THE GEORGE WASHINGTON UNIVERSITY LAW SCHOOL
PUBLIC LAW AND LEGAL THEORY WORKING PAPER NO. 68

A USER'S GUIDE TO THE STORED COMMUNICATIONS ACT - AND A LEGISLATOR'S GUIDE TO AMENDING IT

Orin S. Kerr

Accepted Paper
GEORGE WASHINGTON LAW REVIEW
(Vol. 72, 2004)

A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It

Orin S. Kerr[*]

Introduction

The privacy of stored Internet communications in the United States is governed by a federal statute known as the Stored Communications Act ("SCA").[1] The SCA was enacted in 1986 as part of the Electronic Communications Privacy Act.[2] Despite its obvious importance, the statute remains poorly understood. Courts, legislators, and even legal scholars have had a very hard time making sense of the SCA.[3] The statute is dense and confusing, and few cases exist explaining how the statute works.[4] The uncertainty has made it difficult for legislators to legislate in the field, reporters to report about it, and scholars to offer scholarly guidance in this very important area of law.

This Article presents a user's guide to the SCA. My primary goal is to explain the basic structure and text of the Act so that legislators, courts, academics, and students can understand how it works—and in some cases, how it doesn't work. I hope to explain the nuts and bolts of the statute's many distinctions and dichotomies to reveal both the statute's dynamics and its drafters' choices. I will suggest that the statute works reasonably effectively, although certainly not perfectly. The SCA is a bit outdated and has several gaps in need of legislative attention, but by and large it reflects a sound approach to the protection of stored Internet communications. I will also explore some of the present controversies that surround how best

[*] Associate Professor, The George Washington University Law School.

[1] *See* 18 U.S.C. §§ 2701–2711 (2000). The statute has been given various names by different commentators. Its names have included: (1) the "Electronic Communications Privacy Act" or "ECPA" because it was first enacted as part of that statute; (2) "Chapter 121" because it has been codified in Chapter 121 of Title 18 of the United States Code; (3) the "Stored Wired and Electronic Communications and Transactional Records Access" statute or "SWECTRA" because that is the formal title given to Chapter 121 in Title 18; and (4) "Title II" because it was enacted as the second title of ECPA. For reasons too complicated and uninteresting to explain here, I find it easiest and simplest to refer to the statute as simply the Stored Communications Act, or "SCA."

[2] *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

[3] *See* Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 820–21 (2003) (citing cases).

[4] *See id.* at 821–26 (discussing the number of cases interpreting the SCA and explaining how the paucity of case law derives from the absence of a statutory suppression remedy).

to interpret the SCA. In particular, the recent United States Court of Appeals for the Ninth Circuit decision in *Theofel v. Farey-Jones*,[5] offers a new view of the SCA's basic structure that is quite different from the traditional understanding that the Justice Department has followed. Similarly, the United States Court of Appeals for the First Circuit is reviewing en banc a panel opinion in *United States v. Councilman*[6] that departs considerably from accepted understandings of the line between the SCA and the Wiretap Act. Future litigation on these issues appears inevitable, and those working with the SCA need to understand how the *Theofel* and *Councilman* depart from the traditional understanding.

In the final section of the Article, I will use my explanation of the SCA as a point of departure for analyzing how Congress should amend the statute in the future. I recommend four specific ways that Congress should rework the SCA to better protect the privacy of stored Internet communications, clarify its protections, and update the statute for the present. Specifically, I argue that Congress should: (1) raise the threshold the government must satisfy to compel the contents of certain Internet communications; (2) simplify the statute dramatically by eliminating the confusing categories of "electronic communication service" and "remote computing service"; (3) repeal 18 U.S.C. § 2701 because its primary effect has been to confuse the courts; and (4) restructure the remedies scheme for violations of the statute.

I. Why the Stored Communications Act Exists

To understand the SCA, it helps to begin by considering why Congress enacted the statute in the first place. We need to start with the Fourth Amendment and see why the architecture of the Internet raises several puzzling issues for the scope of Fourth Amendment protection. A brief excursion into how the Fourth Amendment applies to the Internet will explain the function and importance of the SCA.

The Fourth Amendment offers strong privacy protections for our homes in the physical world.[7] Absent special circumstances, the government must first obtain a search warrant based on probable cause before searching a home for evidence of crime.[8] When we use a computer

[5] Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004).

[6] United States v. Councilman, 373 F.3d 197 (1st Cir. 2004). As this Symposium was going to press, the First Circuit voted to rehear the case en banc and withdrew the panel opinion. *See United States v. Councilman*, No. 03-1383, 2004 WL 2230823 (1st Cir. Oct. 5, 2004).

[7] *See* Kyllo v. United States, 533 U.S. 27, 31 (2001).

[8] As Justice Scalia summarized in *Kyllo*: "At the very core of the Fourth Amendment stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion. With few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no." *Id.* (internal

network such as the Internet, however, a user does not have a physical "home," nor really any private space at all. Instead, a user typically has a network account consisting of a block of computer storage that is owned by a network service provider, such as America Online or Comcast. Although a user may think of that storage space as a "virtual home," in fact that "home" is really just a block of ones and zeroes stored somewhere on somebody else's computer. This means that when we use the Internet, we communicate with and through that remote computer to contact other computers. Our most private information ends up being sent to private third parties and held far away on remote network servers.[9]

This feature of the Internet's network architecture has profound consequences for how the Fourth Amendment protects Internet communications—or perhaps more accurately, how the Fourth Amendment may not protect such communications much at all. The law here remains unclear, and the details are mostly untested. However, the architecture of the Internet provides three reasons why it may be difficult under current doctrine for the Fourth Amendment to offer strong privacy protections online. These reasons explain why the significant privacy protections that apply to homes in the physical world may not apply to "virtual homes" in cyberspace, and why Congress has tried to fill this possible gap with the SCA.

The first reason is the uncertainty over whether and when Internet users can retain a "reasonable expectation of privacy" in information sent to network providers, including stored e-mails.[10] Internet Service Providers ("ISPs") act as third parties that hold and process a user's information on the user's behalf. The Supreme Court has repeatedly held, however, that the Fourth Amendment does not protect information revealed to third parties.[11] Several courts have applied this rationale and held that an Internet user does not retain a reasonable expectation of privacy in

quotations and citations omitted).

[9] *Cf.* United States v. Bach, 310 F.3d 1063, 1066–68 (8th Cir. 2002), *cert. denied*, 123 S. Ct. 1817 (2003) (considering the Fourth Amendment implications of a remote network search at an Internet service provider).

[10] I discuss the doctrinal arguments both for and against finding Fourth Amendment protection in remotely stored files in an amicus brief filed in the *Bach* case. *See* Brief of Amicus Curiae Professor Orin S. Kerr, United States v. Bach, 310 F.3d 1063 (8th Cir. 2002) (No. 02-1238), *available at* http://www.epic.org/privacy/bach/kerr_amicus.pdf (last visited August 17, 2004).

[11] *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743–44 (1979); United States v. Miller, 425 U.S. 435, 443 (1976); Couch v. United States, 409 U.S. 322, 335 (1973); Hoffa v. United States, 385 U.S. 293, 302 (1966). As the Court stated in *Miller*:

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

Miller, 425 U.S. at 443.

noncontent information disclosed to an ISP.[12] The theory of these cases is that by communicating with their ISPs, Internet users have revealed information to their ISPs and have relinquished their Fourth Amendment rights in that information.[13] It is too early to tell whether courts will adopt the same rationale for content information, such as e-mails. Some early precedents suggest that they will not, but others suggest that they will, at least in some circumstances.[14] Either way, it remains unclear today whether files held by ISPs on behalf of their users can retain a Fourth Amendment "reasonable expectation of privacy."

The Fourth Amendment rules governing grand jury subpoenas offer a second reason why the Fourth Amendment apparently offers weak privacy protection online. Because ISPs are third-party corporate entities, investigators do not ordinarily search the servers of ISPs directly. Investigators do not break down the ISP's door and start looking for the files themselves.[15] Instead, they obtain a court order compelling the network provider to disclose the information to the government. This is important under existing Fourth Amendment doctrine: the Fourth Amendment generally allows the government to issue a grand jury subpoena compelling the disclosure of information and property, even if it is protected by a Fourth Amendment "reasonable expectation of privacy."[16] When the government obtains a court order such as a subpoena that

[12] *See* Guest v. Leis, 255 F.3d 325, 335–36 (6th Cir. 2001) (finding no expectation of privacy in noncontent information disclosed to ISP); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (same); United States v. Hambrick, 55 F. Supp. 2d 504, 508–09 (W.D. Va. 1999) (same), *aff'd*, 225 F.3d 656 (4th Cir. 2000) (unpublished table decision).

[13] *See, e.g.*, *Leis*, 255 F.3d at 335–36. This approach matches the rationale applied by courts that have held that the Fourth Amendment does not protect account records belonging to customers of the phone company and Western Union. *See* United States v. Fregoso, 60 F.3d 1314, 1321 (8th Cir. 1995) (holding that telephone company customers do not retain a reasonable expectation of privacy in account information held by the telephone company); *In re* Grand Jury Proceedings, 827 F.2d 301, 302–03 (8th Cir. 1987) (holding that Western Union customers have no reasonable expectation of privacy in Western Union records concerning the customers' activities).

[14] *Compare* United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996) (rejecting the disclosure rationale and holding that a defendant maintains Fourth Amendment protection in remotely stored AOL e-mails), *with* United States v. Geter, No. NMCM 9901433, 2003 WL 21254249, at *5 (N-M. Ct. Crim. App. May 30, 2003) (appearing to accept the rationale and rejecting a claim to Fourth Amendment protection in remotely stored e-mails on a government network). *See also Bach*, 310 F.3d at 168 ("While it is clear to this court that Congress intended to create a statutory expectation of privacy in e-mail files, it is less clear that an analogous expectation of privacy derives from the Constitution.").

[15] In the one case where they did try this, they were successfully sued. *See* Steve Jackson Games, Inc. v. U.S. Secret Serv., 816 F. Supp. 432, 443 (W.D. Tex. 1993), *aff'd*, 36 F.3d 457 (5th Cir. 1994).

[16] *See In re* Subpoena Duces Tecum, 228 F.3d 341, 346–49 (4th Cir. 2000).

requires the recipient of the order to turn over evidence to the government within a specified period of time, the order will generally comply with the Fourth Amendment if it seeks relevant information and is not overbroad.[17] Such circumstances do not require probable cause. This analysis also apparently applies when a suspect stores materials remotely with a third party, and the government serves the third party with the subpoena.[18] Although the cases are sparse and hardly models of clarity, they suggest that so long as the third party is in possession of the target's materials, the government may subpoena the materials from the third party without first obtaining a warrant based on probable cause.[19]

The third reason that the Fourth Amendment generally offers weak privacy protections online is that most ISPs are private actors. Most are commercial service providers, not government entities.[20] Under the private search doctrine, the Fourth Amendment "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."[21] As a result, even if the Fourth Amendment protects files stored with an ISP, the ISP can search through all of the stored files on its server and disclose them to the government

[17] *See* United States v. Dionisio, 410 U.S. 1, 8–12 (1973); *In re* Horowitz, 482 F.2d 72, 75–80 (2d Cir. 1973) (Friendly, J.).

[18] *See, e.g.*, United States v. Schwimmer, 232 F.2d 855 (8th Cir. 1956). In *Schwimmer*, the government served a subpoena on a third-party storage facility in possession of the defendant's papers. *See id.* at 859. Harry Schwimmer was a Kansas City lawyer suspected of involvement in a tax evasion and public corruption scheme in his role as an attorney. *See id.* at 858. By the time the grand jury investigating the case focused on Schwimmer, he had closed his office, boxed up his files, and placed them in storage before going to Puerto Rico. *See id.* at 858–59. The grand jury served two subpoenas on the storage company, ordering it to disclose books, records, and files of Harry Schwimmer either on its premises or under its control. *See id.* at 859. Schwimmer learned of the subpoenas and returned to Missouri to challenge them on the ground that they violated his Fourth Amendment rights. *See id.* The court held that Schwimmer had standing to challenge the subpoenas, *see id.* at 861; that the first subpoena was constitutionally unreasonable because it was merely part of "an abstract hunt for possible crime in Schwimmer's legal practice," *id.* at 862; and that the second, more narrow subpoena complied with the Fourth Amendment, *see id.* at 863. Although the court formally expressed the reasonableness inquiry in remarkably cryptic language, *see id.* at 861, in practice it seems to have applied the usual subpoena reasonableness standard, rather than a search warrant standard. *Cf.* Newfield v. Ryan, 91 F.2d 700, 702–03 (5th Cir. 1937) (permitting subpoena served on telegraph company for copies of defendants' telegrams in the telegraph company's possession); United States v. Barr, 605 F. Supp. 114, 116–19 (S.D.N.Y. 1985) (applying subpoena reasonableness standard to subpoena served on private third-party mail service for the defendant's undelivered mail in the third party's possession).

[19] I discuss this issue in greater depth in my amicus brief in *United States v. Bach*. *See* Brief of Amicus Curiae Professor Orin S. Kerr, *supra* note 10, at 15–24.

[20] *See, e.g.*, Cyber Promotions, Inc. v. Am. Online, Inc., 948 F. Supp. 456, 458 (E.D. Pa. 1996).

[21] United States v. Jacobsen, 466 U.S. 109, 113 (1984) (quotation omitted).

without violating the Fourth Amendment.[22]

Taken together, these three reasons make it difficult for robust Fourth Amendment protections to apply online. Because private files are held remotely by private ISPs, current doctrine does not protect remotely stored noncontent files and leaves the protection of stored content files unclear. And even if those files are protected, they likely can be subpoenaed by the government without probable cause. And even if the files cannot be subpoenaed, private ISPs can search through the files and disclose the fruits to law enforcement under the Fourth Amendment's private search doctrine. As I have written elsewhere, these details of how the Internet works make it almost "custom designed" to frustrate claims of strong Fourth Amendment protection in remotely stored files under current Fourth Amendment doctrine.[23]

The SCA addresses this imbalance by offering network account holders a range of statutory privacy rights against access to stored account information held by network service providers. The statute creates a set of Fourth Amendment–like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information. It does this in two ways. First, the statute creates limits on the government's ability to compel providers to disclose information in their possession about their customers and subscribers.[24] Although the Fourth Amendment may require no more than a subpoena to obtain e-mails, the statute confers greater privacy protection.[25] Second, the statute places limits on the ability of ISPs to voluntarily disclose information about their customers and subscribers to the government.[26] Although the private search doctrine of the Fourth Amendment allows private providers to make such disclosures, the SCA imposes limitations on the circumstances in which such a disclosure can occur.[27]

II. Entities Regulated by the Stored Communications Act

The focal point of the SCA is the set of network service providers regulated by the statute. The statute creates rights held by "customers" and "subscribers" of network service providers in both content and noncontent

[22] *See* United States v. Steiger, 318 F.3d 1039, 1046 (11th Cir. 2003) (concluding that searches of defendant's computer over the Internet by an anonymous computer hacker did not violate the Fourth Amendment because there was no evidence that the government was involved in the search); United States v. Hall, 142 F.3d 988, 993 (7th Cir. 1998); United States v. Kennedy, 81 F. Supp. 2d 1103, 1112 (D. Kan. 2000).

[23] Kerr, *supra* note 3, at 812–13.

[24] *See* 18 U.S.C. § 2703 (2000 & Supp. I 2003).

[25] *See id.*

[26] *See id.* § 2702.

[27] *See id.*

information held by two particular types of providers. To know whether and how the SCA protects the privacy of a particular communication, you must start by classifying the provider to see whether it falls within the scope of the providers regulated by the statute—and if it does, which category of provider applies. If the provider fits within the two categories, the SCA protects the communication; otherwise, only Fourth Amendment protections apply. At this point, though, a warning to the reader may be in order: the distinction that the SCA draws reflects the technology of the 1980s and seems a bit cryptic at first.[28] Still, the framework makes sense once understood as a whole.

The SCA provides privacy protection to communications held by two types of providers.[29] As the 1986 Senate Report on the SCA explains, computer network account holders at that time generally used third-party network service providers in two ways.[30] First, account holders used their accounts to send and receive communications such as e-mail.[31] The use of computer networks to communicate prompted privacy concerns because in the course of sending and retrieving messages, it was common for computers to copy the messages and store them temporarily pending delivery.[32] The copies that these providers of "electronic communication service" created and placed in temporary "electronic storage" in the course of transmission sometimes stayed on a provider's computer for several months.[33]

The second reason account holders used network service providers was to outsource computing tasks.[34] For example, users paid to have remote computers store extra files or process large amounts of data.[35] (This was in the era before spreadsheet programs, so users generally needed to outsource tasks to perform what by today's standards are simple number-crunching jobs.) When users hired such commercial "remote computing services" to perform tasks for them, they would send a copy of their private information to a third-party computing service, which retained the data for storage or

[28] Further, it is a framework that some courts have misunderstood thanks to the unusual way in which many SCA cases are litigated. *See infra* Part VI.C.

[29] Parts of this discussion derive from a discussion of the SCA that I authored in 2001 as part of a Justice Department manual. *See* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (2002), *available at* http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm [hereinafter DOJ MANUAL].

[30] *See* S. REP. NO. 99-541, at 2–3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3556–57.

[31] *See id.*

[32] *See* H.R. REP. NO. 99-647, at 22 (1986).

[33] *See* S. REP. NO. 99-541, at 3, *reprinted in* 1986 U.S.C.C.A.N. at 3557.

[34] *See id.*

[35] *See id.*

processing.[36] Remote computing services raised privacy concerns because the service providers often retained these copies of their customers' files for long periods of time.[37]

The SCA adopts these two distinctions, freezing into the law the understandings of computer network use as of 1986. The text regulates two types of providers: providers of electronic communication service ("ECS") and providers of remote computing service ("RCS"). The statute defines ECS as "any service which provides to users thereof the ability to send or receive wire or electronic communications,"[38] and it defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof,"[39] plus any backup copies of files in such temporary storage.[40] RCS is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system."[41] An "electronic communications system" is in turn defined as "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications."[42]

The narrow scope of the SCA has two important implications. First, there are many problems of Internet privacy that the SCA does not address. The SCA is not a catch-all statute designed to protect the privacy of stored Internet communications; instead it is narrowly tailored to provide a set of Fourth Amendment–like protections for computer networks. Unfortunately, some judges have had a difficult time realizing this, and have twisted the statute to do things that it was never intended to do.[43] For example, several district courts have applied the SCA to regulate the placement of electronic cookies on home computers.[44] To do this, they have needed to hold that a home computer used to surf the web is a provider of ECS that falls within the SCA.[45] This is quite plainly incorrect.

[36] *See id.*

[37] *See id.*

[38] 18 U.S.C. § 2510(15) (2000 & Supp. I 2003). For example, "telephone companies and electronic mail companies" generally act as providers of electronic communication services. *See* S. REP. NO. 99-541, at 14, *reprinted in* 1986 U.S.C.C.A.N. at 3568.

[39] 18 U.S.C. § 2510(17)(A).

[40] *Id.* § 2510(17)(B).

[41] *Id.* § 2711(2).

[42] *Id.* § 2510(14).

[43] *See* Kerr, *supra* note 3, at 829–36.

[44] *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001); *In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272 (C.D. Cal. 2001); Chance v. Avenue A, Inc., 165 F. Supp. 2d 1154 (W.D. Wash. 2001).

[45] *See In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d at 507; *In re Intuit Privacy Litig.*, 138 F. Supp. 2d at 1275–76; *Chance*, 165 F. Supp. 2d at 1161.

While a home computer configured as a mail server could provide ECS in theory,[46] the home computer of an end user is not protected by the SCA.[47] This is consistent with the SCA's purpose: home computers are already protected by the Fourth Amendment, so statutory protections are not needed.

The second implication of the two distinctions adopted by the SCA is that we need to distinguish between providers of ECS, providers of RCS, and providers that provide neither ECS nor RCS. These distinctions are important because, as we will see shortly, the scope of privacy protections hinges on such distinctions. The distinction between providers of ECS and RCS is made somewhat confusing by the fact that most network service providers are multifunctional. They can act as providers of ECS in some contexts, providers of RCS in other contexts, and as neither in some contexts as well. In light of this, it is essential to recognize the functional nature of the definitions of ECS and RCS. The classifications of ECS and RCS are context sensitive: the key is the provider's role with respect to a particular copy of a particular communication, rather than the provider's status in the abstract.[48] A provider can act as an RCS with respect to some

[46] I say "in theory" because the home user would need to set up a server with its own third-party users, which most home users do not do. The key is the third-party relationship: because the SCA only protects information held by third-party providers, some kind of third-party relationship is needed for the SCA to apply. *See In re* Pharmatrak, Inc. Privacy Litig., 220 F. Supp. 2d 4, 13 (D. Mass. 2002), *rev'd*, 329 F.3d 9 (1st Cir.), *later proceeding at* 292 F. Supp. 2d 263 (D. Mass 2003).

[47] This is clear from the definition of "electronic communication service" in 18 U.S.C. § 2510(15): it means a "service which provides to users thereof the ability to send or receive wire or communications." 18 U.S.C. § 2510(15). Thus the statute envisions a provider (the ISP or other network service provider) and a user (the individual with an account with the provider), with the user's communications in the possession of the provider.

[48] The text of the statute makes this clear by limiting the scope of ECS protections to contents or backups of contents in temporary "electronic storage," see 18 U.S.C. §§ 2702(a)(1), 2703(a), and limiting the scope of RCS protections to files "held or maintained . . . solely for the purpose of providing storage or computer processing services," *id.* § 2703(b)(2). The only sensible explanation for these limitations is that the SCA allows both protected categories to apply to the same provider, covering different communications held by a provider at a given time in different ways. Files in temporary "electronic storage" are held by the provider acting as an ECS, and contents "held or maintained . . . solely for the purpose of providing storage or computer processing services" are held by the provider acting as an RCS. Any other reading would create enormous holes in the statute that its drafters presumably did not intend. Focusing on the provider's status in the abstract would create major gaps in the statute by offering no protection to files held by providers beyond the narrow category protected. For example, consider the privacy protections that apply to contents of communications held by providers of ECS. Those rules apply only to communications held in temporary "electronic storage" pending delivery to the content's destination. *See id.* § 2703(a). If you categorize providers in the abstract, however, pretty much every ISP fits within the definition of a provider of ECS. *See id.* § 2510(15) (defining ECS as "*any service* which provides to users thereof the ability to send or receive wire or electronic communications" (emphasis added)). Under the traditional understanding of "electronic storage," very few communications held by an ISP are held in temporary

communications, an ECS with respect to other communications, and neither an RCS nor an ECS with respect to other communications. In the case of a public provider, for example, files held in intermediate "electronic storage" are protected under the ECS rules;[49] meanwhile, files held for long-term storage by that same provider are protected by the RCS rules.[50] The same treatment exists for different copies of the same communication: a provider can act as an ECS with respect to one copy of a communication, as an RCS with respect to another copy, and as neither an ECS nor an RCS with respect to a third copy.

What does this mean in practice? Some cases are easy. For example, when an e-mail sits unopened on an ISP's server, the ISP is acting as a provider of ECS with respect to that e-mail.[51] On the other hand, if I author a document and send it via ftp to a commercial long-term storage site for safekeeping, the storage site is acting as a provider of RCS with respect to that file. There are closer cases, however, and some of these closer cases are important ones. In particular, the proper treatment of opened e-mail is currently unclear. The traditional understanding has been that a copy of opened e-mail sitting on a server is protected by the RCS rules, not the ECS rules.[52] The thinking is that when an e-mail customer leaves a copy of an already-accessed e-mail stored on a server, that copy is no longer "incident to transmission" nor a backup copy of a file that is incident to transmission: rather, it is just in remote storage like any other file held by an RCS.[53]

An example can help explain how the rules fit together under this traditional understanding. Imagine that I send an e-mail to my friend Jane who has an account at a commercial ISP. When the message first arrives at the ISP, the ISP acts a provider of ECS with respect to the e-mail. The e-mail is in "electronic storage" awaiting Jane's retrieval of the message.[54] Once Jane retrieves my e-mail, she can either delete the message from the ISP's server or leave the message stored on the ISP's server for safekeeping. If Jane chooses to store the e-mail with the ISP, the ISP now acts as a provider of RCS (and not ECS) with respect to that copy of the e-

"electronic storage." Focusing on status in the abstract would mean that most communications held by ISPs are unprotected by the SCA, which is surely a result not intended by the statute's drafters.

[49] *See id.* §§ 2702(a)(1), 2703(a).

[50] *See id.* §§ 2702(a)(2), 2703(b).

[51] *See* Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 461–63 (5th Cir. 1994).

[52] *See* DOJ MANUAL, *supra* note 29, § III.B (2002).

[53] *See* Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 635–38 (E.D. Pa. 2001) (concluding that e-mails taken from post-transmission storage are not in "electronic storage"), *aff'd on other grounds*, 352 F.3d 107 (3rd Cir. 2003); H.R. REP. NO. 99-647, at 64–65 (1986) (noting that opened e-mail stored on a server are protected under provisions relating to remote computing services).

[54] *See Steve Jackson Games*, 36 F.3d at 461.

mail so long as the ISP is available to the public. The role of the ISP has changed from a transmitter of the e-mail to a storage facility available to the public, from an ECS to an RCS.[55] If the ISP is not available to the public, which as I explain later would cover most government and university e-mail accounts,[56] then the ISP provides neither ECS nor RCS, and the remotely stored e-mail now is protected only under the Fourth Amendment. If Jane downloads a copy of the e-mail onto her personal computer, the ISP acts as neither a provider of ECS nor RCS with respect to the downloaded copy regardless of whether the ISP is available to the public. The ISP is not holding the downloaded copy either incident to transmission or for storage; in fact, the ISP does not hold that copy at all. As a result, only Fourth Amendment privacy protections apply.

Although this is the traditional understanding of how the ECS/RCS distinction applies to e-mail, a recent decision by the Ninth Circuit has taken a very different approach. In *Theofel v. Farey-Jones*, the Ninth Circuit concluded that all e-mails held by a server are protected under the ECS rules until "the underlying message has expired in the normal course,"[58] regardless of whether the e-mail has been accessed.[59] As best I can tell, this is a fact-sensitive test: under *Theofel*, a server acts as a provider of ECS with respect to a message until both the user and the ISP no longer need the e-mail message.[60] The Ninth Circuit concluded that whether an e-mail has been accessed is irrelevant, as an already-accessed e-mail can be a backup copy included within the statutory definition of "electronic storage."[61] For reasons that I will relegate to a very long footnote, the Ninth Circuit's analysis in *Theofel* is quite implausible and hard to square with the statutory text.[62] For my purposes here, however,

[55] *See Fraser*, 135 F. Supp. 2d at 635–38; H.R. REP. NO. 99-647, at 64–65.

[56] *See infra* notes 126–29 and accompanying text.

[58] Theofel v. Farey-Jones, 359 F.3d 1066, 1076 (9th Cir. 2004).

[59] *See id.* at 1077 ("[W]e think that prior access is irrelevant to whether the messages at issue are in electronic storage.").

[60] *See id.* at 1076. ("[T]he mere fact that a copy *could* serve as a backup does not mean that it is stored for that purpose. We see many instances where an ISP could hold messages not in electronic storage—for example, e-mail sent to or from the ISP's staff, or messages a user has flagged for deletion from the server.").

[61] 18 U.S.C. § 2510(17)(B) (2000 & Supp. I 2003). *See Theofel*, 359 F.3d at 1077.

[62] An understanding of the structure of the SCA indicates that the backup provision of the definition of electronic storage, *see id.* § 2510(17)(B), exists only to ensure that the government cannot make an end-run around the privacy-protecting ECS rules by attempting to access backup copies of unopened e-mails made by the ISP for its administrative purposes. ISPs regularly generate backup copies of their servers in the event of a server crash or other problem, and they often store these copies for the long term. Section 2510(17)(B) provides that backup copies of unopened e-mails are protected by the ECS rules even though they are not themselves incident to transmission; without this provision, copies of unopened e-mails generated by this universal ISP practice would be unprotected by the SCA.

the key is to understand that the Ninth Circuit's approach differs significantly from the traditional understanding, and it is now governing law in a circuit that includes major ISPs such as Yahoo! and Hotmail. Under *Theofel*, what matters is not whether a file has been accessed, but rather whether the e-mail "has expired in the normal course."[63] Although it is unclear what "normal course" the Ninth Circuit has in mind, the apparent test is whether the user or employees of the service provider have reason to believe that they may need to access an additional copy of the file in the

There are many statutory signals that support this reading. Several were raised by the United States as amicus and rejected by the *Theofel* court, *see Theofel*, 359 F.3d at 1076–77, but a host of other arguments remain. I think the most obvious statutory signal is the text of 18 U.S.C. § 2704, entitled "Backup Preservation." *See* 18 U.S.C. § 2704 (2000). Section 2704 makes clear that the SCA uses the phrase "backup copy" in a very technical way to mean a copy made by the service provider for administrative purposes. *See id.* The statutory focus on backup copies in the SCA was likely inspired by the 1985 Office of Technology Assessment report that had helped inspire the passage of the SCA. *See* OFFICE OF TECH. ASSESSMENT, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES (1985). The report highlighted the special privacy threats raised by backup copies, which the report referred to as copies "[r]etained by the [e]lectronic [m]ail [c]ompany for [a]dministrative [p]urposes." *Id.* at 50. The Ninth Circuit's view that a backup copy is only a temporary copy made by a service provider or a user is hard to square with this understanding.

Theofel also sets up a distinction that conflicts with 18 U.S.C. § 2703(a) and is unworkable in practice. *Theofel* suggests that each e-mail has a definable "lifespan," during which a service provider or user may need a copy of the e-mail. *See Theofel*, 359 F.3d at 1076. During that time, the copy is in "electronic storage" and the ECS rules apply. *See id.* Eventually the e-mail will "expire[] in the normal course," *id.*, at which time the e-mail is no longer in electronic storage and the ECS protections no longer apply. The difficulty is that § 2703(a) already defines such a lifespan elsewhere in explicit statutory terms; the statute provides one set of rules for contents in electronic storage held "for one hundred and eighty days or less" and provides another set of rules for contents in electronic storage held for longer than 180 days. *See* 18 U.S.C. § 2703(a) (2000 & Supp. I 2003). Section 2703(a) plainly contemplates that e-mails can be in "electronic storage" for a long, long time, a premise that the *Theofel* court rejects. *See Theofel*, 359 F.3d at 1076. Further, given that the statute draws an explicit lifespan line in § 2703(a), envisioning a competing distinction in § 2510(17) makes little sense. The apparently subjective nature of the line makes it all the less likely from the standpoint of statutory interpretation: investigators must be able to classify a file before they know what legal process they must obtain to compel it, and normally they cannot tell when a user or service provider no longer needs the file or is storing it for backup purposes.

Finally, the oddity of the Ninth Circuit's approach is also clear from the Ninth Circuit's view that an e-mail can be protected both under the ECS rules and the RCS rules at the same time. *See Theofel*, 359 F.3d at 1076–77. The problem is that the ECS rules and RCS rules can be mutually exclusive. For example, § 2703(a) states that a government entity needs a warrant to compel a service provider acting as an ECS to disclose contents so long as the contents have been in storage for 180 days or less; § 2703(b)(1)(B)(i) states that the government entity can compel a service provider acting as an RCS to disclose contents with only prior notice and a subpoena. *Compare* 18 U.S.C. § 2703(a), *with* 18 U.S.C. § 2703(b)(1)(B)(i). If an e-mail message is covered by both the ECS and RCS rules at the same time, legal process that is permitted under the RCS rules would violate the ECS rules.

[63] *Thoefel*, 359 F.3d at 1076.

future.[64]

III. The Privacy Protections of the Stored Communications Act

The privacy protections contained in 18 U.S.C. §§ 2702 and 2703 provide the heart of the SCA. Section 2703 provides the rules that the government must follow when it seeks to compel a provider to disclose information.[65] Section 2702 provides the rules that govern whether a provider can disclose information to the government voluntarily.[66]

A. Compelled Disclosure Rules in 18 U.S.C. § 2703

Section 2703 mandates different standards the government must satisfy to compel different types of communications. To compel a provider of ECS to disclose contents of communications in its possession that are in temporary "electronic storage" for 180 days or less, the government must obtain a search warrant.[67] To compel a provider of ECS to disclose contents in electronic storage for greater than 180 days or to compel a provider of RCS to disclose contents, the government has three options.[68] First, the government can obtain a search warrant.[69] Alternatively, investigators can use less process than a warrant, as long as they combine that process with prior notice.[70] Specifically, the government can use either a subpoena[71] or a "specific and articulable facts" court order pursuant to 18 U.S.C. § 2703(d),[72] combined with prior notice to the "subscriber or customer" (which can be delayed in some circumstances).[73] The court order found in § 2703(d), often referred to as a "2703(d)" order or simply a "d" order, is something like a mix between a subpoena and a search warrant. To obtain the order, the government must provide "specific and articulable facts showing that there are reasonable grounds to believe" that the information to be compelled is "relevant and material to an ongoing criminal investigation."[74] If the judge finds that the factual showing has been made, the judge signs the order. The order is then served like an ordinary subpoena; investigators bring or fax the order to the ISP, and the ISP complies by turning over the information to the investigators.

[64] *See id.* at 1075 (suggesting that contents are in electronic storage if the user or the ISP may "need[] to download" the file from the ISP's server).

[65] *See* 18 U.S.C. § 2703.

[66] *See id.* § 2702.

[67] *See id.* § 2703(a).

[68] *See id.* § 2703(a)–(b).

[69] *See id.* § 2703(b)(1)(A).

[70] *See id.* § 2703(b)(1)(B).

[71] *See id.* § 2703(b)(1)(B)(i).

[72] *See id.* § 2703(b)(1)(B)(ii).

[73] *See id.* § 2705.

[74] *Id.* § 2703(d).

The rules governing compelled disclosure also cover noncontent records, such as logs maintained by a network server. The rules are the same for providers of ECS and RCS and give the government several ways to compel noncontent records. First, the government can obtain a 2703(d) order to compel such records.[75] Alternatively, the government can obtain a search warrant instead.[76] Investigators can also compel the disclosure of noncontent records if they obtain the consent of the customer or subscriber to such disclosure,[77] and in the rare case that involves telemarketing fraud, they can obtain noncontent records merely by submitting a formal written request to the provider.[78] Finally, the SCA has special rules for compelling a subset of noncontent records that Congress has deemed less private than other records.[79] These records are sometimes known as "basic subscriber information" because they mostly involve information about the subscriber's identity. The government can obtain the following basic subscriber information with a mere subpoena:

> (1) name;
>
> (2) address;
>
> (3) local and long distance telephone connection records, or records of session times and durations;
>
> (4) length of service (including start date) and types of service utilized;
>
> (5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
>
> (6) means and source of payment for such service (including any credit card or bank account number).[80]

One interesting aspect of § 2703 is that it generally allows the government to obtain greater process when lesser process will do. If a provision of § 2703 allows government agents to compel information with a subpoena, it also allows them to obtain that information with a 2703(d) order; if it allows agents to obtain information with a 2703(d) order, then a

[75] *See id.* § 2703(c)(1)(B).

[76] *See id.* § 2703(c)(1)(A).

[77] *See id.* § 2703(c)(1)(C). It is notably unclear how this provision might be legally enforced given that a subscriber's consent is not a court order that a provider must obey. For example, imagine that government investigators obtain a subscriber's consent but have only the subscriber's oral consent, not her written consent. The provider insists on written consent, or else a court order, and refuses to disclose the records to the investigators otherwise. Has the provider violated the statute at that point? Procedurally speaking, how might a court determine this?

[78] *See id.* § 2703(c)(1)(D).

[79] *See id.* § 2703(c)(2).

[80] *Id.*

search warrant is also acceptable. Why might the government want this option? The main reason is efficiency.[81] Investigators may decide that they need to compel several types of information, some of which can be obtained with lesser process and some of which requires greater process. The "greater includes the lesser" rule in § 2703 allows the government to obtain only one court order—whatever process is greatest—and compel all of the information in one order all at once.

B. Voluntary Disclosure Rules in 18 U.S.C. § 2702

The rules regulating voluntary disclosure by providers of RCS and ECS appear in 18 U.S.C. § 2702. Importantly, § 2702 imposes restrictions only on providers of ECS and RCS that provide services "to the public."[82] Nonpublic providers can voluntarily disclose information freely without violating the SCA.[83] Among providers to the public, providers are also free to disclose noncontent information to nongovernment entities.[84] For example, a company can disclose records about how its customers used its services to a marketing company. In contrast, § 2702(a) generally bans disclosure of contents by public providers, as well as the disclosure of noncontent records to any government entities.[85] The statute then provides specific exceptions in which voluntary disclosure is allowed.[86]

For mostly historical reasons that are of little importance today, § 2702 has slightly different exceptions depending on whether the information to be voluntarily disclosed consists of content or noncontent information.[87] In the case of disclosure of contents, a provider can disclose information voluntarily in the following circumstances:

> (1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;
>
> (2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of

[81] Another reason is that greater process may insulate the transaction from Fourth Amendment challenge. For example, the constitutionality of 18 U.S.C. § 2703(b) is unclear; it is possible that a court might conclude that a search warrant is necessary to compel such contents, even if the statute requires less process. If a prosecutor has probable cause and can obtain a search warrant, she may choose to obtain the warrant to compel RCS contents just to make sure that the evidence will not be suppressed as a violation of the Fourth Amendment.

[82] *See* 18 U.S.C. § 2702(a).

[83] This is clear by the fact that the prohibitions in § 2702(a) apply only to providers "to the public." *Id.* By implication, nonpublic providers can disclose without limitation under the SCA. *See* Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1042–43 (N.D. Ill. 1998).

[84] *See* 18 U.S.C. § 2702(c)(6).

[85] *See id.* § 2702(a).

[86] *See id.* § 2702(b), (c).

[87] Voluntary disclosure of contents is covered by § 2702(b). Voluntary disclosure of noncontent records is covered by § 2702(c).

> this title;
>
> (3) 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;
>
> (4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;
>
> (5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;
>
> (6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032);
>
> (7) to a law enforcement agency (A) if the contents—(i) were inadvertently obtained by the service provider; and
>
> (ii) appear to pertain to the commission of a crime; or
>
> (8) to a Federal, State, or local governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.[88]

Of these eight exceptions, numbers one through four are common sense exceptions: a provider can divulge contents if it needs to do so in order to deliver the communication (exceptions one and four), if otherwise required by law (exception two), or if the person whose rights are at stake consents (exception three).[89] The remaining exceptions deal with specific circumstances in which an individual's privacy rights give way to other competing interests. A provider can disclose contents when disclosure is necessary given a dangerous emergency (exception eight);[90] when the provider inadvertently discovers the evidence and it relates to a crime (exception seven);[91] when such disclosure is needed to protect the provider, such as from unauthorized use of the network (exception five);[92] and when

[88] 18 U.S.C. § 2702(b).

[89] *See id.* § 2702(b)(1)–(4).

[90] *See id.* § 2702(b)(8).

[91] *See id.* § 2702(b)(7).

[92] *See id.* § 2702(b)(5). This language is copied from the so-called provider exception of the Wiretap Act, *see id.* § 2511(2)(a)(i), the meaning of which is well known. The provider exception gives a provider the right to conduct reasonable, tailored monitoring of the network to protect the provider's property from unauthorized use and for other legitimate provider reasons, as well as to disclose communications intercepted. *See generally* DOJ MANUAL, *supra* note 29, § IV.D.3.c. The inclusion of the same language in

a provider discovers images of child pornography that the provider must disclose to the police by federal law (exception six).[93]

The exceptions for the disclosure of noncontent records are similar, but not quite identical, to those for contents. A provider of ECS or RCS to the public can disclose noncontent records in the following circumstances:

> (1) as otherwise authorized in section 2703;
>
> (2) with the lawful consent of the customer or subscriber;
>
> (3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;
>
> (4) to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information;
>
> (5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032); or
>
> (6) to any person other than a governmental entity.[94]

For the most part, the differences between the rules for the disclosure of content and noncontent information are subtle ones with little practical importance. One exception is that noncontent records can be disclosed to nongovernment entities without restriction.[95]

IV. Putting the Pieces Together

Although the rules found in § 2702 and § 2703 can seem maddeningly complicated at first, they prove surprisingly straightforward in practice. The rules for compelled disclosure operate like an upside-down pyramid. Because the SCA's rules allow greater process to include the lesser, different levels of process can compel different groups of information. The higher up the pyramid you go, the more information the government can obtain.

At the lowest threshold, only a simple subpoena is needed to compell

the SCA presumably means that the same standards govern disclosure under the SCA.

[93] *See* 18 U.S.C. § 2702(b)(6); 42 U.S.C. § 13032 (2000) (requiring ECS and RCS providers to report to the National Center for Missing and Exploited Children any instance of child pornography of which it becomes aware).

[94] 18 U.S.C. § 2702(c).

[95] *See id.* § 2702(c)(6). Arguably, § 2702(c)(6) is redundant because the prohibitions on disclosure of noncontent information in § 2702(a)(3) expressly do not apply to disclosure to nongovernment entities. Because the prohibition does not restrict such disclosure, there is no need for an exception in § 2702(c)(6).

basic subscriber information.[96] Higher up the pyramid, a 2703(d) order compels all noncontent records.[97] A simple subpoena combined with prior notice compels three categories of information: basic subscriber information,[98] plus any opened e-mails or other permanently held files (covered by the RCS rules),[99] plus any contents in temporary "electronic storage" such as unretrieved e-mails in storage for more than 180 days.[100] A 2703(d) order plus prior notice is sufficient to compel all noncontent records,[101] plus any opened e-mails or other permanently held files (covered by the RCS rules),[102] plus any contents in temporary "electronic storage" such as unretrieved e-mails in storage for more than 180 days.[103] Put another way, a 2703(d) order plus prior notice compels everything except contents in temporary "electronic storage" 180 days or less. Finally, a search warrant is needed to compel everything stored in an account.[104]

The rules governing voluntary disclosure by providers are even simpler in practice. Nonpublic providers can disclose without restriction. Providers of ECS or RCS to the public ordinarily cannot disclose either content or noncontent information.[105] Disclosure is allowed only when an exception applies: in the case of contents, the facts must fit within one of the eight exceptions found in § 2702(b); in the case of noncontent records, the facts must fit within one of the six exceptions found in § 2702(c).

This chart summarizes the basic rules of the SCA:

[96] *See id.* § 2703(c)(2).

[97] *See id.* § 2703(c)(1)(B).

[98] *See id.* § 2703(c)(2).

[99] *See id.* § 2703(b).

[100] *See id.* § 2703(a).

[101] *See id.* § 2703(c)(2).

[102] *See id.* § 2703(b).

[103] *See id.* § 2703(a).

[104] *See id.* § 2703(a)–(c).

[105] *See id.* § 2702(a).

	Voluntary Disclosure Allowed?		**Mechanisms to Compel Disclosure**	
	Public Provider	Nonpublic Provider	Public Provider	Nonpublic Provider
Unopened e-mail (in electronic storage 180 days or less)	No, unless § 2702(b) exception applies [§ 2702(a)(1)]	Yes [§ 2702(a)(1)]	Search warrant [§ 2703(a)]	Search warrant [§ 2703(a)]
Unopened e-mail (in electronic storage more than 180 days)	No, unless § 2702(b) exception applies [§ 2702(a)(1)]	Yes [§ 2702(a)(1)]	Subpoena with notice; 2703(d) order with notice; or search warrant [§ 2703(a), (b)]	Subpoena with notice; 2703(d) order with notice; or search warrant [§ 2703(a), (b)]
Opened e-mail, other content files being stored or processed	No, unless § 2702(b) exception applies [§ 2702(a)(2)]	Yes [§ 2702(a)(2)]	Subpoena with notice; 2703(d) order with notice; or search warrant [§ 2703(b)]	SCA does not apply [§ 2711(2)]
Noncontent records	No, unless § 2702(c) exception applies [§ 2702(a)(3)]	Yes [§ 2702(a)(3)]	2703(d) order or search warrant [§ 2703(c)(1)]	2703(d) order or search warrant [§ 2703(c)(1)]
Basic subscriber information, session logs, IP addresses, (anything in § 2703(c)(2))	No, unless § 2702(c) exception applies [§ 2702(a)(3)]	Yes [§ 2702(a)(3)]	Subpoena; 2703(d) order; or search warrant [§ 2703(c)(2)]	Subpoena; 2703(d) order; or search warrant [§ 2703(c)(2)]

Notably, this chart assumes a traditional understanding of the scope of ECS and RCS, rather than the Ninth Circuit's approach from *Theofel*.[106] Under *Theofel*, the first three rows of this chart should have different labels on the far left column. In the place of "Unopened e-mail (in electronic storage 180 days or less)," the label would be something like, "Unexpired e-mails stored for 180 days or less." In the place of "Unopened e-mail (in electronic storage more than 180 days)," the new label would be "Unexpired e-mails stored for more than 180 days." Where the third row is now labeled "Opened e-mail, other content files being stored or processed," the new label would be "Files remotely stored or processed." It would also

[106] Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004).

be possible for a particular file to fit under two rows at the same time under *Theofel*: an e-mail could be in row one or two and row three at the same time.[107]

V. Dichotomies and Ambiguities in the Stored Communications Act

As the above chart illustrates, the legal categories found in the SCA derive from a series of dichotomies made by its drafters. The applicable rules in particular cases often hinge on subtle statutory distinctions such as the line between compelled and voluntary disclosure, between providers "to the public" and nonpublic providers, and between content versus noncontent records. This section will explore some of the key distinctions, both as a matter of doctrine and as a matter of policy. Notably, the absence of a statutory suppression remedy has resulted in few judicial decisions on these topics.[108] For most of the key issues, our guidance is the text, a few snippets of legislative history, and perhaps one or two judicial opinions.[109]

A. Voluntary Disclosure Versus Compelled Disclosure

One of the most fundamental distinctions in the SCA is the distinction between voluntary disclosure regulated by § 2702 and compelled disclosure regulated by § 2703. In the former, the provider wishes to disclose records to the government; in the latter, the government seeks information from the provider and uses the law to force the provider to disclose the information.

Although many interactions between the police and ISPs fall clearly into one of these categories, some fall into a gray zone somewhere between the two. Consider two examples. A police officer contacts an ISP system administrator and explains that he is investigating a child molestation case. The officer asks the system administrator if he is interested in helping out the police by voluntarily disclosing certain files. Wishing to be a good citizen, the system administrator agrees and turns over files to the agent. Is this a case of "compelled" disclosure or "voluntary" disclosure? Alternatively, imagine that a system administrator contacts the FBI and wants to disclose files but then asks for a subpoena just to make sure there was some sort of documentation of the disclosure. The FBI agent agrees, forwards a subpoena to the system administrator, and then accepts the files. Does the presence of the subpoena turn what was a voluntarily disclosure into a compelled disclosure?

The answers to such questions depend on what standard courts eventually adopt to distinguish between compelled and voluntary disclosure. Perhaps the compelled disclosure provisions should apply if and only if the government obtains a court order. Perhaps the voluntary

[107] *See id.* at 1076–77.

[108] *See* Kerr, *supra* note 3, at 823–25.

[109] *See id.*

disclosure rules apply whenever disclosure counts as "voluntary" according to the standard courts have used to determine voluntariness of consent in the Fourth Amendment context.[110] Or perhaps courts will look to the agency standard of Fourth Amendment law[111] and conclude that whenever an ISP employee acts as a Fourth Amendment agent the government must proceed under the compelled disclosure rules, and that in other cases, only the voluntary disclosure rules apply. Or perhaps courts will find some other standard helpful. At this point, we cannot be sure, and the precise line between voluntary and compelled disclosure rules remains hazy.

The only judicial guidance we have on this question is a recent district court decision, *Freedman v. America Online, Inc.*[112] In *Freedman*, two police officers investigating a threatening e-mail sent from an AOL account filled out a state warrant application and faxed it to AOL seeking the sender's basic subscriber information.[113] The officers did not actually submit the warrant application to a judge, however, rendering the warrant a legal nullity.[114] AOL complied with the terms of the warrant form and faxed the suspect's subscriber information back to the officers.[115] The suspect later sued AOL and the two police officers for violating § 2703.[116] The police officers argued that the case should be resolved under the voluntary disclosure provisions of § 2702, not the compelled disclosure provisions of § 2703.[117] They had merely requested the information, they contended, rather than actually requiring it as regulated by § 2703.[118] The court rejected this argument as "disingenuous."[119] The officers clearly intended AOL to comply with the request,[120] and allowing them to circumvent § 2703 by merely requesting information would "contradict[] Congress's intent to protect personal privacy."[121] The court rejected the argument that the emergency exception of § 2702(c)(4) applied: AOL's

[110] *See* Schneckloth v. Bustamonte, 412 U.S. 218, 226 (1973) (evaluating consent based on the individual's age, education, and intelligence; the physical and mental condition of the person giving consent; whether the person was under arrest; and whether the person had been advised of his right to refuse consent).

[111] *See, e.g.*, United States v. Lambert, 771 F.2d 83, 89 (6th Cir. 1985) (concluding that a private individual acts as an agent of the state for Fourth Amendment purposes if the police instigated, encouraged, or participated in the search and if the individual engaged in the search with the intent of assisting the police in their investigative efforts).

[112] Freedman v. Am. Online, Inc., 303 F. Supp. 2d 121 (D. Conn. 2004).

[113] *See id.* at 123. Note that under the SCA, only a subpoena was required. *See* 18 U.S.C. 2703(c)(2) (2000 & Supp. I 2003).

[114] *See Freedman*, 303 F. Supp. 2d at 123.

[115] *See id.*

[116] *See id.*

[117] *See id.* at 126–27.

[118] *See id.*

[119] *Id*. at 127.

[120] *See id.*

[121] *Id*. at 126.

disclosure was not on its own initiative, the court noted, but was triggered by the officers' request.[122] Although *Freedman* leaves many issues unanswered,[123] it suggests that disclosures will be presumed to fall under § 2703 unless an exception under § 2702 is affirmatively established.

B. Providers "To The Public" Versus Nonpublic Providers

The second critical distinction drawn by the SCA is the line between providers that make their services available "to the public" and those that do not. The distinction is important both for compelled and voluntary disclosure rules. In the case of voluntary disclosure rules, the distinction is critical; the SCA's voluntary disclosure limitations apply only to providers that make services available to the public.[124] As a result, the public/nonpublic line is generally the first inquiry when evaluating the legality of a voluntary disclosure. The distinction also carries importance in the compelled disclosure rules through the definition of RCS. Because an RCS by definition must provide services to the public,[125] opened e-mail held by a provider is protected by the RCS rules if it provides services to the public, but it is not protected by the SCA at all if it does not.

Fortunately, the legislative history of the SCA and a few cases on the question indicate a fairly clear line between the two categories. A provider "to the public" makes its ECS or RCS services available to the public at large, whether for a fee or without cost.[126] For example, a commercial ISP such as America Online or Comcast is available to the public: anyone can sign up and pay for an account. On the flip side, providers do not provide services to the public if its ECS or RCS services are available only to users with special relationships with the provider.[127] If a university provides accounts to its faculty and students or a company provides corporate accounts to its employees, those services are not available to the public.[128] In these contexts, the provider offers the user an account because the provider has a special relationship with the user.

Why does the SCA draw such an important distinction between public and nonpublic providers? The legislative history is not clear on this question, but two plausible explanations exist. First, the law may afford

[122] *See id.* at 128.

[123] *See, e.g.*, *id.* ("The Court declines to speculate whether it would ever be appropriate . . . for the government to notify the ISP of an emergency and receive subscriber information without conforming to the ECPA."). By "the ECPA," the court was presumably referring to § 2703.

[124] *See* 18 U.S.C. § 2702 (2000).

[125] *See* 18 U.S.C. § 2711(2) (2000 & Supp. I 2003).

[126] *See* Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1042–43 (N.D. Ill. 1998).

[127] *See id.* at 1043.

[128] *See id.*

less protection to accounts with nonpublic providers because nonpublic accounts may exist more for the benefit of providers than for the benefit of users. For example, companies often provide e-mail accounts to employees for work-related purposes; the U.S. military often provides accounts to service members for official government business. These nonpublic providers generally have a legitimate interest in controlling and accessing the accounts they provide to users. Plus, their users tend to recognize that the providers will view those provider interests as more important than the privacy interests of users.

In contrast, an individual who contracts with a commercial ISP available to the public usually does so solely for his own benefit. The account belongs to the user, not the provider. As a result, the user may understandably rely more heavily on the privacy of the commercial account from the public provider rather than another account with a nonpublic provider. Many Internet users have experienced this dynamic. When an e-mail exchange using a work account turns to private matters, it is common for a user to move the discussion to a commercial account. "I don't want my boss to read this," a user might note, "I'll e-mail you from my personal account later." The law recognizes this distinction by drawing a line between accounts held with public and nonpublic providers. In practice, the public/nonpublic line often acts as a proxy for the distinction between a user's private account and one assigned to him by his employer.[129]

A related explanation for this distinction is that private providers with a relationship to their users may approach their users' privacy differently than would commercial providers available to the public. To a commercial ISP, a particular customer is a source of revenue, no more and no less. In contrast, nonpublic providers may have a long-term, multifaceted relationship with their users, giving nonpublic providers unique incentives to protect the privacy of their users. The law may wish to protect privacy more heavily in the case of public providers because there is less incentive for public providers to protect their users' privacy. Alternatively, the law may take a more hands-off approach with respect to nonpublic providers in recognition of the different relationships that nonpublic providers may have with their users.

C. Content Information Versus Noncontent Information

The SCA also draws an important line between "contents" of communications and noncontent information—or as the statute labels it, "a record or other information pertaining to a subscriber to or customer of

[129] Network accounts at educational institutions present a potentially troubling exception. Educational institutions often provide Internet accounts to their students, and students often use those accounts as primary, private accounts. Such providers, however, do not provide services to the public.

such service (not including the contents of communications)."[130] Compelled disclosure of content information is regulated by § 2703(a) and § 2703(b),[131] while compelled disclosure of noncontent information is covered by § 2703(c).[132] Similarly, voluntary disclosure of contents is regulated by § 2702(b),[133] while voluntary disclosure of noncontent records is regulated by § 2702(c).[134] The question is, what counts as contents, and what counts as noncontent records?

The SCA itself points to the Wiretap Act for the answer.[135] The Wiretap Act contains a definition for "contents," although somewhat awkwardly the definition states what contents includes, not what it actually is.[136] According to the Wiretap Act:

> "[C]ontents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication.[137]

What does this cover? In the case of an e-mail, it clearly covers the body of the e-mail, that is, the actual text of the message. It is also fairly clear that the subject line of the e-mail counts as "contents," as the subject line generally carries a substantive message.[138] In contrast, logs of account usage, mail header information minus the subject line, lists of outgoing e-mail addresses sent from an account, and basic subscriber information all count as noncontent information.[139]

As I have explained elsewhere,[140] the distinction between content and noncontent information is basic to any communications network, and its functional role explains the different treatment that the two categories receive in the SCA. Content information is the communication that a person wishes to share or communicate with another person. In contrast, noncontent information (sometimes referred to as "envelope" information) is information about the communication that the network uses to deliver and process the content information.[141] Although the line between the two

[130] 18 U.S.C. § 2703(c)(1) (2000 & Supp. I 2003).

[131] *See id.* § 2703(a), (b).

[132] *See id.* § 2703(c).

[133] *See id.* § 2702(b).

[134] *See id.* § 2702(c).

[135] *See id.* § 2711(1) ("[T]he terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section . . . .").

[136] *See id.* § 2510(8).

[137] *Id.*

[138] *See* Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 646 (2003).

[139] *See id.* at 612–13.

[140] *See id*. at 611–16.

[141] *See id.*; *see also* Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949, 953 (1996) (exploring the

occasionally blurs,[142] in most cases the line is clear: it is the line between a message that a person wants to communicate and information about when and how he does so. The SCA gives greater privacy protection to content information for reasons that most people find intuitive: actual contents of messages naturally implicate greater privacy concerns than information (much of it network-generated) about those communications.[143]

distinction between communications and "communications attributes," described as "all the [noncontent] characteristics of a communication that can be learned" about a communication).

[142] The precise scope of "contents" remains a particularly difficult problem in the case of human-to-computer and computer-to-computer communications. *See* Kerr, *supra* note 138, at 645–47.

[143] In his contribution to this symposium, Professor Solove doubts the wisdom of offering lower privacy protection for noncontent information. *See* Daniel Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV ___ (2004). He suggests that the acquisition of noncontent information should require a full search warrant based on probable cause, on the theory that "[e]nvelope information can reveal a lot about a person's private activities, sometimes as much (and even more) than can content information." *Id.* at ___. Solove is correct that in particular circumstances and subject to particular assumptions, noncontent information can sometimes yield the equivalent of content information. Solove gives the example of URLs. *See id.* at ___. If someone visits a website, it may suggest that the user is interested in the topic of the site, which depending on the circumstances may be very private information. *See id.* at ___. I would add examples from the telephone and postal mail context. For example, if someone dials 1-800-MATTRES, you can be pretty sure they need a new mattress. (You leave off the last "S" for savings, or so the advertisements say.) Similarly, a college applicant who receives his admissions decision in the mail in a large stuffed envelope can be reasonably sure from the large envelope that he has been admitted to the college. In these cases, noncontent information can give us clues about content information, supporting inferences about highly private matters.

Despite this, Solove's suggestion that the law should offer increased privacy protection for noncontent information is unpersuasive. The main reason is that it is quite rare for noncontent information to yield the equivalent of content information. It happens in very particular circumstances, but it remains quite rare, and usually in circumstances that are difficult to predict *ex ante*. In the Internet context, for example, noncontent surveillance typically consists of collecting Internet packets; the packets disclose that a packet was sent from one IP address to another IP address at a particular time. This is not very private information, at least in most cases. Indeed, it is usually impossible to know who asked for the packet, or what the packet was about, or what the person who asked for the packet wanted to do, or even if it was a person (as opposed to the computer) who sent for the packet in the first place. Solove focuses on the compelling example of Internet search terms as an example of noncontent information that can be the privacy equivalent of content information. *See id.* This is a misleading example, however, as Internet search terms very well may be contents. *See* Kerr, *supra* note 138, at 644–48. Indeed, the one court to have addressed the question suggested that URL search terms are contents under the Wiretap Act. *See In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 18 (1st Cir. 2003). Despite the fact that noncontent information can yield private information, contents of communications implicate privacy concerns on a higher order of magnitude than noncontent information in the great majority of cases. As a result, it makes sense to give greater privacy protections for the former and lesser to the latter.

Solove's recommendation for a universal warrant requirement is also highly

D. ECS and RCS Today

The fourth issue is the scope of ECS and RCS. I touched on this earlier in the course of contrasting the traditional understanding of ECS with the Ninth Circuit's approach in *Theofel*.[144] There are also questions as to the proper scope of RCS protections. The definition of RCS leaves its scope today somewhat unclear. The SCA defines remote computing service as "the provision to the public of computer storage or processing services by means of an electronic communications system."[145] Computer storage is a relatively clear concept; even today, various businesses and products provide remote storage sites generally for a fee.[146] But how to interpret what counts as a "processing service"?

The invention of the World Wide Web is the primary source of the difficulty. Consider a website such as the popular online auction site eBay.[147] Does eBay provide RCS? Individuals can sign up for an eBay account and can then use that account either to bid on items for sale or to offer items for sale themselves. It is clear that eBay does not provide ECS: the site is a destination online, not a provider that gives users the ability to send and receive communications to the rest of the Internet.[148] But does eBay provide "processing services" for its customers, qualifying it as an RCS? I think the better answer is "no."[149] The legislative history indicates

impractical. *See* Solove, *supra*, at ___. Criminal procedure rules generally allow investigators to take preliminary steps with little or no legal process to enable them to build the case for more invasive steps that require a warrant. Solove would apparently require a warrant before the initial steps can be taken, on the theory that even the initial steps can involve grave privacy concerns. The Fourth Circuit explained the difficulties of such an extravagant approach in a recent decision concerning subpoenas. *See In re* Subpoena Duces Tecum, 228 F.3d 341, 348–49 (4th Cir. 2000). As the Fourth Circuit noted, requiring probable cause for initial investigative steps would result in an "unacceptable paradox": it would result in "the virtual end" to investigations "because the object of such investigations—to determine whether probable cause exists to prosecute a violation—would become a condition precedent for undertaking the investigation." *Id.* at 348. Professor Solove does not explain how his proposal would resolve this "unacceptable paradox" in the context of electronic surveillance.

[144] *See supra* Part II.

[145] 18 U.S.C. § 2711(2) (2000 & Supp. I 2003).

[146] *See, e.g.*, eWEEK.com, Storage News, Product Reviews, Trends and Analysis–eWEEK.com Storage Center, *at* http://storage.ziffdavis.com (last visited Apr. 14, 2004) (website devoted to products and information relating to remote storage software and services).

[147] eBay, http://www.ebay.com (last visited August 17, 2004).

[148] *See* Crowley v. Cybersource Corp., 166 F. Supp. 2d 1263, 1270 (N.D. Cal. 2001).

[149] This is apparently the conclusion that eBay's in-house lawyers have reached. eBay's privacy policy states:

> eBay cooperates with law enforcement inquiries, as well as other third parties to enforce laws, such as: intellectual property rights, fraud and other rights, to help protect you and the eBay community from bad actors. Therefore, in response to a verified request by law enforcement or other government officials relating to a

that "processing services" refer to outsourcing functions.[150] In the era before spreadsheets, a company might send raw data to a remote computing service and ask the service to crunch numbers to calculate its payroll.[151] This seems quite different from eBay: a user does not outsource tasks to eBay but rather uses eBay as a destination for the user's requests concerning buying and selling items.

At a literal level, however, it seems at least possible to conclude that eBay provides RCS. Every website processes information sent to it, and eBay is no exception. If I bid for an item listed on eBay, eBay's computers take in my bid and calculate whether it is the highest bid, taking my bid if it is the highest bid or rejecting it if there are higher ones. In this limited sense, eBay is performing a processing service. I think this is a fairly weak argument for the reasons noted above. But there are no decided cases on how to construe the phrase "processing services" in the SCA, so the answer at least today remains ambiguous.

E. Stored Communications Versus Communications in Transit

The fifth and final dichotomy is not drawn explicitly within the SCA, but rather appears implicitly when the SCA is compared to its companion statutes, the Wiretap Act and the Pen Register statute.[152] While the SCA protects the privacy of stored Internet communications, the Wiretap Act and the Pen Register statute protect the privacy of Internet communications in transit.[153] Specifically, the Wiretap Act protects contents of

> criminal investigation or alleged illegal activity, we can (and you authorize us to) disclose your name, city, state, telephone number, email address, UserID history, fraud complaints, and bidding and listing history without a subpoena. Without limiting the above, in an effort to respect your privacy and our ability to keep the community free from bad actors, we will not otherwise disclose your personal information to law enforcement or other government officials without a subpoena, court order or substantially similar legal procedure, except when we believe in good faith that the disclosure of information is necessary to: prevent imminent physical harm or financial loss; or report suspected illegal activity. Further, we can (and you authorize us to) disclose your name, street address, city, state, zip code, country, phone number, email, and company name to eBay VeRO Program participants under confidentiality agreement, as we in our sole discretion believe necessary or appropriate in connection with an investigation of fraud, intellectual property infringement, piracy, or other unlawful activity.

eBay, eBay Privacy Policy, *at* http://pages.ebay.com/help/policies/privacy-policy.html (last visited August 17, 2004). *See also Dyer v. Northwest Airlines Corps.*, No. A1-04-33, 2004 WL 2009397 (D.N.D. Sept. 8, 2004) (distinguishing businesses that "sell[] its products and services over the internet as opposed to access to the internet itself").

[150] *See* S. REP. NO. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557.

[151] *See id.*

[152] The Wiretap Act appears at 18 U.S.C. §§ 2510–2522 (2000), and the Pen Register statute appears at 18 U.S.C. §§ 3121–3127 (2000). *See generally* DOJ MANUAL, *supra* note 29, § IV.

[153] *See id.* § IV.A; Kerr, *supra* note 3, at 815–16 (2003).

communications in transit, and the Pen Register statute protects the privacy of noncontent information in transit.[154] This means that as a communication travels across the Internet, different laws apply to it at different times. For example, an e-mail message will be protected by the Wiretap Act when in transit, but by the SCA when it is stored. This dynamic raises two questions, one functional and the other doctrinal. The functional question is, why should different laws apply to stored communications and communications in transit? The doctrinal question is, when is a particular surveillance practice regulated under the SCA versus the Wiretap Act or the Pen Register statute?

The likely reason that stored communications are treated differently from communications in transit is that the means of obtaining the former are different from the means of obtaining the latter.[155] A stored communication rests on a network server in a permanent or semipermanent state. If the government wishes to obtain a copy of a stored communication, the government obtains an order compelling the system administrator of the server to locate the file and copy it. It is a one-time event. In contrast, communications in transit are generally obtained by installing a "sniffer" device, a surveillance tool that sits at a point on the network and scans and then filters passing Internet traffic.[156] The sniffer device is installed for a particular period of time, and the filter must be configured in a particular way based on the terms of the applicable court order. The dynamic is a real-time, ongoing process based on an effort to obtain future communications, rather than a one-time event designed to copy past communications in storage. The mechanisms are sufficiently different such that it has led to different legal regimes.[157]

The existence of two legal regimes creates the doctrinal question: how do we know when the SCA applies to a particular surveillance practice, versus when the Wiretap Act or the Pen Register statute applies?[158] The issue is important because computer technologies keep the line from being altogether clear: a digital communication that is primarily in transit may be stored by a computer for just a few milliseconds along the way and may be stored at intermediate points for longer periods.[159] Because the Wiretap Act requires the government to obtain a "super" search warrant rather than the usual warrant required by the SCA,[160] law enforcement agents have an

[154] *See* DOJ MANUAL, *supra* note 29, § IV.B.

[155] *See generally* Kerr, *supra* note 138, at 616–18 (explaining the difference between retrospective and prospective surveillance).

[156] *See id.* at 617.

[157] *See id*. at 616–18.

[158] *See id.* at 618 n.49.

[159] *See* Konop v. Hawaiian Airlines, 302 F.3d 868, 878 n.6 (9th Cir. 2002).

[160] *See* 18 U.S.C. § 2518 (2000) (explaining the steps the government must take to satisfy the legal requirements needed to obtain a wiretap order).

incentive to try to do prospective surveillance normally undertaken under the Wiretap Act using the retrospective authority of the SCA. But does the SCA allow this? If an agent wants to wiretap an e-mail account to obtain copies of every incoming message, does he need to obtain a wiretap order, or can he get a series of 2703(a) search warrants and serve one a day, or even one every hour?

The First Circuit's recent decision in *United States v. Councilman* suggests that legislative attention to this problem is needed.[161] In *Councilman*, a software program was designed and covertly installed at an ISP to intercept and copy all user e-mail from a competitor company.[162] A divided panel of the First Circuit held that the access to the e-mails was regulated by the SCA and not the Wiretap Act.[163] Although the e-mails were copied "as they were being transmitted and in real time,"[164] they were copied when in "storage" in the ISP's computer, even if only for a nanosecond.[165] If allowed to stay on the books, *Councilman* would gut Internet privacy. The decision would force the SCA to shoulder the weight regulating Internet wiretapping practices. The SCA is not designed to protect privacy against real-time wiretapping, however; as the titles of the two statutes might suggest, that is the domain of the Wiretap Act rather than the Stored Communications Act.

As of the date that this Article is going to press, the First Circuit has voted to rehear *Councilman* en banc and has withdrawn the panel opinion. It seems likely that either the First Circuit will reverse course or else that Congress will amend the statute. The question is, what kind of rule is needed? When stored communications are accessed in a way that makes the access the functional equivalent of a wiretap, the surveillance should be regulated by the Wiretap Act, not the SCA. For example, if an agent lines up a string of 2703(a) orders and serves one order per hour, I think that is the functional equivalent of a wiretap. It is reasonable to infer that the purpose of the surveillance is to obtain copies of all incoming messages, not to look for communications stored in a target's inbox. Similarly, it is the functional equivalent of a wiretap if an agent installs software that copies incoming messages a few milliseconds after they arrive. An interpretation of or amendment to § 2510(4) incorporating these insights would achieve three important goals. First, it would track the general distinction between prospective and retrospective surveillance that motivated Congress to regulate stored and in-transit communications in different ways. Second, it would discourage agents from trying to use the

[161] *See* United States v. Councilman, 373 F.3d 197 (1st Cir. 2004).

[162] *Id.* at 199.

[163] *See id.* at 200–04.

[164] *Id.* at 203.

[165] *See id.*

SCA as an end run around the Wiretap Act. Third, it would ensure that the line between the SCA and the Wiretap Act and Pen Register statute is functional and sensible rather than incoherent and arbitrary.

VI. A Legislator's Guide to Amending the Stored Communications Act

So much for the SCA of the present. How about the future? In this section, I discuss four potential areas of reform for the SCA. All four areas involve topics that Congress has overlooked in the past, resulting in a statute that is vague in some places, overly complex in others, and underprotective of privacy interests in others. My reforms fall into four categories: first, bolstering privacy protections for compelled content information; second, simplifying the statute; third, repealing provisions that have caused more harm than good; and fourth, restructuring the remedies scheme for violations of the SCA.

For the sake of simplicity, these recommendations look beyond the interesting and difficult questions raised by the two recent decisions in *Theofel* and *Councilman*. For that reason, I will assume that the traditional understanding of the ECS/RCS distinction governs. To the extent that *Theofel* and *Councilman* remain on the books, reforms designed to address them should be an obvious legislative priority. The panel opinion in *Councilman* guts the privacy protections of the Wiretap Act, and *Theofel* creates a highly implausible standard for determining what process law enforcement must satisfy to compel information from ISPs. Beyond those two cases, however, the SCA raises deeper issues that call for legislative attention.

A. Bolster Privacy Protections for Compelled Content Information

The most obvious problem with the current version of the SCA is the surprisingly weak protection the statute affords to compelled contents of communications under the traditional understanding of ECS and RCS. Only unretrieved e-mail and other temporarily stored files held pending transmission for 180 days or less receive the protection of a full warrant requirement.[166] The lower standard that applies to other stored content covered by the statute is surprisingly low: a subpoena combined with prior notice suffices.[167] Indeed, in practice the standard is even lower, as "prior notice" can be quite easily delayed for long periods of time. Section 2705(b) of the SCA states that "a supervisory official"[168] within the

[166] *See* 18 U.S.C. § 2703(a) (2000 & Supp. I 2003).

[167] *See id.* § 2703(b).

[168] Section 2705(a)(6) defines "supervisory official" as "the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney's headquarters or

executive branch can order notice to be delayed by up to ninety days if there is "reason to believe that notification of the existence of the subpoena may have an adverse result,"[169] such as "destruction of or tampering with evidence"[170] or anything else that "seriously jeopardiz[es] an investigation."[171] A court can authorize additional delays in notice under the same standard.[172] In practice, this means that the government can often compel all opened e-mails from an ISP with a mere subpoena and without meaningful notice—precisely the result that the SCA was enacted to avoid.

The apparent thinking behind the lower thresholds for government access of both permanently stored files and unretrieved files stored for more than 180 days is that the lower thresholds track Supreme Court precedents interpreting the Fourth Amendment. For example, in *Couch v. United States*,[173] a defendant handed over records to her accountant so her accountant could process the data and complete the defendant's tax returns.[174] The Court held that by giving her records to the accountant, Couch had relinquished her reasonable expectation of privacy.[175] A provider acting as an RCS likely falls under this precedent: a person uses an RCS for outsourcing much like Couch used her accountant. Similarly, the strange "180 day rule" dividing § 2703(a) from § 2703(b) may reflect the Fourth Amendment abandonment doctrine at work. Individuals lose the Fourth Amendment protection in property if they abandon the property,[176] and the SCA's drafters may have figured that unretrieved files not accessed after 180 days have been abandoned.

Even assuming that Fourth Amendment principles explain the dividing line between § 2703(a) and (b) as a descriptive matter, this tells us nothing about what standards the SCA *should* adopt. After all, the SCA was passed to bolster the weak Fourth Amendment privacy protections that applied to the Internet. Incorporating those weak Fourth Amendment principles into statutory law makes little sense. The SCA's drafters should have focused on finding the level of privacy protection that best balances privacy and security, not on finding the privacy protections that track Supreme Court cases decided long before the modern Internet.

The legislative solution is to bolster the privacy protections that cover

regional office." *Id.* § 2705(a)(6).

[169] *Id.* § 2705(a)(1)(B).

[170] *Id.* § 2705(a)(2)(C).

[171] *Id.* § 2705(a)(2)(E).

[172] *See id.* § 2705(a)(4).

[173] Couch v. United States, 409 U.S. 322 (1973).

[174] *Id.* at 324.

[175] *See id.* at 334–35.

[176] *See* United States v. Jones, 707 F.2d 1169, 1172 (10th Cir. 1983) ("When individuals voluntarily abandon property, they forfeit any expectation of privacy in it that they might have had.").

stored content held by an RCS or by an ECS for more than 180 days in 18 U.S.C. § 2703(b). There are many ways to do this, of course, ranging from minor additions to major ones. Let me suggest a cautious middle ground. First, Congress should eliminate the phrase "uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena" from § 2703(b)(1)(B)(i), along with its corresponding language in the delayed notice provisions of § 2705(a)(1)(B).[177] This change would require the government to obtain a 2703(d) order to compel stored contents from an RCS and either give prior notice or obtain a *court-issued* delayed notice order. The government would no longer be allowed to compel contents from an RCS with a mere subpoena, or to delay notice without judicial review.

Second, Congress should cut the delay period in 18 U.S.C. § 2705 from a period "not to exceed ninety days"[178] to a period "not to exceed thirty days." The current ninety-day delay period is simply too long. In all but very unusual cases, ninety days of delay is a period out of proportion to the legitimate law enforcement interests in delay articulated in § 2705(a)(2). It may be reasonable for law enforcement to have a thirty-day delay of notice if they are investigating a crime and the notice may tip off the suspect. The thirty-day period gives the police time to assess the evidence, pursue leads, and indict the target if necessary. But in most cases, giving the government ninety days serves no legitimate purpose, especially given that courts can grant extensions of delayed notice for additional periods if circumstances warrant. Shortening the delay period would still allow the government to delay notice for legitimate reasons but would help ensure that notice delayed does not become notice denied.

B. *Simplify the Statute*

The complexity of the SCA prompts an obvious question: are there ways to simplify the statute so that it can be understood more easily? The answer is yes. Most important, Congress could eliminate the confusing categories of ECS and RCS and simply incorporate these concepts into the statute directly. Rather than divide the SCA artificially into two types of providers based on their function, the statute could use just one type of provider and distinguish among the files a provider holds based on its function with respect to that file. For example, Congress could rewrite the statute so that the SCA applied only to "network service providers," which could be defined using a combination of the current definitions for ECS and RCS. The statute could then apply the different rules of the current

[177] The new version of 18 U.S.C. § 2703(b)(1)(B) would read: "with prior notice from the governmental entity to the subscriber or customer if the governmental entity obtains a court order for such disclosure under subsection (d) of this section;".

[178] This phrase appears in 18 U.S.C. § 2705(a)(1)(A), (a)(1)(B), and (a)(4).

SCA to the different types of files held by network service providers. The new text could look like this:

> Section 2703. Compelled Disclosure
>
> A governmental entity may lawfully compel the disclosure of communications and information held, maintained, or possessed by a network service provider in the following circumstances:
>
> (a) to compel the disclosure of contents of communications held in any temporary, intermediate storage incidental to the electronic transmission of the communication for 180 days or less, including any backup copies of such communications, pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant;
>
> (b) to compel the disclosure of contents of communications held by a network service provider to the public for the purposes of computer storage or processing on behalf of a customer or subscriber, or to compel the disclosure of contents of communications held in any temporary, intermediate storage incidental to the electronic transmission of the communication for more than 180 days, pursuant to either (1) a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; (2) a court order issued under subsection (f) of this section,[179] combined with prior notice from the governmental entity to the subscriber or customer or else delayed notice pursuant to Section 2705 of this title, or (3) an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena, combined with prior notice from the governmental entity to the subscriber or customer or else delayed notice pursuant to Section 2705 of this title;
>
> (c) to compel any other contents not covered by (a) or (b) of this subsection pursuant to any other legal means;
>
> (d) except as provided in subsection (e), to compel the disclosure of a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications), pursuant to either (1) a warrant issued using the procedures described in the Federal Rules of Criminal Procedure

[179] Because I have restructured the statute, the provision that allows specific and articulable facts court orders to be applied for and entered would move from § 2703(d) to § 2703(f).

> by a court with jurisdiction over the offense under investigation or equivalent State warrant, (2) a court order issued under subsection (f) of this section, or (3) the consent of the subscriber or customer to such disclosure.
>
> (e) to compel the disclosure of the following information pertaining to a subscriber to or customer of such service—
>
> (1) name;
>
> (2) address;
>
> (3) local and long-distance telephone connection records, or records of session times and durations;
>
> (4) length of service (including start date) and types of service utilized;
>
> (5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
>
> (6) means and source of payment for such service (including any credit card or bank account number)—
>
> either through means described in subsection (d), or else pursuant to an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena.

This text is significantly simpler than the existing statute, and it does exactly the same thing that § 2703 does today.[180] The proposed § 2703(a) and (b) track the function of the current (a) and (b). The proposed § 2703(c) makes clear that content information held by providers not specifically protected by (a) or (b) is not protected by the statute, which is true today but hard to see at first in the current text. The proposed § 2703(d) would do the work of the current § 2703(c)(1), and the proposed § 2703(e) would cover the basic work of the current § 2703(c)(2). The new text would regulate just one kind of provider, and then list the rules for compelling different types of information from the provider based on the same criteria that the current statute adopts. The new text would harness

[180] With one exception: I have deleted the rather silly special rule for obtaining noncontent information for telemarketing fraud cases, currently codified at 18 U.S.C. § 2703(c)(1)(D). This special rule allows the government to compel noncontent records if an investigator "submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing." 18 U.S.C. § 2703(c)(1)(D). Not even a subpoena is required. This provision was passed in 1998 after Congress became concerned about the dangers of telemarketing fraud. *See* H.R. REP. NO. 105-158, at 2–3 (1997), *reprinted in* 1998 U.S.C.C.A.N. 227, 228. Presumably it seemed like a good idea at the time, but today it seems hard to justify treating telemarketing fraud differently than other crimes.

the same functionality as the current version but would be much clearer and easier to follow.

The voluntary disclosure provisions found in § 2702 could receive similar treatment. The difficulty with the current § 2702 is that it uses separate text for different categories even when the rules for the different categories end up being basically the same. Specifically, § 2702(a) contains separate prohibitions on disclosure broken down into the prohibition for contents held by an RCS,[181] for contents held by an ECS available to the public,[182] and for noncontent information.[183] Section 2702 then contains a list of exceptions for contents in § 2702(b) and a separate (but very similar) list of exceptions for noncontent information in § 2702(c).[184] This structure could be simplified by placing all of the prohibitions into one sentence and then combining the exceptions for content and noncontent information.

> Section 2702. Voluntary disclosure
>
> (a) Except as provided in subsection (b), a network service provider to the public or its agent shall not knowingly divulge to any person or entity either the contents of that communication or any record or other noncontent information pertaining to a subscriber to or customer of such service.
>
> (b) A person or entity may divulge—
>
> (1) the contents of a communication to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;
>
> (2) the contents of a communication or noncontent records, or both, as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;
>
> (3) the contents of a communication or noncontent records, or both, 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;
>
> (4) the contents of a communication to a person employed or authorized or whose facilities are used to forward such communication to its destination;
>
> (5) the contents of a communication or noncontent records, or both, as may be necessarily incident to the rendition of the service

[181] *See* 18 U.S.C. § 2702(a)(2).

[182] *See id.* § 2702(a)(1).

[183] *See id.* § 2702(a)(3).

[184] *See id.* § 2702(b), (c).

> or to the protection of the rights or property of the provider of that service;
>
> (6) the contents of a communication or noncontent records, or both, to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032);
>
> (7) the contents of a communication to a law enforcement agency if the contents were inadvertently obtained by the service provider and appear to pertain to the commission of a crime;
>
> (8) the contents of a communication or noncontent records, or both, to a Federal, State, or local governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency; or
>
> (9) noncontent records to any person other than a governmental entity.

Again, this version would simplify the statute without losing its current functionality. The rules would remain the same, but would appear in language simple enough that lawyers, ISPs, law enforcement agents, and judges would be able to understand the statute more easily. Do I expect Congress to change the SCA along these lines any time soon? No. The maxim "if it ain't broke, don't fix it" is true in law as well as in life, and it may seem extravagant to restructure the statute just to make it easier to understand. At the same time, the complexities of the SCA are mostly unnecessary, and simplifying the statute would improve it considerably.

C. Repeal 18 U.S.C. § 2701

A slightly more radical proposal would be to repeal 18 U.S.C. § 2701, the first provision of the SCA that appears in Title 18. Section 2701 is the only part of the SCA that does not relate to procedural rules. Instead, it lays out a substantive criminal prohibition, punishable by up to a year in jail for first offenses and more serious penalties for subsequent offenses:

> [W]hoever—(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished.[185]

[185] 18 U.S.C. § 2701(a) (2000).

Section 2701 is a very close cousin of another criminal statute, 18 U.S.C. § 1030, sometimes known as the Computer Fraud and Abuse Act.[186] Section 1030 is the primary federal computer crime statute.[187] Its basic mechanism is a prohibition on accessing a computer without authorization, or exceeding authorized access, in a variety of different circumstances listed in § 1030(a).[188] Section 2701 adds an additional circumstance to the list: accessing a computer without authorization or exceeding authorization is an offense when the computer is acting as an ECS and the person "obtains, alters, or prevents authorized access" to a file in "electronic storage."[189] Note the narrow scope of § 2701. It applies only to providers of ECS and excludes providers of RCS. The legislative history does not explain why, but the approach is consistent with the SCA's greater protection for files held by providers of ECS than files held by providers of RCS.[190]

Section 2701 should be repealed because its costs greatly outweigh its benefits. The benefits of § 2701 are quite limited because the statute is almost entirely redundant. Section 1030(a)(2) already covers most of the same ground. For example, § 1030(a)(2)(C) provides that:

> [Whoever] intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer if the conduct involved an interstate or foreign communication [shall be punished].[191]

Section 1030(a)(2)(C) is remarkably broad; a "protected computer" includes pretty much any computer connected to the Internet,[192] and a user

[186] *See* 18 U.S.C. § 1030 (2000 & Supp. I 2003).

[187] I have written about this statute and the prohibition on unauthorized access at length in Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596 (2003).

[188] *See id.* at 1616.

[189] 18 U.S.C. § 2701(a).

[190] *See, e.g.*, 18 U.S.C. § 2703(a)–(b) (2000 & Supp. I 2003).

[191] *Id.* § 1030(a)(2)(C).

[192] Section 1030(e)(2) states that "the term 'protected computer' means a computer . . . which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." *Id.* § 1030(e)(2). In most cases, any computer connected to the Internet will satisfy this requirement. *See* United States v. Carroll, 105 F.3d 740, 742 (1st Cir. 1997) ("Transmission . . . by means of the Internet is tantamount to . . . transportation in interstate commerce.").

The definition of "protected computer" includes a notable ambiguity: it is not clear whether the phrase "used in interstate or foreign commerce or communication" refers to use at the time of the event in question, or generally, or at some point in the past. I think the best answer is that "use" refers to use during the event at issue. For example, if a person connects to the Internet from a desktop computer, that computer is a "protected computer" during the time that he is logged on. However, after the user has logged off, the computer is "obtains" a communication simply by viewing it on his screen.[193] This means that § 2701 is at most only a jurisdictional hook that applies in an extremely narrow circumstance. Specifically, § 2701 provides federal jurisdiction for acts of hacking into and otherwise damaging providers of ECS in the rare circumstance that the conduct does not involve an interstate or foreign communication.

Redundancy alone is not a compelling reason to repeal a statute. But § 2701 comes with a significant cost: its vague language has needlessly confused the courts, which have tried to use § 2701 in civil cases to do far more than the SCA's drafters ever intended. As a result, several of the major judicial interpretations of the SCA arise from § 2701 cases and misinterpret the SCA almost beyond recognition. The fault for this lies in part with the civil remedies within the SCA; as I have explained elsewhere, the combination of strong civil remedies and the absence of a statutory suppression remedy for violations of the SCA has led courts to misconstrue the SCA because the courts have a hard time understanding its criminal procedure rules in a civil context.[194] But the fault also lies with § 2701.

The Ninth Circuit's recent decision in *Theofel v. Farey-Jones* illustrates the difficulty.[195] *Theofel* involved an overly broad subpoena for e-mail issued as part of the civil discovery process in a commercial dispute.[196] The subpoena was served on the plaintiff's ISP, and the ISP responded by posting copies of the plaintiff's e-mail on a web server where defendants could (and did) read them.[197] The plaintiffs sued under § 2701 of the SCA.[198] They should have sued under § 2703: the defendants had violated § 2703 by using improper legal process to compel the disclosure of e-mail from an ECS/RCS in violation of § 2703(a) and (b).[199] The plaintiffs instead sued under § 2701, contending that the defendants had caused the ISP employees to commit an unauthorized access of their own server when they retrieved the files from the server and posted them on the website.[200] This is a strange claim, and agreeing with it required creating new, expansive, and (in some cases) extraordinary interpretations of several key concepts in computer crime law: the meaning of authorization, the meaning of access, the scope of ECS protections, and the scope of provider

no longer being used in interstate communication. Under any one of these approaches, however, the phrase "protected computer" is quite broad.

[193] S. REP. NO. 99-432, at 6 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2484.

[194] *See* Kerr, *supra* note 3, at 807.

[195] *See* Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004).

[196] *See id.* at 1071–72.

[197] *See id.* at 1071.

[198] *See id.* at 1072.

[199] *See* Tucker v. Waddell, 83 F.3d 688 (4th Cir. 1996); Freedman v. Am. Online, Inc., 303 F. Supp. 2d 121 (D. Conn. 2004).

[200] *See Theofel*, 359 F.3d at 1071–72.

rights. But eager to find a violation and apparently unaware of how plainly these facts fit into § 2703, Judge Kozinski charged onwards and crafted a dubious theory under which the plaintiffs could win under § 2701.[201] If § 2701 were repealed, courts and litigants would go directly to the relevant sections of § 2702 and § 2703 without being tempted to distort key concepts under § 2701.

D. Alter the Remedies for Violations of the SCA

The remedies for violations of the SCA should also be changed. I have written about this problem at length before,[202] so I will only quickly summarize the argument here and then add a few thoughts on the broader problem.

The current version of the SCA authorizes civil suits for violating the statute, but it does not contain a statutory suppression remedy.[203] The absence of a statutory suppression remedy has added to the confusion about the SCA for two reasons. First, few if any cases exist interpreting the SCA in a routine criminal context that might explain how the statute works.[204] Second, the few cases interpreting the statute have tended to arise in unusual civil contexts far removed from the real problems that led Congress to enact the law.[205] As a result, few cases interpreting the statute exist, and several of the cases that are on the books misconstrue the statute dramatically.[206] Congress could correct this problem by adding a statutory suppression remedy to the SCA. A suppression remedy would guarantee that criminal defendants challenge government and ISP practices under the SCA, giving courts cases and controversies in which to explain clearly how the statute works.[207]

Beyond adding a suppression remedy, Congress should also clarify

[201] On the implausibility of Judge Kozinski's theory about the scope of ECS protections, see *supra* note 62. Kozinski's opinion also reduced the language of § 2703(c)(1) to a nullity. Section 2703(c)(1) has generally been read as a provider exemption from § 2701 liability, but after *Theofel*, that status is unclear. *See Theofel*, 359 F.3d at 1073. Further, Kozinski's reading of § 2701 plainly conflicts with § 2702. While § 2702 permits providers to disclose contents to nongovernment entities, Kozinski's reading of § 2701 conflicts with § 2702 by focusing on the initial step of the ISP's obtaining the information instead of the latter step of the subsequent disclosure. As I see it, the only step that Kozinski got right was the basic framework for determining authorization; his reliance on the distinction between fraud in the factum and fraud in the inducement is the same that I offer as a way of interpreting authorization in my recent article on unauthorized access statutes. *See* Kerr, *supra* note 187, at 1648–56.

[202] *See generally* Kerr, *supra* note 3.

[203] *See id.* at 817.

[204] *See id.* at 823–25.

[205] *See id.* at 829–30.

[206] *See id.* at 830–36 (discussing cases misconstruing the SCA).

[207] *See id.* at 836–40.

who can be sued under the civil provisions of the Act. The statute itself is somewhat unclear as to when the government is liable for violating the statute, as opposed to the ISP, or both. *Tucker v. Waddell*[208] illustrates the problem. In *Tucker*, the United States Court of Appeals for the Fourth Circuit considered a civil suit brought against the City of Durham, North Carolina, by a telephone subscriber named Tucker.[209] Durham police officers had obtained basic subscriber information about Tucker from her telephone service provider, GTE, but had used subpoenas that the district court characterized as "improper."[210] Tucker sued the city on the ground that the agents had used improper subpoenas violating the SCA's requirement that real subpoenas must be obtained to compel basic subscriber information.[211] The Fourth Circuit rejected the argument, holding that the rules of § 2703(c) regulate only providers of ECS and RCS, but not the government:

> The language of § 2703(c) does not expressly proscribe *any* action by governmental entities or their employees. Rather, § 2703(c) only prohibits the actions of providers of electronic communication services and remote computing services. . . . To be sure, this section discusses different courses of action available to governmental entities wishing to obtain customer information, but only in the context of limiting the circumstances under which *providers* may disclose such information.[212]

The court acknowledged that the regulations on compelling content in § 2703(a) and (b) presented a different case: these sections regulated the government, the court concluded, rather than the ISP.[213] As a result, the government could be held liable for violations of § 2703(a) and (b), but not § 2703(c)[214]—and by implication, presumably not any of the voluntary disclosure provisions of § 2702 either.

[208] *See* Tucker v. Waddell, 83 F.3d 688 (4th Cir. 1996).

[209] *See id.* at 689–90.

[210] *Id*. at 690.

[211] *See id.*

[212] *Id*. at 691–92.

[213] *See id.* at 693. According to the court:

> While subsection (c) focuses on the conduct of the service providers, subsections (a) and (b) focus on the conduct of governmental entities. . . . The inclusion, within the same section, of two subsections limiting governmental access to information and one subsection limiting provider disclosure of information makes the distinction between the two eminently clear. . . . A governmental entity that violates the dictates of § 2703(a) or (b) may be held civilly liable for such violation. In contrast, the language of § 2703(c) does not prohibit any governmental conduct, and thus a governmental entity may not violate that subsection by simply accessing information improperly.

Id. at 692–93 (citations omitted).

[214] *See id.* at 693.

The reasoning in *Tucker* is weak, and at least one court has held that amendments to the SCA in the USA Patriot Act have overruled it.[215] But the case makes an important point by illustration: the current text of the SCA says little about when the government can be sued for violations and when providers can be sued. The text provides rules that must be followed and then provides a civil remedy, but it does not explain in what circumstances the government versus providers can be held liable. To the extent that Congress continues to use the civil remedies in the SCA as the primary means of allowing enforcement of the statute, closer attention should be paid to who should pay and in what circumstances.

Conclusion

Law professors are in the business of giving grades, so I will conclude by giving a grade to the SCA. I would give the current SCA a "B." On the positive side, the statute's basic mechanisms are sound. The statute creates a set of Fourth Amendment-like rules in light of the uncertain application of Fourth Amendment protections to stored Internet files. It is a complex statute, but it is complex in part for the same reason that Fourth Amendment doctrine is complex: any effort to give a rule for every circumstance in which the government may obtain evidence must consider a wide range of facts, and the law should provide a context-sensitive rule to be followed for each set of facts. The SCA's distinctions and dichotomies try to recognize the important facts and set rules accordingly; in effect, the statute reflects an effort to codify the notion of Fourth Amendment reasonableness in the context of ISP interactions with law enforcement without the baggage of existing Fourth Amendment doctrine. It is a particularly remarkable achievement given that its enactment dates back to 1986. The SCA has weathered intervening technological advances surprisingly well.

At the same time, the SCA suffers from several flaws. It is more complicated than it needs to be. It has sections that are redundant and merely add confusion. The absence of a statutory suppression remedy has created significant uncertainty about how the statute works. The SCA also offers surprisingly low privacy protections when the government seeks to compel contents other than unretrieved communications held pending transmission for 180 days or less. The SCA needs significant legislative attention to bring its grade up from a "B" to an "A."

[215] *See* Freedman v. Am. Online, Inc., 303 F. Supp. 2d 121, 126 (D. Conn. 2004).