NOTES

COMPULSION OF TEXT MESSAGES AFTER *QUON*: APPLYING OLD LAW TO NEW TECHNOLOGY

Fred Kemper[*]

INTRODUCTION

Congress enacted Title II of the Electronic Communications Privacy Act of 1986 (ECPA), now known as the Stored Communications Act (SCA),[1] five years after the Federal Communications Commission first approved the use of cell phones.[2] In passing the SCA, Congress responded to calls for reform following massive and sudden changes in communications technology.[3] The House committee report accompanying the legislation specifically emphasized these burgeoning tools: "Today, we have large-scale electronic mail operations, cellular and cordless telephones, paging devices, miniaturized

[*] J.D., Boston University School of Law, 2012; B.A., Government, Connecticut College, 2007. I dedicate this Note to my parents and brother for their constant support. I also want to thank Will Bussiere for his expert editing and insightful comments. Any errors are mine.

[1] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, tit. II, 100 Stat. 1848, 1860-68 (codified as amended at 18 U.S.C. §§ 2701-2709, 2711 (2006)).

[2] H.R. REP. NO. 99-647, at 20 (1986).

[3] *Id.* at 17-19.

transmitters for radio surveillance, and a dazzling array of digitized information networks which were little more than concepts two decades ago."[4]

Now, twenty-six years after Congress enacted the SCA, these technologies are commonplace, or even obsolete in some cases; cell phone ownership has ballooned in the past two decades, and paging has been all but replaced by text messaging.[5] Even so, the 1986 SCA still governs how telecommunications providers may release text messages to third parties or the federal government.[6] The federal government uses the SCA frequently, as evidenced by the 4601 requests for user data received by Google in just six months.[7] As the primary law enforcement agency of the federal government, the Department of Justice (DOJ) often uses the SCA in investigations and prosecutions throughout the country.[8] The DOJ has thus developed a strong understanding of the SCA borne out of its extensive experience with the statute.[9]

Despite the DOJ's understanding and expertise, the United States Court of Appeals for the Ninth Circuit fundamentally disagreed with the DOJ's functional interpretation of the SCA in *Quon v. Arch Wireless Operating Co.*[10] The Ninth Circuit disagreed not only as to how text message technology fits within the statute but also as to how the statute operates in general. On appeal, the Supreme Court reviewed the Fourth Amendment portion of the Ninth Circuit's decision, but it denied certiorari as to the SCA issue.[11] Therefore, the Ninth Circuit's interpretation of the SCA is still good law.

Even before *Quon*, legal scholars, courts, and legislators had tried to untangle the language of the SCA and apply it to controversies, but to no avail.[12] Technological advancements such as the advent of text messaging

---

[4] *Id.* at 18.

[5] *See* Jeff Brown et al., *SMS: The Short Message Service*, COMPUTER, Dec. 2007, at 106, 106. In just five years, from 2006 to 2011, the number of text messages sent per month in the U.S. has increased from 12.5 billion to 196.9 billion. *Wireless Quick Facts*, CTIA, http://ctia.org/advocacy/research/index.cfm/aid/10323 (last visited Feb. 26, 2012).

[6] *See* 18 U.S.C. § 2702.

[7] Julia Angwin, *Secret Orders Target Email*, WALL ST. J., Oct. 9, 2011, http://online.wsj.com/article/SB10001424052970203476804576613284007315072.html.

[8] One DOJ official described the SCA as a "vital tool" in law enforcement and national security. *The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary*, 111th Cong. 58 (2010) [hereinafter *Hearing*] (statement of James A. Baker, Associate Deputy Att'y Gen., United States Department of Justice).

[9] *See infra* Part II.C.

[10] Quon v. Arch Wireless Operating Co., 529 F.3d 892, 903 (9th Cir. 2008), *rev'd on other grounds sub nom.* City of Ontario v. Quon, 130 S. Ct. 2619 (2010).

[11] *Quon*, 130 S. Ct. at 2627.

[12] *See, e.g.*, 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, 1209 (2004).

technology have contributed to confusion and uncertainty about how to properly interpret the statute. The lack of cases explaining the operation of the statute compounds this confusion.[13] Although technology has changed dramatically, Congress's unwillingness or inability to update the statute, combined with concerns about privacy protection and uncertainty, has prompted many groups to vigorously call for reform.[14] Critics specifically target ECPA and the SCA because these laws mandate the procedures for disclosure of content of electronic communications to the government.[15] Until Congress takes action, the government, courts, and industry are all stuck applying this antiquated law to new technologies.

Since *Quon*, commentators have written about the implications of the Ninth Circuit's decision; none, however, have sought to resolve the competing interpretations of the Ninth Circuit and the DOJ.[16] This Note argues that while the Ninth Circuit's interpretation of the SCA is simpler to apply, the DOJ's interpretation better follows the text of the statute while preserving the balance Congress struck between the competing goals of ensuring prosecutorial effectiveness and protecting individual privacy. Further, this Note will show not only that the DOJ interpretation is correct but also that when understood in the context of text messaging technology, the Ninth Circuit's interpretation is unworkable. To accomplish this, Part I provides an overview of text messaging technology. Part II provides an overview of the statutory framework and the DOJ and Ninth Circuit interpretations. Part III, through statutory analysis and an application of current technology, shows the merits of the DOJ's interpretation. Finally, Part IV argues that even if courts disagree with this Note's findings, they should still defer to the DOJ's interpretation under *Skidmore*.

I. TEXT MESSAGING TECHNOLOGY

To determine how text messaging fits into the framework of the SCA, it is necessary to have a basic understanding of how text messaging technology works. Text messaging is accomplished by means of a short message service

[13] *Id.* at 1208.

[14] For example, Digital Due Process is a "coalition" of private industry and non-profit groups hoping "[t]o simplify, clarify, and unify the ECPA standards, providing stronger privacy protections for communications and associated data in response to changes in technology and new services and usage patterns." DIGITAL DUE PROCESS, http://digitalddueprocess.org (last visited Apr. 10, 2012).

[15] Different provisions of ECPA apply depending on what information the government is seeking and when. *See, e.g.*, Kerr, *supra* note 12, at 1231-32. For example, communications in transit are covered by the wiretapping provisions, and non-content information is protected under the pen register provisions. 18 U.S.C. §§ 2518, 3121 (2006).

[16] *See* Drew C. Arena, Quon v. Arch Wireless*: The Issue the Supreme Court Won't Address*, 1006 PLI/PAT 369, 371-72 (2010).

(SMS).[17] When someone sends a text message to another person, the sender's phone routes the message to a short message service center (SMSC) maintained by the cell phone service provider.[18] The SMSC interacts with other SMSCs or other short message entities, storing the message and delivering it "when the recipient is on the network."[19] Because SMS messages typically cannot exceed a certain number of characters, the SMSC may break one long message into several shorter messages.[20] SMSCs typically operate as "store and forward" mechanisms, in which the system will resend the message until it can connect with the end user's device.[21] SMCSs often have a limit on how long they will store a message.[22]

Consider one of the most popular cell phone providers, Verizon Wireless, which uses SMS technology.[23] According to Verizon Wireless, if a message is sent to a phone that is powered off or outside the network area, "the network will store the message for later delivery."[24] Next, "[t]he network will attempt to deliver the message for 5 days (120 hours) from the date of Verizon Wireless' receipt of the message."[25] Verizon deletes any messages not delivered within the five-day span.[26] After receiving a message, users may keep it for an indefinite period of time, but they cannot receive new incoming messages if the phone's memory is full.[27] Another popular cell phone provider, AT&T, uses SMS technology as well.[28] It stores text messages for an even longer period than Verizon Wireless. When an AT&T phone cannot

[17] For a discussion on the development of SMS technology, see Mark Milian, *Why Text Messages Are Limited to 160 Characters*, L.A. TIMES TECH. BLOG (May 3, 2009, 1:28 PM), http://latimesblogs.latimes.com/technology/2009/05/invented-text-messaging.html.

[18] Brown et al., *supra* note 5, at 108.

[19] *Id.*

[20] *Id.* at 106.

[21] Brown et al., *supra* note 5, at 106; John Lenarcic & Joan Richardson, *Reflections on the Gestation of Polymorphic Innovation: The Exploitation of Emergence in Social Network Development via Text Messaging*, 7 ISSUES IN INFORMING SCI. & INFO. TECH. 89, 91 (2010). SMSCs can also operate as "forward and forget" mechanisms, in which "the system sends the message to the end device without assurance of receipt or an attempt to redeliver in the case of failure." Brown et al., *supra* note 5, at 106. This method, however, is not often used.

[22] Brown et al., *supra* note 5, at 108.

[23] *Text Messaging*, VERIZON WIRELESS, http://support.vzw.com/faqs/TXT%20messaging/faq.html (last visited Apr. 12, 2012).

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *What Are the Different Types of Messaging?*, AT&T WIRELESS, http://att.com/esupport/article.jsp?sid=KB102636 (last visited Apr. 12, 2012).

receive a message, "AT&T will attempt to deliver the message for up to seven days."[29]

A review of the technology shows that sending a message from a user to the intended recipient involves numerous steps in which the message is intermediately stored. Further, while providers operate slightly differently in terms of how long the message is stored, the general SMS operation of most providers is similar. This intermediate storage system has implications for the SCA's classification of providers and therefore for when and how the federal government can compel disclosure of text message communications.

II. CURRENT LAW

A. *The Statutory Framework*

ECPA and the SCA govern the "collection and disclosure of the content of . . . phone calls and emails, as well as content that has been stored remotely."[30] Specifically, § 2703 of the SCA "creates a code of criminal procedure that federal and state law enforcement officers must follow to compel disclosure of stored communications from network service providers."[31] Section 2702 further "regulates voluntary disclosure by network service providers of customer communications and records," and § 2701 "prohibits unlawful access to certain stored communications."[32] Under ECPA, "content[]" for which the government may seek disclosure consists of "any information concerning the substance, purport, or meaning of that communication."[33]

The SCA further classifies an electronic communication provider as either an electronic communication service (ECS) or a remote computing service

---

[29] *Text Message Delivery Confirmation*, AT&T WIRELESS, http://att.com/esupport/article.jsp?sid=52635 (last visited Apr. 12, 2012). T-Mobile, meanwhile, stores text messages in its system for just three days if delivery is ineffective. *Text Messaging (SMS) FAQs*, T-MOBILE, http://support.t-mobile.com/docs/DOC-1713 (last visited Apr. 12, 2012).

[30] *Hearing*, supra note 8, at 58 (2010) (statement of James A. Baker, Associate Deputy Att'y Gen., United States Department of Justice).

[31] COMPUTER CRIME & INTELLECTUAL PROP. SECTION, CRIMINAL DIV., U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 115 (2009), *available at* http://justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf [hereinafter COMPUTER CRIME].

[32] *Id.*

[33] 18 U.S.C. § 2510(8) (2006). Because this Note focuses on compulsion of text message communications, it will deal only with "content" as defined by the statute. See *id.* § 2703(c)(1)-(2) for compulsion of basic subscriber information or records, including name of subscriber, address, etc. There is no controversy over the fact that text messages count as "content" in the statutory scheme, as courts have consistently followed the relevant analysis for content information. *See, e.g.*, Quon v. Arch Wireless Operating Co., 529 F.3d 892, 903 (9th Cir. 2008); COMPUTER CRIME, *supra* note 31, at 123 ("[S]tored emails or voice mails are 'contents,' as are word processing files stored in employee network accounts.").

(RCS). An ECS, as defined throughout ECPA, is "any service which provides to users thereof the ability to send or receive wire or electronic communications."[34] An ECS can hold content in "electronic storage," which is "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[35] Electronic storage can exist, for example, "when a message sits in an e-mail user's mailbox after transmission but before the user has retrieved the message from the mail server."[36] An RCS, meanwhile, is "the provision to the public of computer storage or processing services by means of an electronic communications system."[37]

To be considered "public" under the definition of an RCS, the service must be "available to any member of the general population who complies with the requisite procedures and pays any requisite fees."[38] The DOJ cites Verizon Wireless as a public service provider because "anyone can obtain a Verizon account."[39] Providers that only offer services to "those with a special relationship with the provider do not provide service to the public."[40]

The distinction between an ECS and an RCS is critical in determining the proper method of compulsion of content. If a communication is held in electronic storage by an ECS for 180 days or less, the government can only compel disclosure through a warrant.[41] If the communication is held in storage for more than 180 days, a government entity may compel disclosure from an

[34] 18 U.S.C. § 2510(15).

[35] *Id.* § 2510(17).

[36] United States v. Councilman, 418 F.3d 67, 81 (1st Cir. 2005).

[37] 18 U.S.C. § 2711(2). An "electronic communications system" is defined by ECPA as "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." *Id.* § 2510(14). Electronic communications *systems* and electronic communication *services* should not be confused with each other, despite the ECPA drafters' best efforts to effect such an outcome by placing the two definitions next to each other (albeit alphabetically) in the statute. This Note will always intend for ECS to mean "electronic communication services," thereby avoiding the difficulty of finding a different abbreviation for electronic communications systems.

[38] *See* COMPUTER CRIME, *supra* note 31, at 119.

[39] *Id.* at 120.

[40] *Id.* ("For example, an employer that provides email accounts to its employees will not be an RCS with respect to those employees, because such email accounts are not available to the public." (citing Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1043 (N.D. Ill. 1998))). This Note will only address public service providers because, by definition, they are readily available for public use and therefore have the greatest impact on everyday technology users.

[41] 18 U.S.C. § 2703(a).

ECS through a warrant, subpoena, or a 2703(d) court order.[42] The same broader range of compulsion tools is available to the government if the communication is stored by an RCS, regardless of the time elapsed since initial storage.[43] Since the threshold for getting a 2703(d) court order is lower than what is required for a warrant, it is easier for the government to obtain communications stored by an RCS rather than by an ECS (if stored for 180 days or less).[44]

The SCA also contains numerous exceptions that govern when divulging contents of a communication is lawful.[45] An exception is triggered when a person divulges the contents of a communication to the "intended recipient" or with "consent" of the intended recipient or "to a person employed or authorized . . . to forward such communication to its destination."[46] The SCA also contains exceptions if the divulging of contents is incidental to "rendition of the service," or "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" or in the event of "an emergency involving danger of death or serious physical injury."[47]

B. *The Ninth Circuit's "Static Classification"*

In *Quon v. Arch Wireless Operating Co.*,[48] the Ninth Circuit heard arguments about the Ontario, California, Police Department's viewing of text messages sent and received by Jeff Quon, a police officer.[49] The City of Ontario contracted with wireless text messaging provider Arch Wireless, which supplied "twenty two-way alphanumeric pagers" that were distributed to the city's employees.[50] The court relied upon technical information provided by Arch Wireless's director of information technology, who explained that a

[42] *Id.* § 2703(a)-(b), (d).

[43] *Id.* § 2703(b). For an explanation of how 2703(d) orders operate and their uses, see Kerr, *supra* note 12, at 1219-20. Under a 2703(d) order, the government can compel disclosure pursuant to § 2703(b)-(c) on a showing of "specific and articulable facts . . . that there are reasonable grounds to believe that the contents of a[n] . . . electronic communication . . . are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). The lower threshold for governmental disclosure of permanently stored communications and those not retrieved for more than 180 days is intended to follow the Supreme Court's Fourth Amendment precedents. Kerr, *supra* note 12, at 1234. The time requirement of 180 days may also track the Fourth Amendment's abandonment doctrine. *Id.*

[44] *See* Arena, *supra* note 16, at 371-72.

[45] 18 U.S.C. § 2702(b).

[46] *Id.* § 2702(b)(1), (3)-(4).

[47] *Id.* § 2702(b)(5), (7)-(8).

[48] 529 F.3d 892 (9th Cir. 2008).

[49] *Id.* at 898.

[50] *Id.* at 895.

message is sent using a radio frequency transmission.[51] Arch Wireless enters the message into its network and sends it to a computer server, where the message is archived.[52] The message is stored in the system "for a period of up to 72 hours, until the recipient pager is ready to receive delivery of the text message" by virtue of being turned on and "located in an Arch Wireless service area."[53] Once the pager is ready, the server sends the stored message to the "transmitting station [owned by Arch Wireless] closest to the recipient pager."[54] Finally, the message is delivered to the recipient.[55]

The *Quon* court had to decide whether Arch Wireless violated the SCA in releasing the transcripts of the messages to the city,[56] applying what this Note will call the "static classification" method. In its analysis, the court first determined that Arch Wireless was an ECS because it was a "service which provides to users thereof the ability to send or receive wire or electronic communications," as it provided a service that enabled Quon to send and receive text messages.[57] The court further determined that Arch Wireless was not an RCS because it did not provide "computer storage" or "processing services" to the city.[58] Even though Arch Wireless was "storing" the messages, the court stated that Congress "contemplated this exact function could be performed by an ECS as well."[59] To support its conclusion, the court cited legislative history that stated that an RCS refers to the "processing or storage of data by an off-site third party" and gave examples of storage such as hospitals maintaining off-site data storage for medical files.[60] In essence, the court viewed an RCS as a provider that acts as a "virtual filing cabinet," and since text messaging services do not act as "virtual filing cabinets," the court reasoned that Arch Wireless could not be an RCS.[61]

Finally, the court analogized its decision with the Ninth Circuit case of *Theofel v. Farey-Jones*.[62] The *Theofel* court held that a "provider of e-mail services" was "undisputedly an ECS" because it stored emails on its servers for "backup protection."[63] The court in *Quon* determined that the service provided in *Theofel* was "closely analogous" to Arch Wireless's service even though the provider in *Theofel* stored the communications "as backup for the user," while

[51] *Id.* at 895-96.

[52] *Id.* at 896.

[53] *Id.*

[54] *Id.*

[55] *Id.*

[56] *Id.* at 898.

[57] *Id.* at 901 (quoting 18 U.S.C. § 2510(15) (2006)).

[58] *Id.* (quoting 18 U.S.C. § 2711(2)).

[59] *Id.*

[60] *Id.* at 901-02 (citing S. REP. NO. 99-541, at 10-11 (1986)).

[61] *Id.* at 902.

[62] 359 F.3d 1066 (9th Cir. 2004).

[63] *Quon*, 529 F.3d at 902 (citing *Theofel*, 359 F.3d at 1075).

in *Quon* it was "not clear for whom Arch Wireless archived the text messages" but that the archive was nonetheless clearly for "backup protection."[64] With Arch Wireless classified as an ECS and with no dispute that Arch Wireless knowingly released the transcripts, the court found a violation of the SCA.[65]

C. *The DOJ's "Variable Classification"*

The Ninth Circuit's view on the application of the SCA to text messaging departs from the view of the DOJ and many commentators,[66] who advocate for what this Note will call the "variable classification" method. In its computer crime and evidence guide, the DOJ states that the Ninth Circuit's approach "is contrary to the language of the statute and its legislative history."[67] While the Ninth Circuit held that the text messaging service provider was an ECS and therefore not an RCS, the DOJ asserts that "[t]he definitions of ECS and RCS are independent of each other, and *therefore nothing prevents a service provider from providing both forms of service to a single customer*."[68] Citing the legislative history, the DOJ analogizes text messaging providers to email service providers, stating that an email service provider is an ECS, but an email stored after transmission would be protected as an RCS.[69] Further, the DOJ concludes: "[t]he key to determining whether the provider is an ECS or RCS is to ask what role the provider has played and is playing with respect to the communication in question."[70]

Many courts have followed the variable classification method. For example, the Federal District Court for the Eastern District of Michigan stated in *Flagg v. City of Detroit*[71] that a provider "may be deemed to provide both an ECS and an RCS to the same customer" and that if the text message is archived to serve as backup protection for the user, then it is held in electronic storage by an ECS.[72] If the archived text message functions as "computer storage," then the provider is an RCS.[73] The court further observed that it was "puzzled" by the Ninth Circuit's determination that Arch Wireless did not "retain[] a permanent copy of the text messages or store[] them for the benefit of the City" but that the messages were merely "'archived' on Arch Wireless's

---

[64] *Id.* (internal quotation marks omitted).

[65] *Id.* at 903.

[66] *See, e.g.*, Kerr, *supra* note 12, at 1208-09.

[67] COMPUTER CRIME, *supra* note 31, at 120.

[68] *Id*. (emphasis added).

[69] *Id.* (citing H.R. REP. NO. 99-647, at 65 (1986)).

[70] *Id.*

[71] 252 F.R.D. 346 (E.D. Mich. 2008).

[72] *Id.* at 362 (citing 18 U.S.C. § 2510(17)(B) (2006)).

[73] *Id.* (citing 18 U.S.C. § 2711(2)). The *Flagg* court found that because the provider under scrutiny did not continue to offer text messaging service to its subscriber and the messages archived were the only available record, the message could not have been a backup copy and must have been storage. *Id.* at 363.

server."[74] The *Flagg* court noted that "an 'archive' is commonly understood as a permanent record," and that the district court in *Quon* itself stated that Arch Wireless kept a repository where the text messages were archived for "permanent record-keeping" after they were read.[75] The *Flagg* court continued,

> [O]nce a service provider has successfully delivered a given text message to its intended recipient and the message has been opened and read, it would appear that any retention of a copy of this message in an "archive" could only be intended "for the benefit of" the customer, because this practice would serve no apparent purpose, whether backup or otherwise, for the service provider in its role as ECS.[76]

Therefore, after the text message is read, the provider acts as an RCS.

The Federal District Court for the District of Columbia also adopted the variable classification method in *United States v. Jackson*.[77] In *Jackson*, the court held that the government established probable cause that the text messages in question were relevant to an ongoing criminal investigation.[78] Given that the provider, Verizon Wireless, stated that it would comply with the court order, the court granted the government's 2703(d) order to compel any text message contents that were stored within an RCS.[79] The court stated that the government could only compel those text messages that were "properly" stored within an RCS; therefore, implicitly, the court recognized that the provider could also be storing text messages as an ECS at the same time.[80] *Jackson* and *Flagg* both support the DOJ's view that a provider should be labeled an ECS or an RCS "with respect to the communication in question" and not based upon a broad generalization of what type of service the provider performs.[81]

Numerous commentators also support the variable classification method. For example, Professor Orin Kerr stresses the importance of distinguishing among providers of an ECS, an RCS, or neither.[82] Professor Kerr also indicates, however, that the distinction between these providers is confusing

---

[74] *Id.* at 362 n.29 (quoting Quon v. Arch Wireless Operating Co., 529 F.3d 892, 902-03 (9th Cir. 2008) (internal quotation marks omitted)).

[75] *Id.* (quoting Quon v. Arch Wireless Operating Co., 445 F. Supp. 2d 1116, 1136 (C.D. Cal. 2006), *aff'd*, 529 F.3d 892 (9th Cir. 2008), *rev'd on other grounds sub nom.* City of Ontario v. Quon, 130 S. Ct. 2619 (2010)).

[76] *Id.*

[77] No. 07-0035, 2007 WL 3230140 (D.D.C. Oct. 30, 2007).

[78] *Id.* at *4.

[79] *Id.*

[80] *Id.*

[81] *See* COMPUTER CRIME, *supra* note 31, at 120.

[82] Kerr, *supra* note 12, at 1215-16.

because "most network service providers are multifunctional."[83] Therefore, providers can act as an ECS, an RCS, or neither, depending on the context.[84] It is critical to determine not the "provider's status in the abstract" but rather the "provider's role with respect to a particular copy of a particular communication."[85]

Like the Ninth Circuit, the DOJ claims to derive authority for its interpretation from the legislative history and wording of the statute itself. The Ninth Circuit's static classification method, however, is undermined by a direct reading of the statute and how the statute interacts with text-messaging technology. In support of this proposition, this Note will analyze the original sources and interpretive methods from which the Ninth Circuit and the DOJ claim authority.

III. STATUTORY ANALYSIS OF COMPETING INTERPRETATIONS

Since both the DOJ and the Ninth Circuit claim to rely on the text of the statute and its legislative history, this Part assesses the legislative history, plain text, and legislative purpose of the statute to demonstrate the greater legitimacy of the variable classification method. This Part argues that the static classification method is unworkable when applied to current technology, while the variable classification method fits with current technology and comports with the text and history of the statute.

A. *A Plain Text Reading Supports Variable Classification*

Since the proper applications of RCS and ECS are in dispute, this Note will first look to where the terms are defined. Both ECSs and RCSs hold electronic communications in storage. However, ECSs hold content in "electronic storage," which is only temporary and incidental to transmission or backup protection for the communication.[86] By contrast, RCSs hold "computer storage or processing services" in an "electronic communications system," the definition of which is not exclusive to temporary uses.[87] The key difference between the two is not what is being stored, but the reason for the storage. Nothing in the definitions of the terms bars the idea that a service provider's role could shift depending on the reason for storage.

Section 2702(a) of the SCA sets up the prohibition on releasing electronic communications by providers of RCSs and ECSs.[88] The section merely states that "a person or entity providing" such service shall not divulge the

[83] *Id.* at 1215.

[84] *Id.*

[85] *Id.*

[86] 18 U.S.C. § 2510(17) (2006).

[87] *Id.* § 2711(2).

[88] 18 U.S.C. § 2702(a).

communications unless an exception applies.[89] Subsection (a)(2)(B) states that an RCS cannot divulge a communication held "solely for the purpose of providing storage or computer processing services . . . if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing."[90] Stating that an RCS may be provided "solely for the purpose of providing storage or computer processing services"[91] could lead to competing inferences. In one respect, the statute's reference to communications held for only one purpose may lend credence to the static classification method; stating that an RCS cannot divulge communications held solely for that purpose, meanwhile, implies that RCSs can provide services other than solely storage or computer processing. But to say that RCSs could not provide more than just storage or computer processing would make § 2702(a)(2)(B) mere surplusage.[92]

The variable classification method is also bolstered through the analysis of the dictionary definitions of the terms. A dictionary contemporary to passage of the SCA defines "storage," in terms of computers, as "memory."[93] The definition of "memory," also as relating to computers, is "the capacity of a computer to store information subject to recall."[94] The dictionary's definition of computer storage would seem to have more bearing on the definition of RCS than ECS, because an RCS provides "computer storage."[95] Given modern-day technology, it would be difficult to imagine that a text message in any step of the transmission process would not be retrievable by the service provider.[96] A stored post-transmission message, however, would likely be much easier to access than a message in electronic storage being routed between SMCSs. This functional distinction strengthens the assertion that depending on what stage of transmission a message is in, the type of storage should be classified differently, and therefore so should the provider.

In terms of the plain textual interpretation of the statute, the Ninth Circuit resolved the issue rather cursorily. The *Quon* court held that Arch Wireless was an ECS because it fit within the statutory definition of an ECS and did not provide the type of services that an RCS does.[97] Even though Arch Wireless stored communications on behalf of the customer, the court settled on an ECS categorization because such storage was temporary, incidental to

[89] *Id.*

[90] *Id.* § 2702(a)(2)(B).

[91] *Id.*

[92] *Cf., e.g.*, United States v. Menasche, 348 U.S. 528, 538-39 (1955) ("It is our duty to give effect, if possible, to every clause and word of a statute . . . ." (internal quotation marks omitted)).

[93] THE RANDOM HOUSE DICTIONARY OF THE ENGLISH LANGUAGE 1877 (2d ed. 1987).

[94] *Id.* at 1199.

[95] 18 U.S.C. § 2711(2).

[96] *See supra* Part I.

[97] Quon v. Arch Wireless Operating Co., 529 F.3d 892, 901 (9th Cir. 2008).

communication, or for backup protection.[98] The Ninth Circuit's determination, however, is overly simplistic. A provider can receive the communications to be stored by providing text-messaging services and still be an RCS as to the stored communications themselves. Nothing in the SCA says an ECS cannot also be an electronic communications system, given that an ECS is a service that allows users to send or receive electronic communications, while an electronic communications system is a facility for the transmission of electronic communications.[99] RCSs provide storage or processing by means of an electronic communications system, but that electronic communications system could also be an ECS allowing users to send and receive electronic communications. This means that an ECS can be a conduit for an RCS and that a provider could grant users both types of services. Therefore, in determining whether a communication is held in computer storage or processing by an RCS or in electronic storage by an ECS, we cannot merely decide whether a provider more closely fits the definition of RCS or ECS; a provider can concurrently offer both services and so can act as either type of service to any communication at any given time. Given this conclusion, a textual approach to the SCA strongly supports the use of the variable classification method.

B. *The Legislative History Supports Variable Classification*

In addition to textual support, analysis of the legislative history of the statute, particularly the House and Senate committee reports, favors the variable classification method.

The House committee report discusses cell phone technology, as well as paging devices, but it does not discuss how the different stages of electronic transmission would affect the designation of a service as an ECS or an RCS.[100] This may imply that the designation does not change, but remains static. It is tempting to say that the dog did not bark,[101] but it is more likely that in drafting the bill, Congress did not discuss or raise the issue because the answer seemed obvious. The report does say that people use RCSs "to process and store their

---

[98] *Id.*

[99] *Compare* 18 U.S.C. § 2510(15) (2006) ("'[E]lectronic communication service' means any service which provides to users thereof the ability to send or receive *wire or electronic communications* . . . ." (emphasis added)), *with id.* § 2711(2) ("[T]he term 'remote computing service' means the provision to the public of computer storage or processing services *by means of an electronic communications system* . . . ." (emphasis added)), *and id.* § 2510(14) ("'[E]lectronic communications system' means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of *wire or electronic communications* . . . ." (emphasis added)).

[100] *See* H.R. REP. NO. 99-647, at 20, 23-24 (1986).

[101] *See, e.g.*, Church of Scientology v. IRS, 484 U.S. 9, 17-18 (1987) (describing the "dog that didn't bark" canon, in which a lack of a discussion or mention of a large change in prevailing law may indicate that Congress did not intend a potentially drastic change).

own data."[102] Further, it states that in computer processing, the facilities of an RCS are used in a "time-sharing arrangement" with the subscriber.[103] This may cut both ways, as all providers, such as Verizon Wireless, hold text messages for a certain period of time until they are sent. Such storage resembles a time-sharing arrangement, where the provider agrees with the subscriber to hold the message until it is successfully sent.

In terms that appear to favor the variable classification method, the House report states that the electronic communications kept by an RCS are protected from governmental access only if the communications were given to the RCS "solely for the purpose of providing storage or computer processing services to the subscriber or customer."[104] This language implies that RCSs can provide more than just computer storage or processing services; it suggests that RCSs can receive electronic communications for other purposes, given that only two purposes are protected from governmental intrusion. This is even more apparent in the Senate committee report, which states, "Existing telephone companies and electronic mail companies are providers of electronic communication services. Other services such as remote computing services may also provide electronic communication services."[105] Here, the legislative history supports the variable classification method by contemplating that a provider can act as an ECS or an RCS to different customers or communications at different times.

The Ninth Circuit highlighted two sections of the Senate report to back up the static classification method and its holding that Arch Wireless was not an RCS.[106] First, the court reviewed the "Purpose" section of the Senate report, which states, "With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information."[107] The report then discusses storage of "medical files" and other information in "offsite data banks" where businesses transmit their data for processing.[108] These processing services store copies of the communication as part of their processing, which the report implies is what is meant as being held by an RCS.[109] The court also cited a section of the Senate report that discusses the meaning of RCS, namely the emergence of "remote computer service companies" that provide offsite services to users.[110] Given

[102] H.R. REP. NO. 99-647, at 23 ("A subscriber or customer to a remote computing service transmits records to a third party, a service provider, for the purpose of computer processing.").

[103] *Id.*

[104] *Id.* at 69.

[105] *See* S. REP. NO. 99-541, at 14 (1986).

[106] Quon v. Arch Wireless Operating Co., 529 F.3d 892, 901-02 (9th Cir. 2008).

[107] *Id.* at 901 (quoting S. REP. NO. 99-541, at 3).

[108] *Id.*

[109] *Id.*

[110] *Id.* at 901-02 (quoting S. REP. NO. 99-541, at 10).

the explanation and extensive list of what would be considered an RCS,[111] one could infer that RCSs are services that only resemble those listed. Citing to this specific legislative history, however, is problematic. The "Purpose" section the court drew from does not specifically say anything about the distinction between an ECS and an RCS, but merely discusses emerging technologies.[112] Further, the section on RCS providers does not say that the emerging technologies it is discussing are the only ones whose providers count as RCSs. Therefore, the section may not have direct bearing on whether a provider can be both an ECS and an RCS, as it may simply be giving examples of what could be considered an RCS. In sum, while the Ninth Circuit relies on ambiguous and unreliable legislative history, the DOJ's variable classification method is supported by direct statements in the committee reports and thus represents the correct interpretation.

C. *The Legislative Purpose Favors Variable Classification*

Unlike a textual reading or legislative history analysis, the legislative purpose of the SCA does not conclusively support the variable classification method. Still, the variable classification method better comports with the overall purpose of the statute and reflects the bargain that Congress made in balancing the competing concerns of privacy and the availability of effective prosecutorial tools. The House report sets out the purpose of the statute as providing the procedural framework for the government to access stored communications records.[113] The report also emphasizes the importance of privacy protection, citing the Framers' desire "to guard against the arbitrary use of government power to maintain surveillance over citizens."[114] In discussing the act itself, the report states that one purpose is to make sure that emerging technologies were also within the ambit of statutory protection.[115] This concern is especially highlighted when the report discusses potential abuse of surveillance power by the government. The report quotes Judge Richard Posner's observation that "the enormous power of government makes the potential consequences of its snooping far more ominous than those of . . . a private individual or firm."[116] The report further recognizes that new and burgeoning technologies did not fit neatly within the old wiretapping statute, which prompted concerns in the communications industry over customer

[111] S. REP. NO. 99-541, at 10-11.

[112] *Id.* at 1-3.

[113] H.R. REP. NO. 99-647, at 16 (1986).

[114] *Id.*

[115] *Id.* at 18 ("Unfortunately, the same technologies that hold such promise for the future also enhance the risk that our communications will be intercepted by either private parties or the government.").

[116] *Id.* at 19 (alteration in original) (quoting Richard A. Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 SUP. CT. REV. 173, 176).

privacy.[117] The industry feared that if customers perceived other mediums of communications to be more secure (e.g., paper mail), they might forgo the electronic medium for an alternative form of communication.[118]

Given the concern over the privacy of customers of electronic communications providers, as well as the problems inherent in the communications industry because of uncertainty over the application of privacy laws, one could argue that the general purpose of the statute is to protect consumers from unwarranted governmental intrusion. Assuming this is the general purpose, the statute should be read in new and ambiguous circumstances towards protecting communications from disclosure to the government. Further, the issues expressed in the House report track those expressed by commentators on the current application of the statute, referring to both privacy rights and business concerns.[119]

Since the classification as either an ECS or an RCS has significant influence on what service providers can release to the government, ambiguity in the statute should perhaps be read in a way that maximizes the number of service providers that are categorized as ECSs. This is because the government can only compel communications that ECSs hold in electronic storage for fewer than 180 days by using a warrant, rather than a 2703(d) court order. If the communication is stored in an RCS, however, the government can compel disclosure by using 2703(d) at any time or by using a subpoena with prior notice, as long as it meets the proper threshold.[120] The static classification method would likely provide more privacy protection than a variable categorization because under a static classification method, text message providers would have to be categorized as ECSs. Given that text messages are transmitted through different conduits before ultimately being transferred to a user's cell phone and that messages can be stored and resent by the provider until the intended recipient is able to receive messages on the network,[121] it would be difficult to imagine how the provider could not be deemed an ECS at those times. While a communication is held by an SMCS and being routed or re-routed to a user, it is likely in electronic storage because the storage is only temporary and incidental to the actual transmission.[122] Even if the sent message is over the character limit that can be sent using a SMS, it is likely still in electronic storage because any editing or processing of the message occurs just to make it deliverable.[123] This also echoes email jurisprudence on

[117] *Id.* at 26.

[118] *Id.*

[119] *See* Arena, *supra* note 16, at 371-72.

[120] *See supra* notes 41-44 and accompanying text.

[121] See *supra* Part I.

[122] *See* 18 U.S.C. § 2510(14) (2006) (defining the function of an ECS as providing "electronic storage" for electronic communications).

[123] *See* Brown et al., *supra* note 5, at 106.

the SCA, where a message sitting in a user's email inbox before the user reads it is considered to be in electronic storage.[124]

While the legislative history highlights privacy concerns, it also discusses the importance of prosecutors' abilities to use the statute effectively in criminal investigations.[125] Statically classifying providers as ECSs would reduce the effectiveness of the SCA, making it much more difficult for the government to compel communications and forcing it to obtain a warrant in most investigations. As Deputy Attorney General James A. Baker stated, "[R]aising the standard for obtaining information under ECPA may substantially slow criminal and national security investigations."[126] In contrast, statically classifying providers as RCSs would raise privacy concerns in allowing the government to compel RCS-stored communications without a warrant. The variable classification system would allow prosecutors to use a 2703(d) order when a provider acts as an RCS, but it also would require a warrant if the provider acts as an ECS. Congress likely created this bifurcated system, allowing for flexibility in whether to treat the provider as an ECS or an RCS, in order to balance these privacy and enforcement concerns. Courts should not upset this balance and should therefore adopt the variable classification method to resolve this controversy.[127]

As shown, even though the legislative purpose could support either classification method, the variable classification method better reflects the intent of Congress in upholding the balance it initially created by establishing two classes of storage for electronic communications. Since the text, legislative history, and legislative purpose support the variable classification method, courts should apply it in future controversies.

D. *Current Technology Renders Static Classification Unworkable*

Not only does a statutory analysis favor the variable classification method, but the current state of the telecommunications industry also compels the same conclusion. The Ninth Circuit's static classification method is actually unworkable, since many communication providers offer numerous types of services to the same customers.[128] Advances in technology have decreased prices for data storage, prompting many providers to offer it for free for Internet uses.[129] Providing many types of services greatly complicates provider classification, if such classification must be static. Following the Ninth Circuit's reasoning in *Quon*, any ECS that provides online storage of

---

[124] *See* United States v. Councilman, 418 F.3d 67, 85 (1st Cir. 2005).

[125] H.R. REP. NO. 99-647, at 16 (1986) (recognizing an ECPA goal of "eas[ing] certain procedural requirements for interception of wire communications by federal law enforcement officers").

[126] Angwin, *supra* note 7.

[127] *See supra* Part II.C.

[128] Arena, *supra* note 16, at 372-73.

[129] *Id.*

communications will be protected as an ECS and not as an RCS because the storage will be for "backup protection."[130] This narrow interpretation of the SCA, that any data stored by a provider that acts as an ECS is in electronic storage, becomes effectively unworkable when considering how some providers actually operate. In fact, this may be the case in *Quon* itself.

As discussed above, the provider in *Quon*, Arch Wireless, operated its text-messaging service much like Verizon Wireless and T-Mobile.[131] Arch Wireless stored the text messages until it delivered them when the intended recipient was in a service area.[132] As the *Flagg* court indicated, however, the classification of Arch Wireless as an ECS is problematic because Arch Wireless stated that it "archived" the messages on its servers.[133] "Archived" implies that the records were kept there for permanent or long-term storage, clearly not incidental to the transmission of the communication.[134] Further, the trial court in *Quon* stated that the storage that Arch Wireless provided was "long-term . . . not incidental to the transmission of the communication itself, and . . . not meant for backup protection," but instead as a repository where read messages were "archived for a permanent record-keeping mechanism."[135] Because of this, the type of storage that was provided by Arch Wireless is difficult, if not impossible, to fit within the definition of electronic storage.[136] The phrase "backup protection" in the definition implies that the storage serves as protection for the service provider against data loss.[137] Once a message is delivered and the recipient reads it, the recipient can keep the message on his or her phone indefinitely, as long as the phone has sufficient memory available.[138] Because the provider successfully sent the message, any retention of the communication by the provider seems to be only for the "benefit of the customer" as an archive.[139] Providing storage for the customer closer resembles the RCS definition of providing "computer storage" than the definition of electronic storage relevant to an ECS.[140] This shows that even in

[130] *Id.* at 373.

[131] *See supra* notes 51-55 and accompanying text.

[132] Quon v. Arch Wireless Operating Co., 529 F.3d 892, 895-96 (9th Cir. 2008).

[133] Flagg v. City of Detroit, 252 F.R.D. 346, 362 n.29 (E.D. Mich. 2008) (quoting *Quon*, 529 F.3d at 902-03).

[134] *Id.* at 363 n.29.

[135] Quon v. Arch Wireless Operating Co., 445 F. Supp. 2d 1116, 1136 (C.D. Cal. 2006).

[136] *See* 18 U.S.C. § 2510(17) (2006) (defining electronic storage as "any *temporary*, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service *for purposes of backup protection* of such communication" (emphasis added)).

[137] *See Flagg*, 252 F.R.D. at 362 n.29.

[138] *See, e.g.*, *supra* note 27 and accompanying text.

[139] *Flagg*, 252 F.R.D. at 363 n.29 (internal quotation marks omitted).

[140] *See supra* note 99.

Quon itself, the static classification method is unworkable. At some point after the message was received and read, Arch Wireless became an RCS. This functional reality provides further support for the variable classification method.

IV. THE WEIGHT OF THE DOJ'S INTERPRETATION: *SKIDMORE* DEFERENCE

In addition to statutory analysis, administrative law provides strong support for the variable classification method. Given that the DOJ uses the statute and has a view on its proper interpretation, courts may resolve the controversy by deferring to the DOJ under *Skidmore*.[141] Imagine a scenario in which the DOJ is prosecuting an individual suspected of smuggling drugs across state borders. When police initially arrest the suspected smuggler, they see him in the process of sending a text message, warning other suspected drug smugglers that the police have caught on to their scheme. In compiling their case against the smuggler, the prosecutor and investigators believe that the suspect used his cell phone to communicate with potential clients or suppliers. Unfortunately, the suspect deleted all messages before the investigators could retrieve them from the phone. The DOJ decides to compel disclosure of any text messages held by the suspect's cellular provider through use of a 2703(d) order, because the DOJ believes that the communications it seeks are in computer storage provided by an RCS. The DOJ then asserts that the classification of a provider as an ECS and an RCS are not static, and that after the text messages were sent and read, any copies held by the provider must be held in an RCS. A magistrate judge grants the government order. The suspect, now the defendant, seeks review of the magistrate decision in the District of Massachusetts. The District Court affirms the magistrate judge, and the case is appealed to the First Circuit. Should the First Circuit defer to the DOJ's interpretation of the SCA in resolving the case?

The First Circuit would not have to defer fully to the DOJ's interpretation of the statute because the DOJ's manual would not be eligible for *Chevron* deference.[142] Given that the DOJ has only discussed its view of the statute in the form of advisory opinions, its interpretation of the statute does not have "the force of law" and would therefore fail the preliminary requirements for *Chevron* deference.[143] As stated in *Christensen v. Harris County*,[144] "Interpretations such as those in opinion letters – like interpretations contained in policy statements, *agency manuals*, and enforcement guidelines, all of which

---

[141] *See* Skidmore v. Swift & Co., 323 U.S. 134, 139-40 (1944).

[142] *See* United States v. Mead Corp., 533 U.S. 218, 226-27 (2001) (setting the litmus test for deference under Chevron U.S.A. Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837 (1984), at "rules carrying the force of law"); Doe v. Leavitt, 522 F.3d 75, 86 (1st Cir. 2009) (holding that an agency manual was not entitled to *Chevron* deference but could receive *Skidmore* respect).

[143] *See, e.g.*, Cass R. Sunstein, *Chevron Step Zero*, 92 VA. L. REV. 187, 190-91 (2006).

[144] 529 U.S. 576 (2000).

lack the force of law – do not warrant *Chevron*-style deference."[145] Instead, the *Christensen* court stated that things like agency manuals are "entitled to respect" to the extent they have "power to persuade," citing *Skidmore*.[146] Therefore, while likely not entitled to *Chevron* deference, the DOJ manual may be entitled to *Skidmore* deference.

The Supreme Court in *Skidmore* signaled that deference should be given to the informed and experienced judgment and opinions of agencies even if such opinions are not binding.[147] The weight of this deference should be "somewhere between the poles of independent judgment and controlling deference."[148] In *Skidmore*, the Court gave deference to an administrator's determination even though it did not have the force of law.[149] The Court stated that the administrator's policies were "made in pursuance of official duty, based upon more specialized experience and broader investigations and information than is likely to come to a judge in a particular case."[150] Further, the court gave a list of reasons why courts should give more or less weight to the non-legal determinations of an agency: "thoroughness evident in its consideration, the validity of its reasoning, its consistency with earlier and later pronouncements, and all those factors which give it power to persuade, if lacking power to control."[151] Lower courts have applied this *Skidmore* deference to agency manuals. For example, in *Doe v. Leavitt*,[152] the First Circuit applied *Skidmore* deference to an agency's guidebook, which the court stated was essentially a manual.[153]

---

[145] *Id.* at 587 (emphasis added).

[146] *Id.* (quoting *Skidmore*, 323 U.S. at 140).

[147] *Skidmore*, 323 U.S. at 139-40; *see also* Kristin E. Hickman & Matthew D. Krueger, *In Search of the Modern* Skidmore *Standard*, 107 COLUM. L. REV. 1235, 1236 (2007) (stating that *Skidmore* is seen as the "Supreme Court's best expression of its policy of judicial deference toward many if not most agency interpretations of law"). Although more than sixty years old, *Skidmore* still enjoys status among courts as its own independent theory of judicial deference. *See, e.g.*, United States v. Mead Corp., 533 U.S. 218, 239 (2001) ("[W]hereas previously, when agency authority to resolve ambiguity did not exist the court was free to give the statute what it considered the best interpretation, henceforth the court must supposedly give the agency view some indeterminate amount of so-called *Skidmore* deference.") (Scalia, J., dissenting). *Skidmore* deference is still a widely contentious topic, and there is little consensus on what it means in practical terms. Hickman & Krueger, *supra*, at 1236-37. For the purposes of this Note, *Skidmore* deference is assumed to require some sort of deference, but less than that under *Chevron.*

[148] Hickman & Krueger, *supra* note 147, at 1241.

[149] *Skidmore*, 323 U.S. at 140.

[150] *Id.* at 139.

[151] *Id.* at 140.

[152] 552 F.3d 75 (1st Cir. 2009).

[153] *Id.* at 80.

Courts have also previously given the DOJ's recommendations deference,[154] and since the DOJ has extensive expertise and familiarity in prosecution and the statutes involved in compelling disclosure of communications, a strong argument supports judicial deference to the DOJ's interpretation of the SCA. The DOJ has an entire unit devoted to computer crimes, the Computer Crime and Intellectual Property Section (CCIPS).[155] CCIPS investigates and prosecutes computer crimes and also partners with academia and the private sector in authoring a manual for all the DOJ prosecutors on how to conduct investigations involving technology.[156] The DOJ expresses its view on the interpretation of the statute in that manual. CCIPS further helps "resolve unique legal and investigative issues raised by emerging computer . . . technologies" and "train[s] federal, state, and local law enforcement personnel."[157] The DOJ's vast experience in prosecuting and investigating crimes that involve emerging technologies demonstrate the type of "specialized expertise" that the administrator had in *Skidmore*.[158] Therefore, although a judge would not be required to defer to the DOJ in interpreting the provision in question, there is a strong case for *Skidmore* deference, and so courts may be more likely to follow the DOJ's variable classification method over the Ninth Circuit's static classification method.

Although the DOJ's reasoning and expertise in use of the statute may be persuasive, courts may be skeptical of giving deference in this instance.[159] As the previous discussion indicates, the static classification method gives greater privacy protection and makes it harder for government agencies to compel disclosure of communications.[160] The DOJ arguably has an incentive to provide a competing interpretation that allows it to contend that information is

[154] *See, e.g.*, Leegin Creative Leather Prods., Inc. v. PSKS, Inc., 551 U.S. 877, 900 (2007) (discussing the weight given by the Court to the DOJ's recommendation to replace the prevailing antitrust standard under the Sherman Act because the DOJ was one of the prominent "antitrust enforcement agencies"); William N. Eskridge, Jr. & Lauren E. Baer, *The Continuum of Deference: Supreme Court Treatment of Agency Statutory Interpretations from* Chevron *to* Hamdan, 96 GEO. L.J. 1083, 1111-13 (2008) (discussing cases in which courts gave "consultative" deference to agencies, including the DOJ).

[155] *Computer Crime & Intellectual Property Section*, U.S. DEP'T OF JUSTICE, http://justice.gov/criminal/cybercrime (last visited Apr. 12, 2012).

[156] *Id.*; *see also* COMPUTER CRIME, *supra* note 31.

[157] U.S. DEP'T OF JUSTICE, *supra* note 155.

[158] Skidmore v. Swift & Co., 323 U.S. 134, 139 (1944).

[159] There does seem to be something unsettling about a court giving deference to an agency like the DOJ that serves a law enforcement function. While this is a valid concern, *but see infra* note 162 and accompanying text, the Supreme Court, while not specifically citing *Skidmore*, has given weight to the DOJ's interpretation of the Sherman Act, even though the DOJ is one of the largest enforcers of the statute's provisions, *see supra* note 154 and accompanying text. Therefore, a grant of *Skidmore* deference in this instance would properly recognize the expertise the DOJ has in the use and operation of the statute.

[160] *See supra* Part II.B.

held in an RCS and not an ECS. The burden to compel disclosure from an RCS is lower, and so the DOJ could compel stored communications during investigations without having to satisfy the demanding standard for retrieval from an ECS. Courts may be especially apprehensive because this issue invokes constitutional privacy concerns and because ECPA's congressional history discusses concern over governmental intrusion and abuse of power.[161] But the DOJ's thoughtful and thorough approach to the SCA in its manual indicates that it has also taken those concerns into account.[162] Courts can thus safely consider *Skidmore* deference to the DOJ, secure in the knowledge that the agency has considered not only the technical implications of the SCA but also its constitutional implications.

CONCLUSION

A review of the text, legislative history, and purpose of ECPA and the SCA, combined with pragmatic technological considerations, leads to one conclusion: the DOJ's variable classification method is the correct application of the statute. A question remains: why did the Ninth Circuit misapply the statute? It would be easy to dismiss this erroneous decision as a natural result of the complexity of the statute and the difficulty in applying an old scheme to current, ever-evolving technology. While these considerations may have played a role, the Ninth Circuit may have deliberately chosen to craft an easier, less burdensome analysis to apply.

The court's simplistic methodology makes determining the proper mode of compulsion quite easy. Under the Ninth Circuit method, a court would merely have to determine whether the provider is "any service which provides to users thereof the ability to send or receive wire or electronic communications"[163] or if the service provides "computer storage" or "processing services."[164] The simplicity and ease of application of the statute may lessen industry concerns over uncertainty.[165] If a provider were able to determine easily whether the communications it held were in electronic storage or computer storage, it might be more willing to comply with prosecutors' requests for those communications because the specter of suit for wrongful disclosure would be lessened. Certainty would also allow technology developers to design new products and services that would provide greater protection via ECS rather

[161] *See supra* notes 115-116 and accompanying text.

[162] *See, e.g.*, COMPUTER CRIME, *supra* note 31, at 112 (discussing the necessity of avoiding seizure of communications belonging to disinterested parties in an SCA action).

[163] Quon v. Arch Wireless Operating Co., 529 F.3d 892, 900 (9th Cir. 2008) (quoting 18 U.S.C. § 2510(15) (2006)).

[164] *Id.* (quoting 18 U.S.C. § 2711(2)).

[165] *See, e.g.*, Mark Stanley & Harley Geiger, *For Business' Sake, Gov't Surveillance Law Must Be Reformed*, BUSINESS 2.0 PRESS (Sept. 29, 2010, 10:31 AM), http://business2press.com/2010/09/29/for-business%E2%80%99-sake-gov%E2%80%99t-surveillance-law-must-be-reformed.

than RCS, quelling user concerns.[166] The Ninth Circuit's static classification method would also conserve judicial resources. To determine if something is in either electronic storage or computer storage under the variable classification method, an investigation of the purposes of storage is needed. If the process of determining the provider's role were easier, fewer resources would be needed to classify the provider.

While the Ninth Circuit's classification method is undoubtedly simpler to apply, the variable classification method better comports with the statute's text and preserves the vital balance Congress struck between prosecutorial effectiveness and individual privacy concerns. Just because the classification of a provider as an ECS or an RCS as to each communication may be burdensome does not mean that a court should step into the legislature's role and craft a new solution. Frustrations over the application of the statute and increasing judicial attention may prompt congressional action, especially if privacy concerns are not protected by the SCA as thoroughly as many believe necessary.[167] As evidenced by the proliferation of groups calling for ECPA's reform,[168] greater judicial attention may also increase the number and strength of interest groups pushing for reform.

In reforming the SCA, Congress should focus on simplicity of interpretation and ensure that the SCA can track further developments in technology. Since providers often supply computer storage, data analysis, and communications transmission to the same customers, the distinctions between ECSs and RCSs are too cumbersome to give customers sufficient privacy protection and allow the government to conduct effective investigations. Therefore, instead of classifying a provider as an ECS or an RCS, the statute should provide different levels of privacy protection for different modes of communication and data. For example, once a user sends a text message, the message should receive the same level of protection whether it is en route or received and read by the intended recipient. This way, the government could compel disclosure of the communication from the provider without the provider or government worrying about running afoul of federal law. Further, the system would provide certainty to customers, quelling industry concerns. This approach would still have to comply with Fourth Amendment jurisprudence but would end judicial confusion and disagreement over the statutory requirements of compulsion.

This Note highlights what will likely be a growing problem in statutory construction: how ever-evolving technology will fit into outdated statutes like the SCA. As shown, Congress cannot anticipate all technological advancements and cannot or may be unwilling to amend statutory schemes after development of new communication mediums or other technology. In

[166] *Id.*

[167] For a suggestion on how to amend the SCA to reflect current technological realities, see Kerr, *supra* note 12, at 1233-42.

[168] *See, e.g.*, DIGITAL DUE PROCESS, *supra* note 14.

terms of the SCA, however, calls for reform by the private sector and confusion among federal prosecutors and investigators may be enough to spur a change to a simpler statutory scheme that would work with current technology. Perhaps after twenty-six years of technological development, Congress will amend ECPA and the SCA to reflect current technological realities.