Notre Dame Law Review

Volume 88 | Issue 1 Article 10

11-1-2012

A Distinctionless Distinction: why the RCS/ECS Distinction in the Stored Communications Act Does Not Work

Eric R. Hinz

A DISTINCTIONLESS DISTINCTION: WHY THE RCS/ECS DISTINCTION IN THE STORED COMMUNICATIONS ACT DOES NOT WORK

*Eric R. Hinz**

Introduction

On April 30, 2003, Tamara Greene was shot dead by a .40 caliber pistol, the same caliber used by the Detroit police.[1] Mayor Kwame Kilpatrick, celebrating his election as the youngest mayor of Detroit, is alleged to have had a party half a year earlier at the mayoral Manoogian Mansion. The party was supposedly attended by strippers—including Tamara Greene.[2] According to a member of the mayor's protection unit, the mayor's wife arrived at the party and physically assaulted Ms. Greene.[3] Less than a year later, Tamara Greene was dead.

The murder occurred during an ongoing investigation into Kilpatrick, his security force, and the Manoogian party. This led to widespread speculation that the Detroit police had been involved in the killing.[4] Police officers involved in investigating the murder and the other incidents were either transferred or fired, including a deputy police chief.[5] Tamara Greene's family brought a suit against the City

* J.D. Candidate, Notre Dame Law School, 2013; B.S., Boston College, 2010. I would like to thank the Honorable Stephen J. Murphy, III for his inspiration on the topic, Professor Jay Tidmarsh for his continued mentoring throughout law school, the staff of the *Notre Dame Law Review* for their hard work and good cheer, and finally my family for their love and support.

1 David Ashenfelter, *Mystery of Who Killed Stripper Thickens—Ex-Cop's Affidavit in Suit Says Officer Shot Her; City's Lawyer Calls That Absurd*, Detroit Free Press, Mar. 4, 2008, at 1A, *available at* http://crimeindetroit.com/Documents/Mystery%20of%20Who%20Killed%20Stripper%20Thickens.pdf.

2 *Id.*

3 Curt Guyette, *Internal Affairs?*, Metro Times, May 26, 2004, http://www2.metrotimes.com/editorial/story.asp?id=6269.

4 Ashenfelter, *supra* note 1.

5 *Firing Deputy Police Chief Starts New Storm for Mayor of Detroit*, N.Y. Times, May 16, 2003, at A20, *available at* http://www.nytimes.com/2003/05/16/us/firing-deputy-police-chief-starts-new-storm-for-mayor-of-detroit.html?src=pm.

for obstructing the investigation. As part of the suit, they requested thousands of city text messages surrounding the dates of the incident.[6]

Later, during a whistleblower suit about the improprieties of the mayor, Kilpatrick and his then chief of staff, Christine Beatty, testified that the two of them had not had an extramarital affair together.[7] The mayor lost the suit and planned on appealing until the case was suddenly settled for $8.4 million. It was later discovered that the reversal and settlement came after the mayor's counsel found out that the plaintiffs were seeking to introduce thousands of text messages between the mayor and his chief of staff detailing the affair—evidence that the mayor had perjured himself.[8] These text messages led to Kilpatrick's resignation as mayor and subsequent criminal charges.[9]

As the cases resulting from Mayor Kilpatrick's actions show, text messages have become increasingly important in both civil and criminal suits. The disclosure of stored electronic communication, such as text messages, is governed by the Stored Communications Act (SCA).[10] The case allowing Tamara Greene's family to discover city text messages, *Flagg v. City of Detroit*,[11] has become an increasingly cited case interpreting the SCA. The Act creates a distinction between providers of Electronic Communication Services and Remote Computing Services.[12] A court must determine which category a provider falls into, as both have different discovery standards. As *Flagg* shows, this analysis is not an easy one; the court went as far as admitting that part of its analysis could be "mistaken."[13] This Note argues that the categories created by the Stored Communications Act do not adequately differentiate between different services, frequently overlap, and are unable to convincingly categorize contemporary services.

Part I describes the background, scope, categories, and disclosure standards of the Stored Communications Act. Particularly, Part I.C

6 *See* Flagg v. City of Detroit, 252 F.R.D. 346, 355 (E.D. Mich. 2008) (finding text messages from city officials satisfied the definition of "public records" and the SCA did not preclude discovery of these electronically stored communications).

7 Nick Bunkley, *Detroit Mayor Loses Fight Over Secret Papers*, N.Y. TIMES, Feb. 28, 2008, at A14, *available at* http://www.nytimes.com/2008/02/28/us/28detroit.html.

8 *Id.*

9 Bill McGraw, *The Rise and Fall of Kwame Kilpatrick*, DETROIT FREE PRESS, Sept. 5, 2008, http://www.freep.com/article/20080905/NEWS01/809050448/The-rise-fall-Kwame-Kilpatrick.

10 *See* 18 U.S.C. §§ 2701–12 (2006) (detailing the different evidentiary standards the government must meet to access cell phone records, including text messages).

11 252 F.R.D. 346 (E.D. Mich. 2008).

12 *See infra* Part I.B.

13 *Flagg*, 252 F.R.D. at 363.

delves into the different results that occur based on a court's categorization of a service. Part II discusses some important cases that seek to interpret and apply the Act, often with contradictory results. Part III discusses ways the Act could be applied to contemporary services. Specifically, it seeks to show how many common services could be considered either an electronic communication service or a remote computing service depending on the result desired by the court. Finally, Part IV analyzes recent amendments proposed to the SCA in light of much criticism and suggests an alternative path that Congress should take.

I. The Stored Communications Act

The Stored Communications Act,[14] a part of the Electronic Communications Privacy Act (ECPA),[15] was passed in 1986 to fill a perceived need to protect the privacy of electronic communication.[16] Due to rapid technological advances in computing and communication, individuals and corporations had a plethora of new options to process and store data and communicate with others.[17] These advances pushed the scope of the Fourth Amendment as understood in existing case law and statutes in effect at the time.[18] This section explores the background and history surrounding the Act and provides an explanation of the relevant parts of the Act.[19]

---

14 18 U.S.C. §§ 2701–12.

15 Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in 18 U.S.C.).

16 *See* S. Rep. No. 99-541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555 ("[This] bill . . . update[s] and clarif[ies] Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies."); H.R. Rep. No. 99-647 (1986).

17 S. Rep. No. 99-541, at 1–2, *reprinted in* 1986 U.S.C.C.A.N. at 3555 ("When the Framers of the Constitution acted to guard against the arbitrary use of Government power to maintain surveillance over citizens, there were limited methods of intrusion into the 'houses, papers, and effects' protected by the [F]ourth [A]mendment. During the intervening 200 years, development of new methods of communication and devices for surveillance has expanded dramatically the opportunity for such intrusions.").

18 *See id.*

19 While ECPA contains sections regarding interception of communication (Title I) and pen registers and other tracking devices (Title III), they are not within the scope of this Note. Further, sections of the SCA examining the civil penalties for violations of the Act are not necessarily important for the subsequent analysis.

A. Background

The SCA was passed in large part to cover areas of electronic information left open by the Fourth Amendment.[20] The Fourth Amendment protects one's "reasonable expectation of privacy."[21] This protects the inside of one's house,[22] the inside of one's car that is not in plain view,[23] the contents of a phone conversation,[24] etc. However, once a purportedly protected piece of communication has been placed in plain view[25] or released to a third party,[26] it no longer receives the same protection.

This "third-party doctrine" made it especially difficult to apply the Fourth Amendment protections to the electronic communications covered in the SCA. With the growth of computing services and electronic mail, individuals and businesses had many more choices in determining their communication and computing needs.[27] While

20 *See* S. REP. NO. 99-541, at 3, *reprinted in* 1986 U.S.C.C.A.N. at 3557 ("With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information.").

21 *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("My understanding of the [Fourth Amendment] rule that has emerged . . . is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

22 *See* Kyllo v. United States, 533 U.S. 27, 31 (2001) (citing Silverman v. United States, 365 U.S. 505, 511 (1961)) (finding the "very core of the Fourth Amendment" recognizes the "right of man to retreat into his own home and there be free from unreasonable governmental intrusion" (internal quotations omitted)).

23 *See* Arizona v. Gant, 556 U.S. 332, 335 (2009) (holding police may search a vehicle incident to an arrest only if the arrestee has not been secured or it is reasonable to believe evidence substantiating the arrest may be found).

24 *See Katz*, 389 U.S. at 358–59 (finding unconstitutional the warrantless installation of a government wiretap on a public telephone booth).

25 *See* Horton v. California, 496 U.S. 128, 133 (1990) (citing Arizona v. Hicks, 480 U.S. 321, 325 (1987); Illinois v. Andreas, 463 U.S. 765, 771 (1983)) ("If an article is already in plain view, neither its observation nor its seizure would involve any invasion of privacy.").

26 *See* United States v. Miller, 425 U.S. 435, 443 (1976) ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities . . . ."); *see also* Patricia L. Bellia, *The Memory Gap in Surveillance Law*, 75 U. CHI. L. REV. 137, 139–41 (2008) (discussing how the law has responded and should respond to increased data storage of personal information by third parties). *But see* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").

27 *See* S. REP. NO. 99-541 (1986), at 3, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557 ("With the advent of computerized recordkeeping systems, Americans have lost the

businesses may have utilized computers around the time the SCA was enacted, the amount of computing power needed to process large amounts of data was still very expensive. So, businesses often sent their data processing needs off to other businesses. The problem, though, was that as soon as they gave their data to a third party for processing, it was controlled by a third party and was no longer subject to Fourth Amendment protections.[28]

The committee reports accompanying the proposed bill used the example of the choice faced by hospitals.[29] Hospitals have large amounts of records and data to process. While it would now be quite affordable to process this information in-house, at the time, the computing power needed would have been very expensive for a normal business. It often made financial sense for the hospitals to send the information out for processing elsewhere. In the course of processing the information, services often made copies to hold in storage in case a backup was needed.[30] However, by doing this, information that had been protected was released to third parties, effectively eliminating the protections.

Similar issues arose with the increase of electronic communication. Congress recognized that there was a big gap between the protections provided for first class mail and those afforded to electronic communication.[31] There was a great deal of law protecting mail from being opened without authorization, but there was nothing comparable to protect messages sent by newer forms of technology.[32] Yet, businesses and individuals used electronic communication in virtually the same way as traditional first class mail. Congress was concerned that this gap could create uncertainty and "may unnecessarily discourage

---

ability to lock away a great deal of personal and business information. For example, physicians and hospitals maintain medical files in offsite data banks, businesses of all sizes transmit their records to remote computers to obtain sophisticated data processing services.").

28 *See Miller*, 425 U.S. at 441–443 ("[Information conveyed to a third party no longer falls under Fourth Amendment protection] 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.").

29 S. REP. NO. 99-541, at 3, *reprinted in* 1986 U.S.C.C.A.N. at 3557.

30 *Id.*

31 *Id.* at 5, *reprinted in* 1986 U.S.C.C.A.N. at 3559.

32 *See id.* ("A letter sent by first class mail is afforded a high level of protection against unauthorized opening by a combination of constitutional provisions, case law, and U.S. Postal Service statutes and regulations. . . . [Yet] there are no comparable Federal statutory standards to protect the privacy and security of communications transmitted by new noncommon carrier communications services or new forms of telecommunications and computer technology.").

potential customers from using innovative communications systems . . . [and] may discourage American businesses from developing new innovative forms of telecommunications and computer technology."[33]

Electronic communication was included within the SCA because, unlike modern e-mail, storage of messages was an important part of transmission.[34] At the time the statute was written, e-mail was transmitted over telephone lines. A subscriber would type a message on a computer, connect to the telephone line, and then send it to the recipient electronic mail company.[35] The message would be stored until the intended recipient connected with the company and the message would be downloaded to the final computer. While the provider would store the message as part of the transmission, a final copy was actually downloaded to the recipient computer.[36] The same privacy issues that occurred with remote computer processing occurred with electronic mail because the provider, at least temporarily, had a copy of the message.[37]

B. The Scope of the Stored Communications Act

To fill in the potential gaps in privacy protection, Congress passed the Stored Communications Act. The SCA seeks to balance the privacy concerns of Internet subscribers, while also creating channels for the government to obtain information necessary for investigations.[38] The statute does this in two primary ways.[39] First, it prevents the voluntary disclosure of electronic communication to the public.[40]

---

33 *Id.* While Congress was very concerned with protecting privacy interests, it also seemed concerned with creating clear standards to protect law enforcement from liability and the admissibility of evidence. *Id.*

34 *Id.* at 8, *reprinted in* 1986 U.S.C.C.A.N. at 3562.

35 *Id.*

36 *See id.* It is helpful to note at this point that modern e-mail generally does not work this way. Unless a user imports his or her mail into Outlook or a similar program, the user will rarely actually have a copy of his e-mail saved to the computer. *See infra* Part III.B.

37 *See* H.R. REP. NO. 99-647, at 22 (1986) ("[The provider] may technically have access to the contents of the message and may retain copies of transmissions.").

38 *In re* Subpoena Duces Tecum to AOL, LLC, 550 F. Supp. 2d 606, 610 (E.D. Va. 2008).

39 *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1212 (2004) ("The statute creates a set of Fourth Amendment-like privacy protections by statute, regulating the relationships between government investigators and service providers in possession of users' private information.").

40 18 U.S.C. §2702 (2006).

Second, the Act sets in place the procedural framework that the government must follow to compel disclosure.[41]

The SCA makes a very important distinction based on the prevalent functions of network service providers at the time. This distinction is one of the central aspects of the Act and is the focus of this Note. In order to determine the level of applicable protections, a court must determine if the service provides an Electronic Communication Service (ECS) or if it provides a Remote Computing Service (RCS).[42] Services that provide for the sending and receiving of electronic communication such as e-mail and text messages are electronic communication services.[43] The Act regulates the information transmitted and stored by these services. Meanwhile, services that provide storage and processing are remote computing services.[44] The Act regulates the use of the information delivered to, and retained by, these services.

The SCA defines an ECS as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[45] Since it is the storage of the sent information that is at issue in the statute, the Act defines electronic storage as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof,"[46] and "such communication [as is stored] . . . for purposes of backup protection of such communication."[47] On the other hand, an RCS is "the provision to the public of computer storage or processing services by means of an electronic communications system."[48]

---

41 *Id.* §2703.

42 *See* Flagg v. City of Detroit, 252 F.R.D. 346, 362 (E.D. Mich. 2008) ("[S]ervice providers contract with their customers to provide either an ECS or an RCS, but not both."); *see also* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965 (C.D. Cal. 2012) (analyzing whether Facebook and MySpace provide ECS, RCS, both, or neither); Kerr, *supra* note 39, at 1213 ("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.").

43 18 U.S.C. § 2510(15).

44 *Id.* § 2711(2).

45 *Id.* § 2510(15).

46 *Id.* § 2510(17)(A).

47 *Id.* § 2510(17)(B). The term "backup protection" is left undefined by the statute and committee reports, leading to much of the confusion the courts have faced in trying to classify various services. This will be discussed in more depth in Part II, *infra*.

48 *Id.* § 2711(2). Further, the Act defines an "electronic communications system" as "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related

An important point is that the designation of ECS or RCS refers to the specific service provided, not to the providers that facilitate the service.[49] This is important because the services provided by one provider could be classified as an ECS at one point and an RCS at another. As Professor Orin Kerr points out, the test is "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."[50] So, as an example,[51] when one person sends electronic communication to another person, the provider of the service remains an ECS during the process up until the point when the message is opened.[52] After reading the communication, the recipient of the communication may decide he wants that communication for future reference. So, he will save it through the same provider that transmitted the message to him. Now, the provider is holding the message in storage and is acting as an RCS.[53]

C. Disclosure Under the Stored Communications Act

The SCA sets guidelines for how and when an ECS or RCS provider can disclose communication. The Act first prohibits *voluntary disclosure* of communication that falls within either of the two services, subject to a series of exceptions. Then, the Act lays out the procedural requirements that the government must follow to *compel disclosure* from these service providers.

---

electronic equipment for the electronic storage of such communications." *Id.* § 2510(14).

49 *See* Kerr, *supra* note 39, at 1215.

50 *Id.*

51 This example is overly simplistic, but the nuances of the distinctions will be further developed in Part II, *infra*.

52 *See* Theofel v. Farley-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004) ("[Subsection (A) of the SCA applies] only to messages in 'temporary, intermediate storage' [which is] limited . . . to messages not yet delivered to their intended recipient." (citation omitted)).

53 *See* Flagg v. City of Detroit, 252 F.R.D. 346, 362–64 (E.D. Mich. 2008) (detailing the distinction between ECS and RCS).

1. Prohibitions on Voluntary Disclosure

The SCA prohibits providers of ECS and RCS from knowingly[54] disclosing the contents of electronic communication.[55] For an ECS, this means that it cannot disclose communication in "electronic storage"[56]—that is, storage incidental to the transmission or held for backup purposes.[57] For an RCS, this means the provider cannot disclose communication held by the service solely as storage or for computer processing[58]—but only if the RCS provider is not allowed to access the communication for reasons other than storage and processing.[59]

Section 2702 then provides a list of exceptions for when ECS and RCS providers may disclose content and non-content information. Content information is "information concerning the substance, purport, or meaning of that communication,"[60] whereas non-content information would include customer records, activity logs, etc.[61] Providers may disclose content information:

> (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 [Title 18];
> (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;

---

54 The committee reports make clear that the term "knowingly" means the provider "was aware of the nature of the conduct, aware of or possessing a firm belief in the existence of the requisite circumstances and an awareness of or a firm belief about the substantial certainty of the result." H.R. REP. NO. 99-647, at 64 (1986). Further, it means that "reckless" and "negligent" conduct does not meet the threshold. S. REP. NO. 99-541, at 37 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3591.

55 18 U.S.C. § 2702(a) (2006).

56 *Id.* § 2702(a)(1).

57 *Id.* § 2510(17)(B).

58 *Id.* § 2702(a)(2)(B).

59 *Id.* This restriction was likely made in an attempt to mirror the Fourth Amendment protections. If the provider is able to access electronic communication for reasons other than the two elaborated, the argument could no longer be made that the service is really just providing an extension of what the subscriber could do in his or her house. The arrangement would be much more analogous to sharing the information with another person, cueing the third-party doctrine. *See supra* Part I.A.

60 18 U.S.C. § 2510(8).

61 *Id.* § 2702(a)(3).

> (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 . . . ;
> (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 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.[62]

The third exception creates an important distinction that effectively creates different disclosure standards.[63] For an ECS to disclose content, it must have consent from either the originator, an addressee, or an intended recipient. An RCS, on the other hand, may get consent from any of the above, *or* the service subscriber. This, in practice, can make a big difference and can make it much easier to obtain information from an RCS than an ECS.[64] More importantly, the list of exceptions is more noteworthy for what it leaves out than for what it contains—there is no exception for complying with civil discovery subpoenas.[65] Courts have consistently held that this omission was deliberate, preventing third-parties from obtaining information through a subpoena.[66]

The non-content voluntary disclosure exceptions closely map the content disclosure exceptions.[67] In essence, non-content information like customer records, ISP numbers, etc. can be disclosed to anyone *except for a governmental entity*.[68] This seems to point to a strong desire

62 *Id.* § 2702(b) (emphasis added).

63 *See* Flagg v. City of Detroit, 252 F.R.D. 346, 359 (E.D. Mich. 2008).

64 *See id.*

65 18 U.S.C. § 2702(b). *See generally* Gaetano Ferro et al., *Electronically Stored Information: What Matrimonial Lawyers and Computer Forensics Need to Know*, 23 J. AM. ACAD. MATRIM. LAW. 1, 3–12 (2010) (explaining the difficulties in attaining stored communication in civil suits).

66 *See, e.g.*, Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 975–76 (C.D. Cal. 2010) (allowing plaintiffs to quash subpoenas delivered to providers of ECS); Viacom Int'l Inc. v. YouTube Inc., 253 F.R.D. 256, 264 (S.D.N.Y. 2008) (holding that the lack of "exception for disclosure of such communications pursuant to civil discovery requests" in the SCA prevents disclosure through a civil subpoena); *In re* Subpoena Duces Tecum to AOL, LLC 55 F. Supp. 2d 606, 611 (E.D. Va. 2008) ("[T]he statutory language of the [SCA] does not include an exception for the disclosure of electronic communications pursuant to civil discovery subpoenas.").

67 *See* 18 U.S.C. § 2702(c).

68 *Id.* § 2702(c)(6).

by Congress to prevent providers from voluntarily giving any information to the government.[69] If the government wants any information from a network service provider, it will need to follow the rules listed in § 2703.

2. Rules for Compelled Disclosure by the Government

The rules for compelled disclosure by the government are much more complex than for voluntary disclosure. While the voluntary disclosure rules treat ECS and RCS providers in roughly the same way,[70] the disparity in privacy protections becomes much more pronounced in compelled disclosure. The SCA creates a hierarchy of protections with the most private services receiving the most protections. As the communication becomes more distant from the originator or recipient, the process law enforcement must follow becomes less and less rigorous.[71]

There are two levels of process afforded electronic communication in electronic storage by a provider of ECS. First, the government may only obtain content information held in storage for 180 days or less pursuant to a warrant issued by a court of competent jurisdiction.[72] This means that for up to 180 days, the government will need to obtain a warrant to retrieve a person's unopened e-mail. After 180 days, the information in storage will be treated in the same manner as RCS storage, allowing for more options and less process. First, like pre-180 days ECS storage, the government can use a warrant to get content information from an RCS or from an ECS after 180 days.[73] The government may do so without notice. Second, the government may avoid getting a warrant and obtain information by providing notice[74] and an administrative subpoena or a 2703(d) order.[75] A

69 Orin Kerr points out the redundancy of this exception. *See* Kerr, *supra* note 39, at 1222 & n.94. The sixth exception allows a provider to give non-content information to anyone but a governmental entity. Yet, the restrictions on voluntary disclosure of non-content information in § 2702 specifically apply only to the government. So, the exception in § 2702(c) is unnecessary. *Id.*

70 *See supra* Part I.C.1.

71 *See* 18 U.S.C. § 2703.

72 *Id.* § 2703(a).

73 *Id.* § 2703(b)(A).

74 Section 2705 allows notice to be delayed for up to ninety days if a court or supervisory official believes notification may have adverse results. The section lists adverse results as endangering an individual, risk of flight, tampering of evidence and witnesses, or "otherwise seriously jeopardizing an investigation or unduly delaying a trial." *Id.* § 2705(a)(2).

75 *Id.* § 2703(b)(B). The SCA treats post-180 days ECS content the same as all RCS content. *Id.*

2703(d) order can be obtained from any court so long as the governmental entity can present "specific and articulable facts" reasonably demonstrating that the contents or records sought are relevant to the investigation.[76]

As the trend would indicate, even less process is required for compelling disclosure of non-content records. The government may require disclosure pursuant to a warrant,[77] with a 2703(d) specific and articulable facts order,[78] or through the consent of the subscriber or customer.[79] Lowering the burden from content disclosure, the SCA does not require the government to provide notice to the subscriber or customer when the government is compelling non-content information.[80] For certain non-content communication, the government must merely provide a subpoena to a network service provider.[81] The government can get such basic information about a subscriber or customer as his or her name, address, connection records and times, start dates, identity numbers such as telephone numbers or network addresses, and means of payment such as credit card numbers.[82]

Through these differing process requirements, the importance of distinguishing whether a provider storing information is acting as an ECS or an RCS becomes clear. In the realm of § 2702 voluntary disclosure, the rule is almost the same for both types of public providers: barring certain exceptions, either provider may not voluntarily[83] dis-

76 *Id.* § 2703(d). A 2703(d) order may be issued pursuant to this SCA "by any . . . court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." *Id.*

77 *Id.* § 2703(c)(1)(A).

78 *Id.* § 2703(c)(1)(B).

79 *Id.* § 2703(c)(1)(C). The SCA also allows the government to compel disclosure of non-content information by merely submitting a formal request when it is relevant to an "investigation concerning telemarketing fraud." *Id.* § 2703(c)(1)(D).

80 *Id.* § 2703(c)(3). The ability to obtain this information without any notice to the subscriber has been increasingly criticized lately. The government frequently requires ISPs to secretly disclose customer information and contacts. *See* Julia Angwin, *Secret Orders Target Email: WikiLeaks Backer's Information Sought*, WALL ST. J. (Oct. 9, 2011, 10:31 PM), http://online.wsj.com/article/SB10001424052970203476804576613284007315072.html?mod=wsj_share_facebook (detailing the U.S. government's "secret court order" to Google and small Internet provider Sonic.net Inc. to "turn over information from the email accounts" of WikiLeaks volunteer Jacob Appelbaum).

81 18 U.S.C. § 2703(c)(2).

82 *Id.* § 2703(c)(2)(A)–(F).

83 This includes civil subpoenas. *See supra* notes 65–66 and accompanying text.

close content information to anyone, and may not voluntarily disclose non-content customer records to the government.[84] However, there is an important aspect of voluntary disclosure where the distinction between ECS and RCS matters: the exception for consent.[85] A provider of ECS must have the consent of the sender or the receiver of the communication, while a provider of RCS need only get consent of the subscriber to the service.[86] This has large implications since many services are subscribed to by a larger organization, like a company, for use by its members or employees. In the course of civil litigation, an opposing party may seek the stored emails of an individual. If an employee (sender or recipient) refuses to give consent for disclosure,[87] but the company (subscriber) is willing to consent, the party seeking disclosure will only be able to get to information if the service provider can be classified as an RCS. With § 2703 compelled disclosure, the differences in treatment of ECS and RCS providers are even more pronounced. The government may only compel a provider of ECS to disclose information stored for less than 180 days pursuant to a warrant.[88] However, if the government can classify the provider of electronic storage as an RCS, it may merely provide the customer notice and send a subpoena or a § 2703(d) specific and articulable facts order.[89] Further, this notice may even be delayed for up to ninety days if it would adversely affect a trial.[90]

II. Confusion in the Courts

There has been a great deal of disagreement and confusion among the courts when it comes to classifying various types of services provided as either ECSs or RCSs. Some of this confusion comes from inherent structural flaws in the statute. This involves two related issues. First, whether communication held "for purposes of backup protection" should be understood expansively or narrowly.[91] Second,

84 *See supra* Part I.C.1.

85 *See* 18 U.S.C. § 2702(b)(3).

86 *See id.*; *see also* Flagg v. City of Detroit, 252 F.R.D. 346, 359–63 (E.D. Mich. 2008) (demonstrating that obtaining the necessary consent for discovery of text messages is much simpler if the service provider can be classified as an RCS rather than an ECS).

87 *But see Flagg*, 252 F.R.D. at 352–58 (holding that consent can be compelled under Fed. R. Civ. P. 34).

88 18 U.S.C. § 2703(a).

89 *Id.* § 2703(b).

90 *Id.* § 2705; *see supra* note 74 and accompanying text.

91 *See* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 902–03 (9th Cir. 2008).

in evaluating the relevant classifications, whether the court should look at the particular service provided for that particular piece of communication, or if it should look at the services provided by the provider and classify the provider itself.[92] Meanwhile, other confusion comes from the development of new and overlapping types of communications services since the enactment of the Act. Due to the changing ways communication is transmitted, it is difficult to categorize the various services. Analogizing to older forms of electronic services happens imperfectly and with conflicting results.[93] This section analyzes the ways some courts have approached these issues. As one will see, with all of the confusion, it would be quite easy for a court to classify most electronic services however it wants.

A. Theofel v. Farely-Jones

As has been discussed above, communication stored by an ECS provider is protected if the storage is (A) temporary, intermediate, and incidental to the transmission, or (B) for purposes of backup protection.[94] Confusion arose as to the status of post-transmission messages still in storage by the provider. Is this what was meant by "backup protection"? Many concluded from the legislative history and the technology at the time that backup protection referred to copies the service provider made while the message was on the provider's server in case an issue arose.[95] These copies could be left on the server for some time, but were not meant as storage for the subscriber. If the user left the messages on the server post-delivery, they would be using the service as an RCS.[96]

However, the Ninth Circuit decided to take a very different approach when it decided *Theofel v. Farley-Jones*,[97] finding that "for purposes of backup protection" should be interpreted expansively.

92 *Compare Flagg*, 252 F.R.D. at 362 (holding that the classification of the service provider changes based on the particular service it is providing), *with Quon*, 529 F.3d at 902–03 (classifying provider Arch Wireless based on the type of services it generally provides).

93 *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 988–89 (C.D. Cal. 2010) (finding it difficult to classify Facebook and MySpace wall posts and comments).

94 18 U.S.C. § 2510(17).

95 *See* S. REP. NO. 99-541, at 8 (1986) *reprinted in* 1986 U.S.C.C.A.N. 3555, 3562. *See also* Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 633–34 (E.D. Pa. 2001) (holding that backup protection involved storage pending delivery, but not post-delivery storage).

96 *See* Kerr, *supra* note 39, at 1216–17.

97 359 F.3d 1066 (9th Cir. 2004).

The case arose out of earlier commercial litigation against Farley-Jones. In the course of discovery, Farley-Jones sent a subpoena to NetGate, the plaintiffs' Internet Service Provider (ISP), for all of the plaintiffs' emails.[98] NetGate initially protested, but provided a sample of emails.[99] The plaintiffs, on hearing of this, asked the magistrate judge to quash the order and also filed a civil suit for violations of the Stored Communications Act, among other statutes. The district court dismissed the claims, bringing this case before the Ninth Circuit.[100]

In determining if these emails were protected under the ECS rules, the court had to first determine if they were in electronic storage. The panel agreed with the determinations of other courts[101] that these emails could not be considered in electronic storage under subsection (A) because they had already been delivered and were not in "'temporary, intermediate storage.'"[102] However, departing from conventional wisdom, the court found that the messages "do fit comfortably within subsection (B)."[103] Accordingly, these messages were clearly stored for backup protection "within the ordinary meaning of those terms."[104]

The court disagreed with previous courts, and arguments by the United States,[105] that backup protection could not include post-transmission storage: subsection (A) already covers any stored communication pending delivery. By interpreting subsection (B) to only cover pre-transmission communication, subsection (B) would be completely superfluous.[106] Rather, unlike (A), (B) does not distinguish between pre- and post-transmission storage. With that interpretation, then, the court found that "prior access [wa]s irrelevant."[107]

Further, the court held that backup copies did not need to be held solely for use by the ISP: an "obvious purpose" for storing backup

98 *Id.* at 1071.

99 *Id.*

100 *Id.* at 1071–72.

101 *See, e.g.*, *In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 512 (S.D.N.Y. 2001) (limiting coverage to messages awaiting delivery); Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001) (same).

102 *Theofel*, 359 F.3d at 1075 (quoting 18 U.S.C. § 2510(17)(A) (2006)).

103 *Id.* Electronic storage is "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17)(B).

104 *Theofel*, 359 F.3d at 1075.

105 The government's position "drains subsection (B) of independent content because virtually any backup of a subsection (A) message will itself qualify as a message in temporary, intermediate storage." *Id.* at 1076.

106 *Id.* at 1075–76.

107 *Id.* at 1077.

copies was to have another copy in case the user wanted to download it again.[108] However, the court did not go so far as to say that all stored copies were for backup protection. If an ISP kept permanent copies of the communication, or if the ISP was the only place the user was storing his messages, it would no longer be providing storage for purposes of backup protection.[109] Since the distinction between backup and non-backup could not be made by prior access, the court introduced the idea that messages had lifespans.[110] The lifespan of a backup was tied to the life of the underlying message.[111] Once that message expired, the copy could no longer be considered for backup purposes.[112] It is important to note that the court never explained what the "lifespan" or "normal course" might be.

Other courts and scholars have been very critical of this result.[113] Professor Orin Kerr believes the Ninth Circuit's approach "is quite implausible and hard to square with the statutory text."[114] He argues that the subsection (B) backup protection provision exists as an attempt to provide a backstop to subsection (A).[115] Service providers make copies of messages for administrative purposes. Since these copies are not the actual communication, they may not qualify for protection under subsection (A). The provision for backup protection keeps these copies from being released.[116] Further, he criticizes the court for its lifespan distinction. The 180 days limit in § 2703 "contemplates that e-mails can be in 'electronic storage' for a long, long time."[117]

B. Quon v. Arch Wireless

While the court in *Theofel*, determined that "backup protection" should be interpreted expansively, it left room for future courts to work out how long something could be in storage before it was no

108 *Id.* at 1075.
109 *Id.* at 1076.
110 *Id.*
111 *Id.*
112 *Id.*
113 *See infra* Parts II.C.–D.
114 Kerr, *supra* note 39, at 1217.
115 *Id.* at 1217 n.61.
116 *Id.* Kerr further develops this idea, arguing that "the most obvious statutory signal is the text of 18 U.S.C. § 2704, entitled 'Backup Preservation.' 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." *Id.* (citation omitted).
117 *Id.* at 1218 n.61 (citation omitted).

longer held by an RCS. However, it did seem to make clear that if the server is the *only* place the message is stored, it is no longer acting as an ECS.[118] Five years later, in *Quon v. Arch Wireless Operating Co.*,[119] the Ninth Circuit had occasion to revisit the holding. Rather than give more guidance on the "lifespan" of communication, the court more fully committed to the idea that a service storing post transmission communication would continue to be considered an ECS indefinitely.[120] In doing so, it explored the second issue, determining that the provider should be classified as a whole, rather than classifying individual services provided.[121]

The City of Ontario contracted with Arch Wireless to provide text-messaging services and devices to City employees.[122] In the course of transmission, the messages were stored on Arch Wireless's servers and a copy was made for an archive.[123] The City began to worry that the devices were being used for non-work related purposes.[124] The City requested transcripts of the text messages from certain pagers, including Quon's, and Arch Wireless complied.[125] The City's review of these messages, many of which were sexually explicit, led to an internal affairs investigation into Quon's behavior.[126] The disclosure and subsequent review of the text messages led to this suit for, among others, violations of the SCA.[127]

The district court granted summary judgment against Quon. Since the messages were already transmitted, the court found that

---

118 Theofel v. Farey-Jones, 359 F.3d 1066, 1077 (9th Cir. 2004).

119 529 F.3d 892 (9th Cir. 2008), *rev'd on other grounds*, 130 S. Ct. 2619 (2010).

120 *Id.* at 902–03.

121 *Id.*

122 *Id.* at 895.

123 *Id.* at 895–96. The court thoroughly described the path the messages take:

> The message leaves the originating pager via a radio frequency transmission. The transmission is received by any one of many receiving stations, which are owned by Arch Wireless. Depending on the location of the receiving station, the message is then entered into the Arch Wireless computer network either by wire transmission or via satellite by another radio frequency transmission. Once in the Arch Wireless computer network, the message is sent to the Arch Wireless computer server. Once in the server, a copy of the message is archived. The message is also stored in the server system, for a period of up to 72 hours, until the recipient pager is ready to receive the delivery of the text message.

Id.

124 *Id.* at 897–98.

125 *Id.* at 898.

126 *Id.*

127 *Id.*

Arch Wireless was acting as an RCS.[128] Since the City was the "subscriber," there was no violation of the SCA by disclosing messages at the City's request.[129] The Ninth Circuit disagreed and overturned the district court judgment, holding that Arch Wireless was an ECS.[130]

It was undisputed that the City was a subscriber to the service.[131] The question, then, turned on whether Arch Wireless was an ECS or an RCS.[132] The court looked at the "nature of the services" offered in order to classify Arch Wireless.[133] At its core, Arch Wireless offered a service that allowed users to send and receive messages electronically. That "more appropriately" fit the definition of an ECS.[134] It was no problem that Arch Wireless *also* archived the messages indefinitely. According to the court, Congress was clear on what was meant by "'storage and processing'" for purposes of an RCS.[135] Storage was seen as a "virtual filing cabinet," and processing referred to "'sophisticated data processing services.'"[136] Thus, the court followed *Theofel* in determining that Arch Wireless was a "conduit for the transmission" and stored the messages as backup protection "'for the user,'" and so was a provider of ECS.[137]

In taking this approach, the court seemed to be taking a step further than *Theofel* in classifying the provider as a whole, as opposed to classifying the service being provided at any given moment.[138] The court did not look at each individual service provided and then designate each service separately. Rather, the court seemed to look at the various services provided and then determine whether in sum they pointed toward a designation of ECS or RCS. So, since electronic messaging was the main reason for the agreement, the provider was considered an ECS. The other services provided, such as archiving, were merely supplemental. Despite the fact that an archive of text messages could easily be considered a virtual filing cabinet, the desig-

128 *Id.*

129 *Id.*

130 *Id.* at 903.

131 *Id.* at 900.

132 If an RCS, there was no violation since the City was a subscriber. However, if an ECS, then there was a violation since the City was not a transmitter or receiver. *See supra* Part I.C.1.

133 *Quon*, 529 F.3d at 900.

134 *Id.*

135 *Id.* at 902 (citation omitted).

136 *Id.* (citation omitted).

137 *Id.* (citation omitted).

138 The court points in this direction from the start when it says, "[t]he nature of the services Arch Wireless offered to the City determines whether Arch Wireless is an ECS or an RCS." *Id.* at 900.

nation of Arch Wireless did not change because that "[wa]s not the function Arch Wireless contracted to provide here."[139] Further, it quickly dismissed comments in *Theofel* that permanent storage would point toward the service changing from an ECS to an RCS.[140] Despite the indefiniteness of the archives, there was no indication that Arch Wireless kept the messages permanently.[141] The implication seems to be that a provider can keep copies of messages after transmission in storage indefinitely and still be considered an ECS so long as it is never specified that the storage will be permanent.

C. Flagg v. City of Detroit

In resolving the issue of stored text messages in the case of Tamara Greene,[142] the court in *Flagg v. City of Detroit*[143] took a very different route than the Ninth Circuit, holding that the stored messages were discoverable. The court in *Flagg* was faced with a very similar service as the court in *Quon*—stored text messages. The court ultimately concluded the messages were discoverable and that the service was most likely acting as an RCS once the stored messages had been received.[144] However, while the court was sure of its result, it never seemed confident in its reasoning, and so it took five different analytical routes to reach its result.[145] Further, rather than responding to the actual request, the court analyzed the situation as if the plaintiff had proceeded differently,[146] and then instructed him to resubmit the request.[147]

The City of Detroit had contracted with SkyTel to provide text messaging devices and services to City employees. The contract was discontinued in 2004, but SkyTel retained copies of the communication.[148] The plaintiff sought all texts sent and received by thirty-four individuals over five years, and texts by all city officials sent during the four-hour time period surrounding the plaintiff's mother's death.[149] The defendants argued that SkyTel could not divulge the messages due to the Stored Communications Act. The Act only allowed for dis-

139 *Id.* at 902.
140 *See id.* at 902–03.
141 *Id.*
142 *See supra* INTRODUCTION.
143 252 F.R.D. 346 (E.D. Mich. 2008).
144 *Id.* at 362–63.
145 *See id.* at 348–50, 352, 358.
146 *Id.* at 358.
147 *Id.* at 366.
148 *Id.* at 347–48.
149 *Id.* at 348.

closure of messages with the consent of the subscriber. The City said that since it was the subscriber, SkyTel could only release the messages with its consent, which it refused to give.[150]

The court started with a discussion of procedure. The plaintiff had requested the messages by sending a third-party subpoena to SkyTel.[151] However, the court thought that the SCA could apply differently to third party subpoenas versus requests directly to the subscriber through a Rule 34 document request.[152] Since the former route would lead to a much more complicated inquiry,[153] the court decided to ignore the actual request and "proceed[ ] under the premise" that the plaintiff had used a Rule 34 request.[154] Rule 34 requires a party to produce any requested documents under the responding party's control.[155] The court explained that "control" included any documents the party had the right to obtain, not just those in its physical possession.[156] Therefore, if the City had the right to obtain the messages from SkyTel, it had to provide them through a Rule 34 request.[157]

The court then proceeded to interpret the SCA in five different ways, all with the result that the City had to provide the messages. First, the court posited that the SCA applied differently to requests from the subscriber than to requests from a third party.[158] The SCA prohibits both ECS and RCS providers from "divulg[ing]" the content of electronic communication.[159] Providing content to an outside party would clearly be "divulging," and therefore a violation.[160] How-

150 *Id.* at 354–55.

151 *Id.* at 352.

152 *Id.* at 358.

153 This is ironic seeing as the route the court eventually took was premised on a fiction that ultimately resulted in an in-depth and complicated analysis under five different routes.

154 *Id.* at 358.

155 *See* FED. R. CIV. P. 34(a)(1) ("A party may serve on any other party a request within the scope of Rule 26(b) . . . to produce and permit the requesting party or its representative to inspect, copy, test, or sample . . . items in the responding party's possession, custody, or control . . . .").

156 *Flagg*, 252 F.R.D. at 353.

157 *Id.* at 355.

158 *Id.* at 358.

159 *See* 18 U.S.C. § 2702(a)(1) (2006) ("[A] person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service . . . .").

160 *Id.*

ever, by the plain meaning of the word "divulge,"[161] one could hardly argue that providing the contents to the subscriber who asked for the contents to be saved is "divulging" content in violation of the act.[162]

Second, the court posited that the SCA would not even apply if SkyTel was an RCS.[163] An RCS is prohibited from divulging content only if the service provider is not "'authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.'"[164] If the contract provided a mechanism for the City to request retrieval of the messages from SkyTel, that would be the needed "authorization to access" that would take SkyTel's services outside the restrictions of the SCA.[165] Therefore, under this theory, the SCA did not apply, and SkyTel could divulge the messages.[166] The court was most surely wrong in this argument. As the court even points out in the next justification, storage would be of little use without a mechanism to retrieve the messages. Therefore, it is highly unlikely that retrieval would take SkyTel's storage services outside the scope of the Act.

Third, the court posited that if its analysis in the second justification was wrong and the activity did fall within § 2702(a), there might be another applicable exception besides lawful consent of the subscriber.[167] The SCA allows for disclosure if it would be "'necessarily incident to the rendition of the service.'"[168] An archive of text messages would be of little use without a mechanism for retrieving them.[169] Therefore, retrieval for the City would be "necessarily inci-

161 The court cites the definition of divulge in Webster's Dictionary as: "'mak[ing] known' or revealing something which is 'private or secret.'" *Flagg*, 252 F.R.D. at 358 (quoting WEBSTER'S NINTH NEW COLLEGIATE DICTIONARY 370 (9th ed. 1986)).

162 *Id.* at 358 ("By fulfilling a request from its customer, the City, to retrieve and forward communications from an archive that has been created and maintained at the customer's request, SkyTel cannot necessarily be characterized as having 'divulged' any information to anyone outside the scope of the confidential relationship . . . .").

163 *Id.* ("If the archive and retrieval service provided by SkyTel qualifies as an RCS, it is still more doubtful that this sort of retrieval would run afoul of § 2702(a).").

164 *Id.* at 359 ("[T]o the extent that the contracts between the City and SkyTel provide a mechanism for the City to request the retrieval of text messages from the archive maintained by SkyTel, such a request presumably would supply the necessary 'authoriz[ation]' . . . ." (quoting18 U.S.C. § 2702(a)(2))).

165 *Id.* at 359.

166 *Id.*

167 *Id.*

168 *Id.* (quoting 18 U.S.C. § 2702(b)(5)).

169 *Id.*

dent to" the storage. So, consent of the City may not have even been needed.[170]

Fourth, in the most important and likely most accurate reading of the SCA, the City had the "lawful consent" needed to get the messages since SkyTel was acting as an RCS, and the City was the subscriber.[171] Since this result was at odds with *Quon*, the court began by criticizing the Ninth Circuit's analysis and conflicting holding. According to the court, *Quon* took an "'all or nothing' approach"[172] whereby it "broadly" categorized Arch Wireless as "providing a service for sending and receiving messages," not as computer storage.[173] Therefore, messages were stored for backup protection.[174] The Ninth Circuit relied on a "unitary approach" where a contract was to provide one or the other, but not both.[175] However, the court here claimed that § 2702(a) focused on specific types of services with regard to a specific piece of information, not the provider as a whole.[176] The inquiry was to what the service was presently doing with the piece of communication. While SkyTel had acted as an ECS while transmitting the messages, at the time of the suit it was holding the messages in an archive as a "virtual filing cabinet," and therefore holding them in computer storage.[177] Even though SkyTel was an RCS, the City was still able to give its consent as a subscriber and was obliged to do so under Rule 34.[178]

Finally, still not satisfied that it had covered all of its bases, "even if the [c]ourt is mistaken[,]"[179] the court analyzed the situation as if SkyTel was acting not as an RCS but as an ECS as under the *Quon* framework.[180] In this situation, SkyTel could have only released the messages with consent of the user.[181] Since the users were all City

170 *Id.*

171 *Id.* at 359–63.

172 *Id.* at 360.

173 *Id.* at 361.

174 *Id.* at 361–62.

175 *Id.* at 362.

176 *Id.*

177 *Id.* at 363 ("[T]he service provided by SkyTel may properly be characterized as a 'virtual filing cabinet' of communications sent and received by City employees." (citation omitted)).

178 *Id.*

179 *Id.*

180 *Id.* at 363–64.

181 *Id.* at 359 (citing 18 U.S.C. § 2702(b)(3) (2006)) ("If this service is deemed to be an RCS, then the consent of the 'subscriber' is sufficient to permit the service provider to divulge the contents of a communication maintained on this service.").

employees, the City could have forced their consent.[182] The employees were clearly told that their communication could be monitored, and they acceded to a policy allowing access.[183]

After finally concluding that, at least in some way or another, the City could retrieve the messages and could be compelled to do so by a Rule 34 request, "[t]he court [found] it best to avoid [the third-party subpoena] question, and to instead insist that [p]laintiff reformulate his third-party subpoena as a Rule 34 request for production directed at the [d]efendant City."[184]

D. Crispin v. Christian Audigier

In *Crispin v. Christian Audigier, Inc.*,[185] a district court case in the Ninth Circuit, the court was forced to apply the SCA to newer forms of electronic communication, illustrating the additional complications that arise. Crispin, an artist, had licensed the defendants to print his artwork on clothing for a fee and required them to include his logo.[186] This suit arose out of claims that the defendants breached the contract by sublicensing the art and not properly attributing it to Crispin.[187] In the course of the litigation, the defendants subpoenaed three third-parties for basic subscriber information and all communication related to the defendants—Media Temple (webmail), Facebook, and MySpace (social networking).[188] Crispin moved to quash the subpoenas on the grounds that, among others, they violated the SCA.[189]

The court realized that it must classify these services as either providers of ECS, RCS, or neither. The court sought to show how both *Quon* and *Flagg* were reconcilable and merely applied the same rule to different factual scenarios[190]—something the court in *Flagg*

182 *Id.* at 364 (citing Riddell Sports Inc. v. Brooks, 158 F.R.D. 555, 559 (S.D.N.Y. 1994)).

183 *Id.* at 364–65. This is especially true for one of the primary challengers, Mayor Kilpatrick, who put the policy in place. *Id.*

184 *Id.* at 366; *see also* Timothy G. Ackerman, *Consent and Discovery Under the Stored Communications Act*, THE FED. LAW., Nov./Dec. 2009, at 42, 44–45 (explaining the role *Flagg* plays in electronic discovery disputes).

185 717 F. Supp. 2d 965 (C.D. Cal. 2010).

186 *Id.* at 968.

187 *Id.*

188 *Id.*

189 *Id.* at 969.

190 *Id.* at 987 ("For this reason, *Weaver* and *Flagg* do not conflict with Ninth Circuit precedent; indeed, they apply the rule set forth . . . to different factual circumstances."). This is ironic, seeing as the two providers provided the exact same service. *See supra* Part II.B–C.

did not think could be done. The court dismissed the Ninth Circuit's application of ECS to both pre- and post-reception communication in *Theofel* and *Quon* by saying the court there was referring to a specific type of communication, not ECS providers generally.[191] Unlike the courts in *Theofel* and *Quon*, the court looked to the particular service provided, not the provider as a whole. Since the provider in *Flagg* no longer provided messaging services, it fell into *Theofel*'s RCS category because it was the only place the messages were stored, ignoring the fact that *Flagg* clearly had rejected *Theofel*'s contention that a received message could be held by an ECS. Therefore, the court concluded that all of the cases just "apply the rule set forth in *Theofel* to different factual circumstances"[192]—that is, if the opened messages were only stored on the providers servers, it could have been considered an ECS.

After interpreting Ninth Circuit precedent in a way that allowed for contrary results, the court looked at the service provided. Media Temple provided "webmail" services. Webmail is analogous to the electronic messaging contemplated in the committee reports. However, unlike email at that time, where messages were retrieved and downloaded, here the messages remained on the provider's server where a user would go to view the message.[193] The services defaulted to storing the messages only on the provider's server. The court found that the provider was clearly acting as an ECS while the messages were stored but had not been read.[194] However, once the user viewed the message, unless he downloaded it to his computer, the provider acted as an RCS because the provider was the only place the message was stored, and it was not there for backup protection.[195]

The court argued that this was in accord with *Theofel* and *Quon*. However, Ninth Circuit precedent in *Theofel* and *Quon* would lead one to think that, at least for webmail, the stored communication would be held by an ECS.[196] Like the providers in both of those cases, Media Temple provided, at its core, a service to send and receive messages.[197] Prior to viewing the messages, the communications would clearly have fallen under section (A) as temporary intermediate storage. As construed in *Theofel* and *Quon*, section (B) backup protection would certainly apply after the communication was viewed. Like in *Theofel* and *Quon*, the messages were left there so that the user

191 *Crispin*, 717 F. Supp. 2d at 987.
192 *Id.*
193 *Id.* at 985.
194 *Id.* at 987.
195 *Id.*
196 *See supra* Part II.A–B.
197 *Crispin*, 717 F. Supp. 2d at 987.

could have viewed them again if he or she needed to do so. Further, like in *Quon*, since it was not clear that messages were left permanently, the dicta in *Theofel* did not apply.[198]

While the result the court came to with regard to webmail is certainly in agreement with *Flagg*, it seems to be inconsistent with the analysis in the questions arising about Facebook and MySpace posts. Facebook and MySpace posts present a unique problem since they are posted with the idea that multiple people will see the post. In its analysis, the court analogized to electronic bulletin board systems (BBS).[199] The electronic bulletin board systems were directly contemplated in the committee reports and were meant to be covered by the SCA.[200] These systems work by disseminating messages to multiple subscribers. A user sends a message to the system, then anyone else who subscribes to the message board can view the message.[201] Provided that there are some restrictions to the general public, electronic bulletin board messages are protected under the SCA.[202] However, it was not clear whether a BBS is an ECS or RCS. The court noticed that multiple other courts had faced the same question and disagreed on whether it was an RCS or an ECS, but they hardly provided any explanation for their choice—leaving little guidance.[203] One such case was a Ninth Circuit opinion concluding that a BBS was an ECS, but the court did not explain why.[204] The court concluded that since the BBS was the final destination of these messages, they could hardly be considered held for temporary, intermediate storage under section (A). So, following the earlier case, the court held that messages on a BBS must be stored for backup protection, even after being viewed.[205] The court explained that this was consistent with *Theofel* and *Quon* because "a user's . . . *passive* decision not to delete a communication after it has been read by the user renders that communication stored for backup purposes . . . ."[206] While this does seem to comport with the

198 *See supra* Part II.A–B.

199 *Crispin*, 717 F. Supp. 2d at 988.

200 *See* S. REP. NO. 99-541, at 8–9 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3562.

201 *Crispin*, 717 F. Supp. 2d at 980 ("The latter is essentially email directed to the community at large, rather than a private recipient." (quoting MTV Networks v. Curry, 867 F.Supp. 202, 204 n.3 (S.D.N.Y.1994))).

202 *Id.* at 981.

203 *Id.* at 988. *Compare* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 879 (9th Cir. 2002) (finding a BBS was an ECS provider), *with* Steve Jackson Games, Inc. v. U.S. Secret Serv., 816 F. Supp. 432, 443 (W.D. Tex. 1993) (finding a BBS was an RCS provider).

204 *See Konop*, 302 F.3d at 879.

205 *Crispin*, 717 F. Supp. 2d at 989.

206 *Id.* (emphasis added).

holdings in both *Theofel* and *Quon*, it seems contrary to the court's earlier interpretation of webmail. The same argument for why viewed messages on a BBS are stored by an ECS could apply to webmail, as webmail users typically "passively" decide not to delete messages after they are viewed.

The court held that Facebook and Myspace effectively work as private BBS. Each user has a page, or a "wall," in which people can post messages. Anyone who is a "friend" of that person may see the posts.[207] Because they are analogous to BBS, the court concluded that Facebook and Myspace were ECS providers, and wall postings were in electronic storage.[208]

The court alternatively held that the messages were protected because the servicers were RCS providers.[209] The court analogized to a case involving YouTube, a video sharing and storage service on the Internet.[210] The court held that YouTube acts as an RCS since its primary role is to store videos that people may access. So long as the users placed restrictions on who could view the videos, they would be protected under the SCA.[211] Under this theory, the court concluded that Facebook and MySpace act as RCS providers because they store others' messages. It is no problem that people can retrieve the messages, because like in *Flagg*, an RCS must have a retrieval mechanism.[212]

III. TECHNOLOGICAL ADVANCES INCREASE CONFUSION

As the above cases have shown, courts have had a very difficult time applying the SCA's categories to service providers. This has created a situation in which courts could find ways to make either category apply. The task of distinguishing has become more difficult with advances in technology. As shown in this section, as Internet sites begin to do more and more tasks, the line between storage and communication is further blurred. By analyzing Dropbox, social networking sites, and webmail, this Note will show how a court could use the arguments in the cases in the previous section to categorize each of these services as either an ECS or an RCS, depending on the result sought.

---

207 *See infra* Part III.C.

208 *Crispin*, 717 F. Supp. 2d at 988–89. This is true so long as the user places some restrictions on access.

209 *Id.* at 990.

210 *Id.*; *see* Viacom Int'l Inc. v. YouTube Inc., 253 F.R.D. 256 (S.D.N.Y. 2008).

211 *YouTube*, 253 F.R.D. at 264–65.

212 *Crispin*, 717 F. Supp. 2d at 990.

A. Dropbox

Dropbox[213] is a file storage and sharing service on the Internet. A user can save any files from her computer to Dropbox and then access and edit the files from any other computer. The service also allows users to share files with other users. This allows multiple users to share information or work on the same project and store it in one location.[214] Initially, providers like Dropbox would seem to clearly fall within the category of RCS. The user electronically transmits his data to the service to be stored and then accessed at a later time.

However, the analysis is not so clear when the sharing function is considered. The service could easily be seen as transmitting electronic communication, and thus as a provider of ECS.[215] As an example, suppose two professors are working on an article together with the assistance of a research assistant. One professor writes a section of the article, edits another portion, and then uploads it to Dropbox. The next professor opens it, reviews the additions and changes, and then adds her own new material along with some notes for suggested changes to earlier portions. After she saves it, the research assistant opens the file to edit the document and supplement the footnotes. He uploads his revisions for approval from the two professors. They then open the document to review and consider the changes, suggested changes, and edits to determine what they will keep.

The service is essentially still just acting as remote storage. However, due to the shared access and ability to change, the users are all using the service to communicate with each other. The service is essentially transmitting electronic communication to the recipients who can then open it and view it, before sending it off again. With this scenario, then, the service is acting as an ECS. Under the *Flagg* rule,[216] the service would be acting as an ECS until the other user opened and viewed the document. If the user takes no further action, the file saved on the server would then be in storage and Dropbox would go back to acting as an RCS. However, under the *Theofel/Quon* rule, even after viewing the document, the file still stored on Dropbox would be there for backup protection, and thus still covered by ECS rules.[217] Under either test, as soon as the recipient uploads changes for another's review, Dropbox again would be acting as an ECS.

---

213 DROPBOX, http://www.dropbox.com (last visited Aug. 22, 2012).

214 *Features*, DROPBOX, http://www.dropbox.com/features (last visited Aug. 22, 2012).

215 *See supra* Part I.B.

216 *See supra* Part II.C.

217 *See supra* Part II.A–B.

B. Webmail

As described above, e-mail at the time of the enactment of the SCA involved sending a message to the provider who would store it until the recipient could download the message to his or her own computer.[218] Even as e-mail became automatic, it still usually involved downloading the message to the user's computer through an e-mail client such as Microsoft Outlook or Apple Mail. Now, however, many use webmail as their primary account through services such as Microsoft's Hotmail, Gmail, and Yahoo! Mail. A user never needs to download the message to one's own computer.[219] Rather, the user logs into his account on the provider's site and views his messages there. Once the message is sent to the recipient, it stays in the same location, unless the user voluntarily deletes it. This allows users to view their messages from any location with an Internet connection.[220]

The courts have consistently treated webmail services as providers of ECS, at least until the message is read.[221] This makes sense because webmail provides basically the same function as older forms of e-mail and electronic communication. Simply, webmail, like all e-mail, is sending messages from one to another. The main controversy remains in differing approaches to categorizing messages after they have been viewed. However, it is not so clear that webmail providers could not be understood as providers of RCS the entire time. When a person sends a message to a webmail account, the message is essentially uploaded to the provider's server where it is stored. The "recipient," by going to his account to view the message can really just be seen as viewing something in electronic storage. The location of the message does not change post viewing—the online inbox is the final location.[222] It is not downloaded or changed—it just remains in the same place. In this sense, it is very similar to Dropbox—a person's webmail account is merely a place where information is stored that only he may access. Webmail, then, could be seen as a provider of

218 *See supra* Part I.A.

219 *See* United States v. Weaver, 636 F. Supp. 2d 769, 772 (C.D. Ill. 2009).

220 *See id.*

221 *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 987 (C.D. Cal. 2010).

222 *See Weaver*, 636 F. Supp. 2d at 772; *see also* Snow v. DIRECTTV, Inc., No. 2:04-CV-515FTM33SPC., 2005 WL 1226158, at *3 (M.D. Fla. May 9, 2005) *report and recommendation adopted*, Snow v. Directv, Inc., 2:04CV515FTM-33SPC, 2005 WL 1266435 (M.D. Fla. May 27, 2005) *aff'd*, Snow v. DirecTV, Inc., 450 F.3d 1314 (11th Cir. 2006) ("Rather[,] his website is the final destination for the information posted . . . .").

RCS, a provider of remote storage with very specific restrictions on who can gain access to any given piece of stored content.[223]

C. Facebook

A third type of modern electronic communication provider is the social networking site. These sites allow people to reconnect, network, and communicate with people on the Internet. The most popular social networking site[224] is Facebook.[225] Users create profiles on which they put personal information such as birthdate, relationship status, interests, activities, favorite books, etc.[226] Depending on their privacy settings, only "friends," or people they approve, can see that information. As part of each user's profile there is a "wall," an electronic message board, on which the user or the user's friends can post comments, videos, articles, and pictures. Access to posts may be restricted to all friends or specific friends.[227] Facebook also contains a message service operating similar to webmail. A user can send a private message to one or more friends, which will only show up in the recipient's message box.[228] Finally, users may join "groups," or topic-specific message boards, that allow users to share with specific people.[229]

The message function of Facebook is analogous to webmail, as it facilitates the sending and receiving of messages that are stored in the online mailbox. Therefore, the same results would occur as in the webmail analysis above. The more complicated question arises with the wall posts. *Crispin* analogized the wall posts to electronic message boards, as they serve similar functions.[230] As *Crispin* realized, though,

223 An interesting point has been raised by scholars over the effects of the SCA on cloud computing. Since many of these services use the data stored by users to tailor advertisements to the user, providers are authorized to use the contents, taking it outside the scope of the restrictions on disclosure by RCS providers. *See* William Jeremy Robison, Note, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1212–23 (2010).

224 *See* Andy Kazeniac, *Social Networks: Facebook Takes Over the Top Spot, Twitter Climbs*, COMPETE PULSE (Feb. 9, 2009, 2:01 PM), http://blog.compete.com/2009/02/09/ facebook-myspace-twitter-social-network/.

225 FACEBOOK, http://www.facebook.com (last visited Oc. 12, 2012).

226 *Facebook Glossary*, FACEBOOK, http://www.facebook.com/help/glossary (last visited Oct. 12, 2012).

227 *Basic Privacy Controls*, FACEBOOK, http://www.facebook.com/help/privacy/basic-controls (last visited Oct. 12, 2012).

228 *Facebook Glossary*, FACEBOOK, http://www.facebook.com/help/glossary (last visited Oct. 12, 2012).

229 *Id.*

230 *See supra* Part II.D.

it is not easy to categorize wall posts. First, they can be categorized as ECS providers. A wall post, like a message board post, is electronic communication from one person to another, or many. So long as there are some privacy restrictions, they are not public communications. Second, they can be categorized as RCS providers. While *Crispin* held this as an alternative argument, it is probably more persuasive. Like videos stored on YouTube and information stored on Dropbox, by posting messages, pictures, and articles, people are storing that information on Facebook. While many can access it, the user can restrict access as much as he or she wants. And, as is frequently stated, an RCS must have some way for users to retrieve the information.

IV. PROPOSED SOLUTIONS

A. A Legislative Response

After repeated criticism and calls for amendment,[231] a proposal has been introduced in Congress. Senator Patrick Leahy, the author of the original ECPA and SCA, introduced the Electronic Communications Privacy Act Amendments Act of 2011 on May 17, 2011.[232] Senator Leahy said he introduced the bill because:

> [T]oday, [the ECPA] is significantly outdated and out-paced by rapid changes in technology and the changing mission of our law enforcement agencies after September 11. . . . With the explosion of new technologies, including social networking sites, smartphones and other mobile applications, there are many new benefits to consumers. But, there are also many new risks to their privacy.[233]

The bill is meant to close many of the loopholes and inconsistencies that have arisen from the original act,[234] provide new protections for location information, and provide new tools to enhance cyber

231 A group of large electronics companies such as Adobe, AOL, and Google formed an advocacy group seeking change of the law. *See* DIGITAL DUE PROCESS, http://www.digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163 (last visited Oct. 12, 2012).

232 *See* Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong. (2011), *available at* http://www.leahy.senate.gov/imo/media/doc/BillText-ElectronicCommunicationsPrivacyActAmendmentsAct.pdf.

233 Senator Patrick Leahy, Chairman, Senate Committee on the Judiciary, On Introduction of The "Electronic Communications Privacy Act Amendments Act of 2011" (May 17, 2011), *available at* http://www.leahy.senate.gov/press/leahy-introduces-benchmark-bill-to-update-key-digital-privacy-law.

234 Senator Leahy stated that "[u]nder the current law, a single e-mail could be subject to as many as four different levels of privacy protections, depending upon where it is stored and when it was sent." *Id.*

security and national security. While the proposed Act does solve many of the enforcement discrepancies, it still leaves unaddressed some of the inconsistencies that have been brought to light.

The first part of the bill amends a small part of § 2702 voluntary disclosure. It expands the 2702(a)(3) prohibition on knowingly divulging records to the government[235] in two ways. First, it keeps the electronic communication service and remote computing service distinction, but adds a third category: geolocation information service. Second, it increases the scope of the clause to include records *and* any contents listed in § 2703(a).[236]

The amendments that most affect the discussion in this Note are those to § 2703 on compelled disclosure.[237] The proposed amendments remove the 180 day rule that places different standards for disclosure of electronic communication from an ECS.[238] Further, it combines what had been § 2703(a) pre-180 ECS communications and § 2703(b) post-180 ECS communication and RCS communication.[239] This raises the legal standard for attaining content stored or processed by an RCS to the same level of ECS content. Now, all content would require a federal or state warrant. The government must provide notice to the subscriber or customer within three days of receiving the contents. However, like in the current Act, notice could be delayed for up to ninety days if a judge determines it would hurt the trial or investigation, or would endanger national security.[240]

The amendments change very little for non-content information such as records. The government may compel disclosure of records from both ECS and RCS providers through a warrant, court order, or consent. For identification information, a subpoena will suffice.[241] No notice would be required for non-content records. The rest of the amendments deal with requirements for attaining geolocation service information and cyber security.[242]

The amendments take a very positive step forward by removing the 180 day rule for ECS communication—a distinction that no longer makes sense. Further, by bringing disclosure by RCS providers up to the same level as ECS providers, the amendments remove one of the most inconsistent parts of the present law. While it does not

235 *See supra* Part I.C.
236 S. 1011 § 2.
237 *See supra* Part I.C.
238 S. 1011 § 3(a)(1).
239 *Id.*
240 *Id.* § 4.
241 *Id.* § 3(a)(1).
242 *Id.* § 5–8.

remove the underlying ECS/RCS distinction, it removes one of the ways that distinction plays out. Now, the government will need to apply to the same standard whether the provider is classified as an ECS or an RCS—making the distinction much less important.

While the amendments move in a positive direction by removing one inconsistency, the bill falls far short by leaving the underlying ECS/RCS distinction in place. Most of the cases discussed above, and most of the circumstances in which this issue is actually litigated, involve discovery in civil suits where the classification makes a big difference in determining who must give permission for disclosure. Courts will still be forced to struggle through the same arguments made above in determining how to proceed with electronic discovery.

B. A Modern Approach

In order to truly remove confusion and conform the SCA to modern technology, Congress must remove the ECS/RCS distinction by combining the categories under one disclosure standard. The Act should be amended by creating one category called "Electronic Computing Service." This designation would apply to any service which provides the users thereof the ability to send or receive, store, or process electronic information.[243] The Act should protect any information held as part of the service provided or held incidental to the service provided.[244] This new definition would include services as distinct as Webmail and Dropbox, and would cover all information stored by these services.

The current prohibition on voluntary disclosure of content information and the relevant exceptions[245] should remain in place. Exception 3, however, should be changed to reflect the new Electronic Computing Service definition. The SCA presently allows for disclosure with the lawful consent of senders or receivers for ECS providers, and for disclosure with the lawful consent of senders, receivers, or *subscribers* for RCS providers.[246] With the combined category, it should only allow for disclosure with the consent of the senders and receivers, but not the subscribers. Therefore, in the case of a civil dispute, a

243 This definition combines the definitions of ECS and RCS found at 18 U.S.C. §§ 2510(15) & 2711(2) (2006), respectively.

244 This replaces the categories in 18 U.S.C. §§ 2510 (17)(A)–(B), and removes the confusion that arises in distinguishing between storage incidental to the transmission and storage for backup purposes and can include long term storage. *See supra* Part II.A–B (explaining the difficulty that courts have had with the inclusiveness of these sections).

245 *See supra* Part I.C.1.

246 *See* 18 U.S.C. § 2702(b).

party could not retrieve content pursuant to a third party subpoena to the provider, but would instead need to compel the consent of the sender or receiver.[247]

Finally, like in Senator Leahy's proposed amendments, Congress should do away with the 180 days requirement for compelled disclosure of electronic communication. Under the SCA's compelled disclosure prohibitions, the government is only required to produce a warrant if the communication is in electronic storage by an ECS for less than 180 days. If it has been in storage for more than 180 days, or is held by an RCS, the government need only produce a 2703(d) order and provide consent.[248] With the combined definition here, Congress should amend the compelled disclosure requirements to require that the government provide a warrant to obtain any content held by an ECS no matter the length of time.

By combining the ECS and RCS categories into one category and changing the rules for voluntary and compelled disclosure to reflect the higher burden, Congress can amend the SCA to account for changes in technology and protect the privacy of those using it. Courts will no longer be faced with the confusion confronted in *Theofel*, *Quon*, *Flagg*, and *Crispin*,[249] nor will they be able to make either of two different categories with competing disclosure standards apply based on the results sought.[250] Webmail, Facebook, and Dropbox all would fall under the ECS category and only one set of disclosure standards would apply.

Conclusion

As this Note has argued, the ECS/RCS distinction in the Stored Communications Act has created categories that do not adequately deal with the controversies that arise. The standards overlap in such a way that the courts have difficulty categorizing various service providers. This has led to a situation in which a court could apply either standard depending on the result it seeks to attain. These difficulties have only been exacerbated by the changes and developments in Internet technology. As a result, calls for changes to the law have come from many quarters. Legislators have responded by introducing a new bill to amend the SCA. While the bill goes far in removing the discrepancies in discovery standards, taking much of the bite out of

247 And not the consent of the subscriber, as was the case in *Flagg*. *See supra* Part II.C.

248 18 U.S.C. § 2703(b); *see also supra* Part I.C.2.

249 *See supra* Part II.

250 *See supra* Part III.

the ECS/RCS distinction, the fundamental distinction still remains and will still play an important role in civil discovery. These problems will only be solved once Congress decides to remove the ECS and RCS categories.