to comply with the request and may raise any number of objections that could drag out the litigation and frustrate the requesting party’s discovery objectives. For another, a producing party may no longer have access to the evidence. In the storage unit example, the producing party may have lost his key

\begin{itemize}
\item \textsuperscript{55} \textit{Fed. R. Civ. P. 26(b)(2)(C)(iii)}.
\item \textsuperscript{56} \textit{Fed. R. Civ. P. 26(b)(2)(B)}.
\item \textsuperscript{57} \textit{Rule 34(a) provides that}:
\begin{itemize}
\item (a) \textbf{In General.} A party may serve on any other party a request within the scope of Rule 26(b):
\begin{enumerate}
\item to produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the responding party’s possession, custody, or control:
\begin{itemize}
\item (A) any designated documents or electronically stored information—including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations—stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form; or
\item (B) any designated tangible things; or
\end{itemize}
\item (2) to permit entry onto designated land or other property possessed or controlled by the responding party, so that the requesting party may inspect, measure, survey, photograph, test, or sample the property or any designated object or operation on it.
\end{enumerate}
\end{itemize}
\end{itemize}
to the storage unit lock. Or, to use a digital example, a producing party may have forgotten his e-mail or cloud service password. And a party willing to spoliate evidence can do so in response to a Rule 34 request but not a subpoena. 

When such circumstances arise, the requesting party may wish to subpoena the third party with access to the evidence. Rule 45 states that a requesting party may compel a third party to “produce designated documents, electronically stored information, or tangible things in that person’s possession, custody, or control; or permit the inspection of premises.”

The Practice Commentaries to Rule 45 recognize that a subpoena is a desirable discovery tool, particularly for acquiring access to real property (such as a storage unit). In providing guidance to the Rule, they state that “[a]n inspection of premises is allowed by the Federal Rules of Civil Procedure on the same terms and through the same devices that a production of documents is, both as against a party, where Rule 34 governs, and against a nonparty, where Rule 45(a)(1)(c) governs.” Importantly, they add that inspection of property may “now be compelled by subpoena, dispensing with the need of a separate action (as prior law required) to secure the inspection of premises controlled by a nonparty. The subpoena would be directed to the person who has control of the premises and the authority to permit entry and inspection.”

A storage unit fits perfectly within this framework.

The courts have agreed. One category of cases deals with subpoenas actually directed to third-party storage facilities. For example, In re Prosser discusses evidence produced by Extra Space Storage in response to a bankruptcy trustee’s subpoena for documents. And the court in In re VisionAmerica, Inc. Securities Litigation entered a consent order allowing the plaintiffs to access and copy documents abandoned by the defendant in a self-storage unit. Although this was a consent order, not a third-party subpoena, the circumstances implied that the storage facility needed to grant access because the producing party had abandoned the material in the storage unit and lacked access to it. These cases therefore stand for the proposition that a third-party storage facility may be subpoenaed to compel documents contained within a self-storage unit or to grant access to the unit.

Storage facilities have acknowledged as much. Regional and national storage facilities Simply Storage and Public Storage both warn customers in their privacy policies that “[w]e may access, monitor, use, or disclose your Informa-

58. See, e.g., FED. R. CIV. P. 45 advisory committee notes.
59. FED. R. CIV. P. 45(a)(1)(A)(iii). Rule 45 was amended in 2006 to include its current reference to “electronically stored information.” See FED. R. CIV. P. 45 advisory committee notes.
60. Id.
61. Id.
64. See id.
tion to do things like... comply with the law or respond to lawful requests or legal process, such as a court order, subpoena, search warrant or other legal requirements of any government authority.”

A second category of cases deals with subpoenas directed at third parties with access to a storage unit, where the third party is not the storage facility itself. In *Food Lion, Inc. v. United Food & Commercial Workers International Union*, the Court of Appeals for the District of Columbia Circuit upheld a contempt order for failure of a third party to produce all relevant records contained in an off-site storage facility in response to a subpoena. Likewise, in *In re Asbestos Products Liability Litigation*, the district court ordered the requesting plaintiff to reimburse a third party for costs incurred while responding to a subpoena for documents contained in a storage facility. And in *Synopsys, Inc. v. Ricoh Co.*, the district court granted the defendants’ Rule 34 production request for “supervised access to the storage facility” but further stated that it “would permit Defendants to issue a subpoena to [the third party], specifically targeted at the documents at the storage facility” in the event that the plaintiff lacked access to the storage facility. Still other cases approved third-party subpoenas for documents contained in storage facilities.

c. Criminal Discovery of Storage Units. Although not directly applicable to the context of civil litigation between private parties, the courts have uniformly recognized that individuals have a reasonable expectation of privacy in their storage units for purposes of the Fourth Amendment. This means that the government generally must obtain a warrant before it can access a defendant’s

66. 103 F.3d 1007, 1020 (D.C. Cir. 1997).
70. See, e.g., 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.’” (citing United States v. Salinas-Cano, 959 F.2d 861, 864 (10th Cir. 1992))); United States v. Johns, 851 F.2d 1131, 1134–35 (9th Cir. 1988) (holding that a sneak-and-peek warrant authorizing the FBI to search a storage unit violated the Fourth Amendment); see also United States v. Smith, 353 F. App’x 229, 230–31 (11th Cir. 2009) (holding that defendant forfeited his reasonable expectation of privacy when his contract with the storage facility permitted the facility management to inspect and upkeep his storage unit in certain circumstances and when the facility manager had opened the unit under such circumstances and then informed the police about weapons contained within); United States v. Lnu, 544 F.3d 361, 365–66 (1st Cir. 2008) (holding that the defendant forfeited his reasonable expectation of privacy in a storage locker in a storage facility when he stopped making rent payments) (citing cases); United States v. Dilley, 480 F.3d 747, 750 (5th Cir.
storage unit.

This point—that an individual has a reasonable expectation of privacy in his storage unit—is important because of why the expectation is considered reasonable. Courts hold that, by renting the unit and placing a lock on it, the individual has taken steps sufficient to ensure that the contents of the storage unit will remain private.71 This is no different from cloud-based storage. When a person sets up a Google Drive account, he is asked to input a password that ensures he alone has access. Granted, Google could access his ESI in violation of the user’s contract, just as the storage facility could cut the lock on his storage unit. But these possibilities do not make the user’s expectation of privacy unreasonable.72

When courts conceive of e-discovery as being fundamentally different from traditional discovery, they risk watering down the Fourth Amendment’s protection of ESI. A person should have the same Fourth Amendment privacy interest in his information in the cloud as he does in his information in a storage unit. The SCA’s distinction between ESI and physical information may therefore have constitutional implications.

B. THE SCA’S FOCUS ON PRIVATE, CIVIL LITIGANTS IS OVERBROAD

The second flaw in the SCA is that it is overbroad in two respects, at least as it applies to private litigants. First, by preventing disclosure to civil litigants, the SCA goes further than the Fourth Amendment would, and the SCA was designed to provide Fourth Amendment-like protections for the digital realm. Second, to the extent that the SCA otherwise furthers general Internet privacy protections, its bar on ISP disclosures to civil litigants does not advance that goal.

1. Fourth Amendment-Like Protections

Scholarly consensus is that the SCA was designed in large part to afford a defendant the same Fourth Amendment protections over his ESI that he would enjoy over his real-world possessions, such as the possessions stored in a storage unit.73 The legislative history states that the SCA “represents a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies,”74 and courts have understood that “a fundamen-
tal purpose of the SCA [was] to lessen the disparities between the protections given to established modes of private communication and those accorded new communications media. But is this a valid justification for the SCA’s bar on ISP disclosures to private litigants?

For starters, this goal may soon be defunct because courts have begun to recognize that the Fourth Amendment applies to the digital realm. In United States v. Warshak, for example, the Sixth Circuit held that “a subscriber enjoys a reasonable expectation of privacy in the contents of emails ‘that are stored with, or sent or received through, a commercial ISP.’” As a result, “[t]he government may not compel a commercial ISP to turn over the contents of a subscriber’s emails without first obtaining a warrant based on probable cause.” In reaching this conclusion, the court analogized to a hotel room, in which a person has a reasonable expectation of privacy even though a maid may enter to clean the room, and to an apartment, where the same is true even though a handyman may enter to fix a leaky faucet. These examples are similar to a storage unit, and the court’s approach is correct.

Unfortunately, not all courts have followed this approach. In Rehberg v. Paulk, the Eleventh Circuit granted the defendants—the district attorney and his chief investigator—qualified immunity because they did not violate a clearly established Fourth Amendment right when they subpoenaed the plaintiff’s ISP to obtain his e-mails. Other courts have relied on the third-party disclosure rule to hold that an e-mail loses its Fourth Amendment protection as soon as it is

75. O’Grady v. Superior Court, 44 Cal. Rptr. 3d 72, 87 (Cal. Ct. App. 2006); see Theofel v. Farey-Jones, 359 F.3d 1066, 1072 (9th Cir. 2004) (“Like the tort of trespass, the Stored Communications Act protects individuals’ privacy and proprietary interests. The Act reflects Congress’s judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility.”).

76. See, e.g., United States v. Warshak (Warshak II), 631 F.3d 266, 288 (6th Cir. 2010) (“Accordingly, we hold that a subscriber enjoys a reasonable expectation of privacy in the contents of emails ‘that are stored with, or sent or received through, a commercial ISP.’” (citing United States v. Warshak (Warshak I), 490 F.3d 455,473 (6th Cir. 2007))); United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996) (holding that defendant had a reasonable expectation of privacy in e-mails sent and stored with AOL because AOL provided contractual privacy protections). There are cases holding that a defendant did not have a reasonable expectation of privacy in the contents of an e-mail once it was received by its recipient. See, e.g., United States v. Jones, 149 F. App’x 954, 959 (11th Cir. 2005) (“[A]n individual sending an e-mail loses ‘a legitimate expectation of privacy in an e-mail that had already reached its recipient.’”); United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) (“[Individuals] may not, however, enjoy . . . an expectation of privacy in transmissions over the Internet or e-mail that have already arrived at the recipient.”). But those cases did not look at whether the defendant had an expectation of privacy in the contents of that communication while it was stored in the cloud or whether information that was stored solely on the cloud—and not communicated to a third party—would be protected.

77. Warshak II, 631 F.3d at 288.

78. Id.

79. Id. at 287 (citing United States v. Allen, 106 F.3d 695, 699 (6th Cir. 1997)).

80. Id. (citing United States v. Washington, 573 F.3d 279, 284 (6th Cir. 2009)).

81. See 611 F.2d 828, 847 (11th Cir. 2010).
delivered to its recipient, reasoning that a person lacks a reasonable expectation of privacy when he shares the information he seeks to keep private with a third party.82

Noted Fourth Amendment scholar Orin Kerr has been critical of these decisions,83 and he is quite right. He admits that—like a letter that is mailed to a third party—an e-mail delivered to its recipient loses Fourth Amendment protection.84 But he argues that the e-mail (which is a copy) delivered to the recipient is different from the e-mail (an original of sorts) stored in the sender’s outbox or with the ISP; the mere fact that the copy has lost its protections does not mean that the government can break into the sender’s home to obtain the original from which the copy was made.85 Under Professor Kerr’s theory, the government could only obtain the e-mail with a subpoena of the e-mail’s recipient.86 It could not obtain the e-mail from the ISP. So if the SCA is meant to create Fourth Amendment-like protections, why does it prevent the ISP from disclosing the contents of the e-mail (when the government cannot subpoena the ISP under the Fourth Amendment anyway) but not prevent the recipient of the e-mail from doing so?

So, under the proper view of the Fourth Amendment, the SCA is unnecessary because communications stored in the cloud will be protected even without the statute. Even if the SCA pursues a worthy goal, it need not bar ISPs from disclosing ESI in response to private-party subpoenas. That is because, to the extent the SCA was designed to mirror the Fourth Amendment, it goes further than the Fourth Amendment’s protections when it prohibits an ISP from disclosing information to a private litigant, not affiliated or working on behalf of the government. The Supreme Court has long held that the Fourth Amendment applies only to searches and seizures performed by the government, either state or federal.87 If Congress truly wanted the SCA to be a digital Fourth Amend-

82. See United States v. Jones, 149 F. App’x 954, 959 (11th Cir. 2005); United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004).
84. See id.
85. Id.
86. See id.
87. See United States v. Jacobsen, 466 U.S. 109, 113 (1984) (“This Court has . . . consistently construed [the Fourth Amendment] as proscribing only governmental action; it is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.” (citation omitted)); Walter v. United States, 447 U.S. 649, 656 (1980) (holding that a wrongful private search does not violate the Fourth Amendment); Coolidge v. New Hampshire, 403 U.S. 443, 489–90 (1971) (holding that evidence was properly admitted when police obtained evidence from the wife of the defendant); see also Sam Kamin, The Private Is Public: The Relevance of Private Actors in Defining the Fourth Amendment, 46 B.C. L. REV. 83, 85 (2004) (“[T]he Fourth Amendment’s coverage depends crucially on the scope of private actors’ conduct . . . . If an individual has allowed private actors access to [an] area, she generally will not be permitted to complain that her rights have been violated when the government seeks access to that area as well.”).
ment, it would have required the government to get a warrant before it could obtain ESI. Instead, the SCA permits the government to obtain ESI with less than a warrant in a broad number of situations. 88

So Congress actually got things entirely backwards. By not creating a private, civil subpoena exception, Congress placed strict limits on private discovery, something not within the Fourth Amendment’s scope. Congress then created broad exceptions for discovery of ESI by the government, something within the scope of the Fourth Amendment.

2. General Internet Privacy Protections

To the extent that the SCA was also designed as a general Internet privacy protection law, the SCA is also overbroad. The SCA “creates a zone of privacy to protect Internet subscribers from having their personal information wrongfully used and publicly disclosed by ‘unauthorized private parties.’” 89

Few would argue that this is not an admirable goal. Indeed, the United States has done far less to protect Internet privacy than other developed nations, such as Germany. 90 But the SCA goes further than necessary to achieve this goal. The SCA’s civil sanctions against persons or entities that violate its protections are likely a sufficient deterrent. The SCA unnecessarily applies to civil discovery. We generally think of civil discovery as exempt from societal notions of privacy. For example, everyone agrees that John Doe has no right to walk up to Jane Doe in the street and compel her to produce the contents of her e-mail inbox for his inspection. But we have recognized that once John sues Jane, he has a right to view e-mails relevant to his claim because society has an interest in effectively resolving private disputes in the judicial forum. 91

Even if Congress were concerned that confidential ESI would be disclosed in

88. See 18 U.S.C. § 2703(a) (2006) (government does not need a warrant to obtain the contents of a wire or electronic communication that has been held in electronic storage for more than 180 days); id. § 2703(b) (government can obtain the contents of a wire or electronic communication, held by a remote computing service, with an administrative or trial subpoena, or with a court order).


90. See Heather Horn, Germany’s War with Facebook and Google over Privacy, ATLANTIC (Dec. 2, 2011, 11:25 AM), http://www.theatlantic.com/international/archive/2011/12/germanys-war-with-facebook-and-google-over-privacy/248914/ (discussing Germany’s efforts to prevent social-networking sites from collecting user information); Kevin J. O’Brien, Despite Privacy Inquiries, Germans Flock to Google, Facebook and Apple, N.Y. TIMES (July 11, 2010), http://www.nytimes.com/2010/07/12/technology/12disconnect.html?_r=0 (“Strict privacy laws are a product of the post-World War II reconstruction, when German lawmakers restricted the use of personal information to prevent the government from singling out citizens and persecuting them.”).

91. See W.E. Aubuchon Co. v. Benefirst, LLC, 245 F.R.D. 38, 41 (D. Mass. 2007) (“Our courts have repeatedly reiterated that notice pleading standard relies on liberal discovery rules . . . and that it is now beyond dispute that broad discovery is a cornerstone of the litigation process contemplated by the Federal Rules of Civil Procedure.” (alteration in original) (quoting Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 311 (S.D.N.Y. 2003) (internal quotation marks omitted))).
discovery, the courts have a ready solution to the problem: protective orders. Rule 26 states that “[t]he court may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense” and sets out a number of protective safeguards a court may impose. These include “designating the persons who may be present while the discovery is conducted” and “requiring that a trade secret or other confidential research, development, or commercial information not be revealed,” among other things. As a result, courts can order that any documents produced during discovery shall be used only for the purposes of that litigation and impose a gag order otherwise. The availability of this remedy solves any general privacy concerns that may exist.

C. THE SCA DOES NOT EFFECTIVELY PREVENT PARTIES FROM DISCOVERING ESI

Even assuming that the SCA is pursuing valid goals with its bar on third-party subpoenas of ISPs, its third flaw is that it fails on its own terms because it is ineffectual. It misses its mark in two ways. First, courts have generally held that the SCA does not protect ESI itself but only the manner in which ESI is produced. So, although the SCA may be raised to quash a subpoena, it is no defense to a direct production request for ESI, which courts allow. Second, to facilitate discovery in the face of the SCA, courts have adopted bizarre measures that conflict with the purposes of the SCA and sometimes result in more, not less, disclosure of private information.

1. Courts May Simply Require Parties to Reformulate Subpoenas as Direct Production Requests

The SCA has not actually prevented requesting parties from obtaining relevant documents; it has merely slowed them down. Perhaps because courts are cognizant of society’s interest in permitting civil discovery and the importance of ESI in that process, they have rarely let the SCA stand in the way of discovery. One way they have permitted discovery is simply by requiring a

---


94. Id. 26(c)(1)(E).

95. Id. 26(c)(1)(G).

96. Even when a court quashes a subpoena on SCA grounds, the requesting party can always reformulate its request as a Rule 34 direct production request. This will likely increase discovery costs and time, as Rule 34 requests may be more heavily litigated.

requesting party to reformulate its third-party subpoena as a direct production request under Rule 34.98

In *Flagg v. City of Detroit*, the plaintiff subpoenaed nonparty service provider SkyTel for text messages sent by the defendants.99 Both SkyTel and the defendants filed motions to quash the subpoena, citing the SCA.100 The court first noted that “§ 2702 lacks any language that explicitly authorizes a service provider to divulge the contents of a communication pursuant to a subpoena or court order.”101 Therefore, for SkyTel to disclose the text messages to the plaintiff, the court said that the defendants must first consent, because § 2702(b)(3) permits disclosure “with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service.”102 Because the court was uncertain that it had the authority to compel the defendants to consent to disclosure by SkyTel,103 it instead ordered the plaintiff to “reformulate his third-party subpoena as a Rule 34 request for production directed at the Defendant.”104 At that point, the defendant would be required to request from SkyTel any relevant text messages that the defendant itself did not have physical possession of and to produce them to the plaintiff.

But as discussed above, Rule 34 requests often lack the efficacy and efficiency of the Rule 45 subpoena. What if the producing party no longer has access to the cloud because it forgot its password? Although the producing party could be forced to request the ESI from an ISP (as in *Flagg*), that is hardly the most efficient solution; it increases the number of people or entities involved, the number of correspondences required, the time from the initial request to the final production, and ultimately, the lawyers’ fees.

---

99. Id. at 348.
100. Id.
101. Id. at 350. The *Flagg* court observed that “the statutory language of the [SCA] does not include an exception for the disclosure of electronic communications pursuant to civil discovery subpoenas,” id. (alteration in original) (citing *In re Subpoena Duces Tecum to AOL, LLC*, 550 F. Supp. 2d at 611), and that “none of the exceptions set forth in § 2702(b) expressly permits disclosure pursuant to a civil discovery order obtained by a private party,” id. (internal quotation marks omitted) (citing U.S. Internet Serv. Provider Ass’n, *Electronic Evidence Compliance—A Guide for Internet Service Providers*, 18 Berkeley Tech. L.J. 945, 965 (2003)).
103. The court acknowledged that such authority would exist if the production request was made under Rule 34. *Flagg*, 253 F.R.D. at 366 (“Moreover, while Rule 34 and its attendant case law provide clear authority for insisting that a party consent to the disclosure of materials within its control, there is very little case law that confirms the power of a court to compel a party’s consent to the disclosure of materials pursuant to a third-party subpoena.”).
104. Id.; see also *Mintz v. Mark Bartelstein & Assocs.*, Inc., 885 F. Supp. 2d 987, 994 (C.D. Cal. 2012) (“Defendants may request documents reflecting the content of Plaintiff’s relevant text messages, consistent with the SCA, by serving a request for production of documents on Plaintiff pursuant to Rule 34.”).
What if the producing party wants to drag out the litigation by heavily contesting the direct production request? Although the court may have the power under Rule 34 to compel a producing party’s consent, this is yet another legal battle that the producing party might wage to slow down discovery. Additionally, there is always the possibility that a producing party will spoliate evidence in response to a production request. A subpoena has no such drawbacks because the opposing party generally has no power to prevent the third party from cooperating with the subpoena.

2. Courts Have Adopted Other Routes Around the SCA, or Simply Ignored It

Courts have fashioned other routes around the SCA as well. These routes occasionally lead to greater disclosure—even of nonrelevant ESI—than is necessary.

In Romano v. Steelcase Inc., the defendant sought a court order permitting it to access all of the plaintiff’s “current and historical Facebook and MySpace pages and accounts, including all deleted pages and related information.” The court briefly noted that the SCA “prohibits an entity, such as Facebook and MySpace from disclosing such information without the consent of the owner of the account.” Without discussing the SCA again in its opinion, the court seemingly took the route the Flagg court declined to take: it ordered the plaintiff to execute a consent form granting the defendant access to her social networking pages.

The substance of the court’s order is important. It directed that “Plaintiff shall deliver to Counsel for Defendant STEELCASE a properly executed consent and authorization as may be required by the operators of Facebook and MySpace, permitting said Defendant to gain access to Plaintiff’s Facebook and MySpace records, including any records previously deleted or archived by said operators.” This order is problematic because it permits greater discovery than Rule 26’s relevance standard does. It is unlikely that every Facebook or

106. Id. at 651.
107. Id. at 652 (emphasis added) (citing § 2702(b)(3), and Flagg, 252 F.R.D. 346).
108. One commentator has suggested that the Romano court simply ignored the SCA outright. See Ward, supra note 18, at 576, 578. I think that this is probably incorrect. The context of the opinion suggests that the court had considered the SCA and thought it would not bar ISP disclosure so long as the plaintiff consented. See Romano, 907 N.Y.S.2d at 657.
109. Romano, 907 N.Y.S.2d at 657; see also Juror No. One v. Superior Court, 142 Cal. Rptr. 3d 151, 159 (Cal. Ct. App. 2012) (“Thus, the question here is not whether respondent court can compel Facebook to disclose the contents of Juror Number One’s wall postings but whether the court can compel Juror Number One to do so. If the court can compel Juror Number One to produce the information, it can likewise compel Juror Number One to consent to the disclosure by Facebook. The SCA has no bearing on this issue.”).
110. Romano, 907 N.Y.S.2d at 657 (emphasis added).
111. A different New York Supreme Court judge later recognized as much. See Winchell v. Lopiccolo, 954 N.Y.S.2d 421, 424 (N.Y. Sup. Ct. 2012) (finding that the defendant’s request “for unrestricted access to Plaintiff’s Facebook page is overbroad”). In Winchell, the court attempted to
MySpace item the plaintiff had ever deleted was relevant to the litigation. Ironically, by circumventing the SCA, the court actually permitted greater discovery than it likely would have if the SCA did not exist; this is surely not what Congress intended.

Other courts have simply ignored the SCA entirely.112 The plaintiffs in Ledbetter v. Wal-Mart Stores, Inc.,113 sued Wal-Mart in tort. Wal-Mart issued subpoenas to a number of social-networking sites, seeking private messages and other information.114 The plaintiffs moved for a protective order on other grounds,115 but apparently no party raised the SCA issue. The court did not discuss it and denied the protective order.116 In Psychopathic Records Inc. v. Anderson,117 the plaintiffs subpoenaed Yahoo! and Hotmail to “to obtain and preserve the Defendant’s email correspondence to third parties relating to this action so that Plaintiffs may assess the amount of Defendant’s third party contacts and sales of infringing products.”118 The court did not utter a word about the SCA and denied the defendant’s motion to quash.119 As in Ledbetter, the defendant apparently failed to raise the SCA, and neither Yahoo! nor Hotmail filed motions to quash.120

These cases mean that the SCA has failed in its mission.121 Even if we assumed that Congress was correct that the SCA should be an impediment to
distinguish Romano on the ground that the requesting party there had first shown that the information on the plaintiff’s public pages contradicted its claims. Id. This seems like a nice way of saying that the Romano court simply got it wrong. After all, unless the Romano court thought that intentional spoliation had occurred (which it did not mention), it could have ordered an in camera review of the deleted evidence, or taken the less drastic step of ordering the plaintiff to retrieve its deleted information from Facebook, and then produce only the relevant documents to the defendant.


114. Id. at *1.

115. Id.

116. Id. at *2. The court’s failure to discuss the SCA is somewhat surprising given that the magistrate judge, Judge Michael Watanabe, has spoken on e-discovery and social media matters at CLE conferences. See, e.g., E-Discovery, Social Media Wrinkles and New Developments, NATIONAL CLE CONFERENCE (Sept. 8, 2011, 9:43 PM), http://nationalcleconference.com/tag/honorable-michael-j-watanabe/.


118. Id. at *1.

119. Id. at *2 (granting the motion to quash only to the extent it sought discovery of e-mail addresses not relevant to the litigation).

120. See id.

121. As one California appellate judge wrote in response to the majority’s holding that the plaintiff could be compelled to consent to disclosure by Facebook, “[t]his is arguably inconsistent with the spirit
civil discovery, it does not have that effect because courts are quick to find ways around it.

III. PROPOSED SOLUTION: AMEND THE SCA

The solution to these problems lies with Congress. It should amend the SCA to include a civil subpoena exception to § 2702’s bar on ISP disclosures to private, civil litigants.122 A new subsection, § 2702(b)(9), could be appended to the current list of exceptions under § 2702(b). It should state:

A provider described in subsection (a) may divulge the contents of a communication to a requesting party in response to a valid court order or discovery or trial subpoena, when the requesting party is a private person or private entity, not acting with or on behalf of a government official or government entity.

This would ensure that the SCA did not interfere with valid civil discovery attempts.

Moreover, the time is ripe to amend the SCA. In 2010, 2011, and 2013, Congress held several rounds of hearings regarding Internet privacy and the SCA,123 and in March 2011 and March 2013, Senator Patrick Leahy introduced


122. Other commentators have urged for the same amendment, albeit on different grounds. See Marc J. Zwilling & Christian S. Genetski, Criminal Discovery of Internet Communications Under the Stored Communications Act: It’s Not a Level Playing Field, 97 J. CRIM. L. & CRIMINOLOGY 569, 597–98 (2007); Burshnic, supra note 18, at 1289 (“A specified disclosure exception would clarify discovery standards for both courts and litigants while lessening the burden on providers and sites subject to the SCA.”). Zwilling and Genetski proposed the following amendment:

A non-governmental entity who is a party to pending criminal or civil litigation may petition the court in which such litigation is pending for an order requiring a service provider to disclose contents of electronic communications in electronic storage or contents of wire or electronic communications in a remote computing service and such order shall issue only if the requesting party can demonstrate that the requested information is relevant and material to the ongoing litigation and is unavailable from other sources, and both the subscriber or customer whose materials are sought and the service provider from whom the materials will be produced are provided reasonable notice and the opportunity to be heard. In the case of a State court, such a court order shall not issue if prohibited by the law of such state. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature, or compliance with such an order would cause an undue burden on such provider. In all cases, the service provider shall be entitled to cost reimbursement by the requesting party, as set forth in 18 U.S.C. § 2706.

Id. This proposed amendment is far lengthier and more complicated than necessary; however, it basically recites the entirety of the Federal Rules governing subpoenas. The amendment proposed in this Note should suffice to resolve the existing problems.

bills to amend it. Those bills, which have not yet been passed, unfortunately focused primarily on the SCA’s provisions governing disclosure to government entities. Any successful amendment would be much improved if it expanded its scope to include the proposed § 2702(b)(9). With the recent explosion of scholarship in this field and Congress’s obvious interest in the subject, now is as good a time as any to amend the SCA to repair its past shortcomings and to update it for the twenty-first century.

CONCLUSION

As currently written, the SCA draws an invalid distinction between e-discovery and traditional discovery; is overbroad in its focus on private, civil litigants; and does not effectively pursue its goals. This Note relies on the analogy of self-storage units to make the point that, as a conceptual matter, the SCA’s private subpoena bar is problematic because it unnecessarily treats e-discovery differently than traditional discovery. This view may have constitutional repercussions: if courts perceive ESI as being fundamentally different from traditional forms of information, they are more likely to deny Fourth Amendment protection to repositories of ESI.

The SCA is also flawed to the extent that its drafters wanted it to act as a digital Fourth Amendment because it is overbroad in its application to private litigants. Finally, as a practical matter, courts have taken unusual and harmful steps to permit discovery of ESI even in the face of the SCA, with the result that courts have simply compelled producing parties to sign consent forms or have issued disclosure orders that give requesting parties greater access than would occur in traditional discovery.

Accordingly, the SCA would better serve the interests of privacy and litigation if Congress amended it to create an exception for ISP disclosure to private, civil litigants in response to a court order or subpoena.

125. The 2013 version of the amendments has been voted out of committee; the likelihood that the bill will be passed is low. See S. 607: Electronic Communications Privacy Act Amendments Act of 2013, GOVTRACK.USA, http://www.govtrack.us/congress/bills/113/s607 (last visited Aug. 5, 2013).
126. S. 607 § 3; S. 1011 §§ 3, 5.