No. 12-

IN THE
Supreme Court of the United States

M. LEE JENNINGS,

Petitioner,

v.

HOLLY BROOME,

Respondent.

On Petition for a Writ of Certiorari to the South Carolina Supreme Court

PETITION FOR A WRIT OF CERTIORARI

MAX N. PICKELSIMER
CARRIE A. WARNER
WARNER, PAYNE & BLACK, LLP
1531 Blanding Street
Columbia, SC 29201
(803) 799-0554

NEAL KUMAR KATYAL*
JESSICA L. ELLSWORTH
JORDAN ESTES
HOGAN LOVELLS US LLP
555 13th Street, N.W.
Washington, D.C. 20004
(202) 637-5528
neal.katyal@hoganlovells.com

Counsel for Petitioner
**Counsel of Record*

QUESTION PRESENTED

The Stored Communications Act was enacted in 1986 to create statutory privacy rights for e-mail users. It prohibits unauthorized access to e-mail in "electronic storage," regulates the voluntary disclosure by e-mail providers of messages in "electronic storage," and specifies what process the government must use to compel e-mail providers to turn over messages that are in "electronic storage." The government must, for example, obtain a warrant based on probable cause to obtain an e-mail that has been in "electronic storage" for 180 days or less.

Whether an e-mail is in "electronic storage" is thus crucial for determining the level of privacy protection it receives under the Act. In the decision below, the South Carolina Supreme Court held that e-mails stored by web-based e-mail providers (such as Yahoo or Gmail) are only in "electronic storage" until they have been accessed and read by the recipient. Pet. App. 15a, 18a. In direct contrast, the Ninth Circuit has held that "prior access is irrelevant" to whether an e-mail is "in electronic storage." *Theofel* v. *Farey-Jones*, 359 F.3d 1066, 1077 (2003).

The question presented is: Whether e-mails stored by an e-mail provider after delivery are in "electronic storage" under the Stored Communications Act.

PARTIES TO THE PROCEEDINGS

The following were parties to the proceedings in the South Carolina Supreme Court:

1. M. Lee Jennings, the petitioner on review, was the plaintiff in the Court of Common Pleas, the appellant in the Court of Appeals, and the respondent in the South Carolina Supreme Court.

2. Holly Broome, the respondent on review, was a defendant in the Court of Common Pleas, an appellee in the Court of Appeals, and the petitioner in the South Carolina Supreme Court.

3. Gail M. Jennings, Brenda Cooke, and BJR Detective Agency, Inc., were defendants in the Court of Common Pleas and appellees in the Court of Appeals. They were not petitioners to the South Carolina Supreme Court because they prevailed in the Court of Appeals. They are not parties to this petition for certiorari.

TABLE OF CONTENTS

TABLE OF CONTENTS—Continued

APPENDICES

TABLE OF AUTHORITIES

Page

CASES:

TABLE OF AUTHORITIES—Continued

Page

CONSTITUTIONAL PROVISION:

STATUTES:

TABLE OF AUTHORITIES—Continued

Page

TABLE OF AUTHORITIES—Continued

Page

OTHER AUTHORITIES:

TABLE OF AUTHORITIES—Continued

Page

IN THE

Supreme Court of the United States

No. 12-

M. LEE JENNINGS,

Petitioner,

v.

HOLLY BROOME,

Respondent.

On Petition for a Writ of Certiorari to the South Carolina Supreme Court

PETITION FOR A WRIT OF CERTIORARI

M. Lee Jennings respectfully petitions for a writ of certiorari to review the judgment of the South Carolina Supreme Court.

OPINIONS BELOW

The decision of the South Carolina Supreme Court is not yet reported, but is currently available at 2012 WL 4808545 and reproduced at Pet. App. 1a-18a. The decision of the Court of Appeals of South Carolina is reported at 389 S.C. 190 and reproduced at Pet. App. 19a-44a. The order of the Court of Common Pleas of South Carolina in the Fifth Judicial Circuit is not reported, but is available at 2008 WL 8185934 and reproduced at Pet. App. 45a-58a.

JURISDICTION

The South Carolina Supreme Court entered judgment on October 10, 2012. This Court's jurisdiction rests on 28 U.S.C. § 1257(a).

STATUTE INVOLVED

The Stored Communications Act makes it unlawful to access, in specified circumstances, "a wire or electronic communication while it is in electronic storage." 18 U.S.C. § 2701(a). It prohibits providers of electronic communications services to the public from divulging "the contents of a communication while in electronic storage by that service," unless an exception applies. 18 U.S.C. § 2702(a)(1). And it requires governmental entities to obtain a warrant to compel disclosure of "the contents of a wire or electronic communication[ ] that is in electronic storage in an electronic communications system" at certain times. 18 U.S.C. § 2703(a).

The scope of each of these statutory restrictions turns on when an email is "in electronic storage." Electronic storage is defined for purposes of the Stored Communications Act as follows:

> "[E]lectronic storage" means—(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication[.]

18 U.S.C. § 2510(17) (incorporated at 18 U.S.C. § 2711(1)).[1]

---

[1] These statutory provisions, and additional provisions of the SCA, are reprinted at Pet. App. 59a-78a.

INTRODUCTION

Courts around the country have reached fundamentally different conclusions as to what e-mails are covered by the significant privacy protections in the Stored Communications Act. And they have been deeply divided in the reasoning for their varied conclusions—as demonstrated by the three divergent approaches adopted in the three opinions comprising the decision below. The discord stems from trying to apply the terms of a statute written more than 25 years ago to the e-mail communications and systems that are everywhere today, but had not yet even been imagined in 1986. As quaint as it sounds, back then Congress contemplated that an e-mail provider might actually print an e-mail to deliver it via the post office. S. Rep. 99-541 at 8 (1986).

In today's world, however, people send and receive dozens, if not hundreds, of e-mails through home computers, work computers, laptops, and smartphones as they go about their days. They access their e-mail through platforms on web browsers (like Gmail or Yahoo), through software on personal computers (like Outlook or Lotus Notes), or through handheld devices (like iPhones or Blackberries). The privacy these users have is governed by the Stored Communications Act. As a result, the answer to what privacy protections apply to what e-mails—and whether the privacy protection turns on an e-mail's status as "unread" or "downloaded"—is a matter of profound importance. It matters to private citizens like Petitioner whose e-mail accounts are hacked. It matters to federal and state law enforcement officers who need to know what they must demonstrate to obtain e-mails as

part of a criminal or civil investigation. And it matters to e-mail providers themselves, faced with determining on a daily basis whether to turn over e-mails to the government and, if so, which ones.

The SCA's privacy protections should not change simply because an internet service provider happens to maintain a server in California, an email happens to be read on a smartphone in South Carolina, or a United States Attorney in Boston wants to review internal emails from a company's Chicago office as part of a criminal investigation. It is critical that the SCA's privacy protections apply consistently nationwide, so that private citizens, law enforcement, and e-mail providers can all be on the same page about when personal and confidential e-mails are truly private and when they are not. This Court has never addressed the SCA's privacy protections, and it is now time to do so.

STATEMENT OF THE CASE

A. The Stored Communications Act

1. Congress passed the Stored Communications Act ("SCA") in 1986 because it believed that existing laws were inadequate to protect the privacy of stored electronic communications, such as e-mail. *See* H.R. Rep. 99-647, at 17-19 (1986); 2 W. LaFave et al., Criminal Procedure § 4.5, at 465-466 (3d ed. 2007). While the Wiretap Act, 18 U.S.C. §§ 2510 *et seq.*, regulated the interception of traditional telephone calls, it was ill-suited to other burgeoning forms of electronic communication. That Act not only was limited to the acquisition of communications containing the human voice, but also applied only to communications in transit, which left *stored* communications unprotected. 2 LaFave, Criminal Procedure § 4.5, at 465-466.

Likewise, the Fourth Amendment was not a good fit for protecting stored electronic communications, given that their content is revealed to a third-party Internet service provider in the course of transmission and storage. *See, e.g.*, *United States* v. *Miller*, 425 U.S. 435, 443 (1976) (the Fourth Amendment generally does "not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed"). In addition, because most e-mail providers are private actors, they are not bound by the Fourth Amendment at all and could voluntarily turn over communications to the government without limitation. As one commentator has noted, the way the Internet works seems almost "custom designed" to frustrate the Fourth Amendment. Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance*, 54 Hastings L.J. 805, 812-813 (2003).

Congress therefore enacted the SCA because existing protections for stored electronic communications were "weak, ambiguous, or nonexistent." Office of Tech. Assessment, *Electronic Surveillance and Civil Liberties* 45 (1985). As the House Committee Report warned, "if Congress does not act to protect the privacy of our citizens, we may see the gradual erosion of a precious right. * * * Additional legal protection is necessary to ensure the continued vitality of the Fourth Amendment." H.R. Rep 99-647, at 19; *see* S. Rep. 99-541 at 5.

2. In pursuit of that object, the SCA has three basic components. First, it prohibits unauthorized access to certain stored communications. 18 U.S.C. § 2701.

Second, it regulates voluntary disclosure by network service providers to the government and private parties. *Id.* § 2702. And third, it creates a "code of criminal procedure" that law enforcement officers must follow in order to compel network service providers to disclose stored communications. Computer Crime & Intellectual Prop. Div., U.S. Dep't of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 115 (3d ed. 2009) (describing 18 U.S.C. § 2703) [hereinafter "DOJ Manual"].[2]

The SCA distinguishes between two types of network service providers. One is an "electronic communications service," which is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).[3] E-mail providers are the most obvious example of this type of provider. *See* S. Rep. No. 99-541 at 14. The second type is a "remote computing service," defined as the "provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2).[4] In 1986, when the SCA was

---

[2] *Available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

[3] An electronic communication is "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce," with a few exceptions not relevant here. 18 U.S.C. § 2510(12).

[4] An electronics communications system is "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).

passed, personal computing was still rudimentary; complex processing tasks had to be outsourced to more powerful machines. A remote computing service would provide storage or processing capacity for a fee. H.R. Rep. 99-647 at 23. Current examples of a "remote computing service" might include (for some uses) Dropbox or Google Docs. The type of network service provider storing a file triggers different levels of privacy protection.

The Act's compelled and voluntary disclosure provisions track these two types of providers. Section 2703, which provides the standards and procedures the government must satisfy before it can compel a network service provider to disclose customer communications or records, accords the highest level of protection to communications held by an "electronic communications service" in "electronic storage" for 180 days or less. *Id.* § 2703(a). The government needs a search warrant to compel disclosure of the contents[5] of such a communication. *Id.* For communications in "electronic storage" for 181 days or more, or for content held by "remote computing services," the government can compel disclosure through other, less stringent means: it can get a warrant; it can get a subpoena, *id.* § 2703(b)(B)(i); or it can obtain an order under section 2703(d).[6]

---

[5] Content is only defined in terms of what it "includes," namely, "any information concerning the substance, purport, or meaning of [an electronic] communication." *Id.* § 2510(8).

[6] To obtain a 2703(d) order, the government must provide "specific and articulable facts showing that there are reasonable grounds to believe" that the information sought is "relevant and material to an ongoing criminal investigation." *Id.* § 2703(d). This is "'an intermediate standard,' 'higher than a subpoena,

Section 2702's voluntary disclosure provision prevents a public electronic communications service from disclosing "the contents of a communication while in electronic storage by that service," unless one of the exceptions applies. *Id.* § 2702(a)(1). Those exceptions include disclosure to an "addressee or intended recipient," compelled disclosure under section 2703, or disclosure with the lawful consent of the communication's "originator" or "intended recipient." *Id.* § 2702(b). Voluntary disclosure of non-content records to the government is subject to a slightly different set of exceptions. *Id.* § 2702(c).

Finally, the SCA defines a substantive crime. Section 2701(a) provides that "whoever * * * intentionally accesses without authorization a facility through which an electronic communication service is provided * * * and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished."

The prohibition of unlawful access set forth in Section 2701 and the disclosure regulations set forth in Sections 2702(a)(1) and 2703(a) all apply to communications that are in "electronic storage," which is defined as:

> (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

---

but not a probable cause warrant,'" and "was intended 'to guard against "fishing expeditions" by law enforcement.'" 2 LaFave, Criminal Procedure § 4.8(c), at 534 (quoting H.R. Rep. No. 103-827, at 31-32 (1994)).

> (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication[.]

18 U.S.C. § 2510(17); *id.* § 2711(1). The scope of the SCA's disclosure provisions and its protections accordingly turns on exactly what is encompassed by this definition.

Any person aggrieved by a violation of the Act may file a civil cause of action against anyone who violated a provision of the SCA "with a knowing and intentional state of mind." *Id.* § 2707(a).

B. Proceedings Below

1. Lee Jennings filed suit under the SCA's civil provisions. The facts are straightforward and not in dispute. Jennings' wife, Gail, found a card for flowers in her car that she suspected was not for her. Pet. App. 2a. When she confronted Jennings, he confessed that he had fallen in love with another woman, but would not reveal her name. *Id.* Gail and Jennings separated that day. Pet. App. 20a.

Gail told her daughter-in-law from a prior marriage, Holly Broome, what had happened. Pet. App. 2a. Broome had previously worked with Jennings and knew that he had a private Yahoo e-mail account. *Id.* She was able to hack into Jennings' Yahoo account by correctly guessing the answers to his security questions and resetting the password. *Id.* She snooped around and discovered several e-mails between Jennings and his paramour. She printed them, and distributed copies to Gail, Gail's divorce attorney, and a private investigator whom Gail had hired. *Id.* Broome did not read any unopened messages; they had all previously been opened and read by Jennings. Pet. App. 16a, 53a.

2. Jennings sued Gail, Broome, the attorney, and the investigator in the Court of Common Pleas for the Fifth Judicial Circuit of South Carolina, alleging violations of the SCA and several state laws. The circuit court granted summary judgment to the defendants on the SCA cause of action, holding that the e-mails accessed by Broome were not in "electronic storage," as required for a violation of the SCA. Pet. App. 53a; *see* 18 U.S.C. §§ 2701(a)(1), 2707(a). The court reasoned that the e-mails failed to satisfy the first part of the definition of "electronic storage" because the "e-mails had already been transmitted and had reached their final destination"; thus they could not be in "temporary, intermediate storage * * * incidental to the electronic transmission." Pet. App. 53a; 18 U.S.C. § 2510(17)(A).

The court further held that whether an email is stored "for purposes of backup protection," as specified in the second prong of the definition, depends on the electronic communications service's purpose in storing the email, and not on any purpose the user may have had. Pet. App. 54a-56a. Because Yahoo was not storing the e-mails for its *own* "purposes of backup protection," the court reasoned that the e-mails failed to satisfy the second prong of the definition of electronic storage. *Id.* The circuit court accordingly dismissed the SCA claim against Broome, as well as against the other defendants because there was no evidence that they had personally violated the statute. Pet. App. 57a-58a. It also dismissed Petitioner's additional state law claims.

3. The South Carolina Court of Appeals reversed the dismissal of the SCA cause of action against

Broome. That court "unquestionably" viewed Yahoo as an "electronic communications service" because Yahoo "provides its users with the ability to send or receive electronic communications." Pet. App. 30a; *see* 18 U.S.C. § 2510(15); S. Rep. No. 99-541, at 14 ("[E]lectronic mail companies are providers of electronic communication services."). The court then held that e-mails stored by Yahoo like Petitioner's were in "electronic storage" under subsection (B) of the definition: they were stored "for purposes of backup protection," even though they were in a post-transmission state. Pet. App. 34a. The court reasoned that "one of the purposes of storing a backup copy of an email message on an ISP's server after it has been opened is so that the message is available in the event the user needs to retrieve it again." *Id.* In so holding, it explicitly agreed with the analysis of the Ninth Circuit regarding this very issue in *Theofel* v. *Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004), and concluded that Broome could be liable. Pet. App. 34a, 40a.

The defendants had argued that "because [Jennings] ha[d] not claimed that he saved the emails anywhere else, the storage of his emails could not have been for the purposes of backup protection." Pet. App. 35a. The Court of Appeals disagreed. It cited numerous court decisions that it read as consistent with Petitioner's cause of action. *Id.* (citing *Cardinal Health 414, Inc.* v. *Adams*, 582 F. Supp. 2d 967, 976 (M.D. Tenn. 2008); *Pure Power Boot Camp* v. *Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548, 555 (S.D.N.Y. 2008); *Fischer* v. *Mt. Olive Lutheran Church, Inc.*, 207 F. Supp. 2d 914, 925-926 (W.D. Wisc. 2002)). Further, it explained that the defendants' interpretation would lead to

"strange results": If their argument were to prevail, "unauthorized access of a person's emails from an [electronic communications service] would be unlawful if the person had previously saved his emails somewhere else, but would be perfectly lawful if the person had not done so." Pet. App. 35a-36a. That result would make no sense, since "a person whose emails were stored solely with an [electronic communications service] would generally suffer *greater* harm if someone 'alter[ed]' or 'prevent[ed] authorized access' to his ECS-stored emails than a person who had saved his emails in additional locations." *Id.* (emphasis added). Finally, the court found further support in the legislative history of the SCA. Pet. App. 36a.

4. The South Carolina Supreme Court granted certiorari to address whether "the e-mails in question were * * * in 'electronic storage' as defined by 18 U.S.C. § 2510(17)." Pet. App. 3a. A badly fragmented court reversed the Court of Appeals, issuing three separate opinions based on three different rationales. Justice Hearn, joined by Justice Kittredge, wrote that the e-mails on the Yahoo server were not stored "for purposes of backup protection" because they were not also stored elsewhere. Noting that the "ordinary meaning of the word backup is 'one that serves as a substitute or support,'" Justice Hearn believed that "Congress's use of the word backup necessarily presupposes the existence of another copy." Pet. App. 7a. Jennings did not download or save another copy of the e-mails in question to another location; therefore, they could not be "stored for backup protection." *Id.*

Chief Justice Toal, joined by Justice Beatty, concurred in the judgment but offered an entirely

different rationale. She believed that the "and" in the definition of electronic storage was conjunctive—not disjunctive—so that electronic storage requires "temporary, intermediate storage" incidental to transmission "*and*" storage "for purposes of backup protection." 18 U.S.C. § 2510(17) (emphasis added). Only emails that meet *both* conditions are in electronic storage under this reasoning. Pet. App. 14a. Because the e-mails in question had already been opened by Jennings, and had already reached their final destination, they were not in "temporary" and "intermediate" storage and thus not in "electronic storage." Pet. App. 14a-16a. The upshot of her reading was that "backup" referred only to "'a copy made by the service provider for administrative purposes'" in the course of transmission. Pet. App. 11a (quoting Orin Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1217 n.61 (2004)). Chief Justice Toal recognized the conflict between her reasoning and the Ninth Circuit's in *Theofel*. She "advocate[d] a rejection of *Theofel* entirely" and instead adopted the interpretation found in the DOJ Manual. Pet. App. 13a.

Justice Pleicones concurred in the result. He agreed with Chief Justice Toal that "backup protection" referred only to backups of "temporary storage of communications during the course of transmission," thus rejecting the Ninth Circuit's decision in *Theofel*. Pet. App. 18a. But he disagreed with the Chief Justice's opinion that the "and" in the definition of electronic storage was conjunctive; he thought that the two prongs of the definition were "necessarily distinct." *Id.*

This petition followed.

REASONS FOR GRANTING THE PETITION

Certiorari review is warranted here. A clear conflict exists between the decision below and the Ninth Circuit's decision in *Theofel*. Only this Court can resolve the split created by these decisions.

Given the prevalence of email (and other stored electronic communications), the SCA is a vital statute that governs how we live our lives. And its privacy protections hinge on the proper interpretation of the term "electronic storage." The question this petition presents arises hundreds of times every day in the law enforcement context alone, as federal or state investigators seek to compel e-mail providers to turn over the contents of user messages. And because e-mail providers' customers write and read emails from all over the country, e-mail providers—as well as their customers and law enforcement—are in the untenable position of not knowing when the SCA's protections are triggered. The prevalence of cloud computing, which exists untethered to a particular jurisdiction, makes this one area of law where consistency is uniquely demanded. Moreover, the decision below is wrong. It conflicts with the text and purpose of the SCA and should be reversed.

Despite the fact that the SCA is the main source of privacy protection for e-mails, text messages, and other increasingly prevalent forms of electronic communication, in the quarter-century since its passage, this Court has never addressed it. Given the pervasiveness of e-mail in modern American society, and the centrality of the question presented to the structure of the SCA, this Court's guidance is sorely needed.

I. THE DECISION BELOW CONFLICTS WITH DECISIONS OF OTHER LOWER COURTS.

The South Carolina Supreme Court has clearly "decided an important federal question in a way that conflicts with the decision of * * * a United States court of appeals." S. Ct. R. 10(c). Three of the five Justices expressly "advocate[d] a rejection of *Theofel* entirely." Pet. App. 13a, 18a. The two other Justices "question[ed] the reasoning expressed in *Theofel*." Pet. App. 7a. Even before this case, the Department of Justice had recognized "a split between two interpretations of 'electronic storage,'" DOJ Manual 123, which the decision below deepens. Indeed, a leading academic authority on the SCA has recognized that the decision below "creates a clear split with *Theofel*." Orin Kerr, *South Carolina Supreme Court Creates Split With Ninth Circuit on Privacy in Stored E-Mails—And Divides 2-2-1 on the Rationale*, Volokh Conspiracy, Oct. 10, 2012 [hereinafter Kerr, *Split with Ninth Circuit*].[7] This Court should grant the petition to resolve the conflict.

1. *Theofel* v. *Farey-Jones* involved an overly broad subpoena served during discovery in a civil lawsuit. 359 F.3d at 1071. Farey-Jones was the defendant in that civil suit and used a "patently unlawful" and "massively overbroad" subpoena to compel an Internet service provider, NetGate, to turn over "[a]ll copies of e-mails sent or received by anyone" at a particular company. *Id.* at 1071-72. NetGate turned over many of those e-mails, even though "[m]ost were unrelated to the litigation, and many were privileged

---

[7] *Available at* http://www.volokh.com/2012/10/10/sourth-carolina-supreme-court-deepens-split-on-privacy-in-stored-e-mails-and-divides-2-2-1-on-the-rationale/.

and personal." *Id.* When employees of the company learned what had happened, they separately sued Farey-Jones and his lawyer for violating the SCA.

The SCA exempts from civil liability conduct "authorized * * * by the person or entity providing * * * an electronic communications service." 18 U.S.C. § 2701(c)(1). The district court had dismissed the suit on the ground that NetGate had "authorized" the defendants' access. The Ninth Circuit, per Judge Kozinski, held that the defendants lacked a valid "authoriz[ation]" under section 2701, because they had "procured consent" (with the subpoena) to access the e-mails "by exploiting a known mistake that relate[d] to the essential nature of [that] access." 359 F.3d at 1073.

The Ninth Circuit then considered whether the e-mails that had been accessed were in "electronic storage" such that they could be the basis for suit under the SCA. The defendants, and the United States as *amicus curiae*, contended that the e-mails were no longer in "electronic storage" because they had already been opened and read by the plaintiffs. They argued that "electronic storage" did not include any "post-transmission storage" at all. *Id.* at 1075. The Ninth Circuit unanimously rejected that argument. It held that "messages remaining on an ISP's server after delivery * * * fit comfortably within subsection (B)" of the definition of electronic storage, which covers e-mails stored "'for purposes of backup protection.'" *Id.* at 1075 (quoting 18 U.S.C. § 2510(17)(B)).

Judge Kozinski's opinion for the court noted that an "obvious purpose for storing messages on an ISP's server after delivery is to provide a second copy of the message in the event the user needs to download

it again." *Id.* at 1075. He further noted that "nothing" in the SCA "requires that the backup protection be for the benefit of the ISP rather than the user." *Id.* In short, the Ninth Circuit rejected the defendants' and United States' interpretation as "contrary to the plain language of the Act." *Id.*

Moreover, as the Ninth Circuit explained, that interpretation would "render[] subsection (B) essentially superfluous." *Id.* If subsection (B) "applies only to backup copies of messages that are themselves in temporary, intermediate storage under subsection (A)"—then subsection (B) would be "drain[ed] * * * of independent content." *Id.* at 1076. That is because "virtually any backup of a subsection (A) message will itself qualify as a message in temporary, intermediate storage." *Id.*

The Ninth Circuit therefore concluded that "prior access is *irrelevant* to whether the messages at issue were in electronic storage." *Id.* at 1077 (emphasis added). Thus, in the nine states comprising the Ninth Circuit, the SCA and its privacy protections apply equally to e-mails that have been read and to those that are unread. And federal and state law enforcement in those nine states are simply stuck with a rule at odds with the interpretation of the statute in the DOJ Manual. *See* DOJ Manual 122-125.

2. As detailed above, the South Carolina Supreme Court "reject[ed] * * * *Theofel* entirely" and "adopt[ed]" the Department of Justice's "'traditional interpretation' of the SCA." Pet. App. 13a. Chief Justice Toal explained that when "an e-mail has been received by a recipient's service provider but has not yet been opened by the recipient, it is in electronic storage." Pet. App. 15a (citing *Steve*

Jackson Games, Inc. v. *United States Secret Serv.*, 36 F.3d 457, 461 (5th Cir. 1994)). But then she parted ways with the Ninth Circuit: "When the recipient opens the e-mail, however, the communication reaches its final destination. If the recipient chooses to retain a copy of the e-mail on the service provider's system, the retained copy is no longer in electronic storage because it is no longer in 'temporary, intermediate storage * * * incidental to * * * electronic transmission.'" *Id.* (citing *Fraser* v. *Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 635-636 (E.D. Pa. 2001)). In her view, subsection (B) applies only to "'copies of unopened e-mails made by the ISP for its administrative purposes.'" Pet. App. 10a-11a (quoting Kerr, *A User's Guide to the SCA*, at 1217 n.61).

Chief Justice Toal was joined by Justice Beatty in her opinion, and Justice Pleicones agreed with the substance of their analysis in a separate opinion. In his view, "[t]he 'backup' covered by subsection (B) is a copy made by the service provider to back up its own servers. It does not include an original e-mail that has been transmitted to the recipient and remains on the provider's server after the recipient has opened or downloaded it." Pet. App. 18a. In sum, the court clearly "reject[ed]" *Theofel*. Pet. App. 13a.

3. The U.S. Department of Justice's "traditional interpretation" of the SCA—referred to several times in the opinions below—is set out in a published manual. *See* DOJ Manual 122-125. There, the Department explains that "the 'backup' component of the definition of 'electronic storage' refers to copies made by an ISP to ensure system integrity." *Id.* at 124. It acknowledges that its view is a "narrow" one,

and that it was "rejected by the Ninth Circuit in *Theofel*." *Id.* Nonetheless, the Manual instructs "law enforcement" outside the Ninth Circuit that they "may continue to apply the traditional interpretation of 'electronic storage,'" while conceding that law enforcement personnel within the Ninth Circuit are bound by *Theofel*.

4. To add to the confusion, district courts are all over the map in interpreting when e-mails are electronically stored for purposes of the SCA. "The majority of courts that have addressed the issue have determined that 'prior access is irrelevant to whether the messages at issue were in electronic storage,' concluding that electronic communications that are stored on a server hosting an electronic communication service after they have been delivered to an end-user remain in 'electronic storage' provided they are retained for purposes of backup protection." *Council on Am.-Islamic Relations Action Network, Inc.* v. *Gaubatz*, 793 F. Supp. 2d 311, 336-337 (D.D.C. 2011) (agreeing with the majority view); *see, e.g.*, *Cardinal Health 414, Inc.* v. *Adams*, 582 F. Supp. 2d 967, 976 (M.D. Tenn. 2008); *Pure Power Boot Camp* v. *Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548, 556 (S.D.N.Y. 2008); *Bailey* v. *Bailey*, 2008 WL 324156 (E.D. Mich. Feb. 6, 2008). Two district courts in the Third Circuit, however, have hewed to the Justice Department's narrow interpretation. *Bansal* v. *Russ*, 513 F. Supp. 2d 264, 276 (E.D. Pa. 2007); *Fraser* v. *Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001). But the Third Circuit has called that narrow interpretation "questionable" without deciding the issue. *Fraser* v. *Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114 (3d Cir. 2003).

Some courts, relying on "dicta in *Theofel*," have held that opened e-mails stored by *web-based* e-mail providers are *not* in electronic storage, because there is not always a separate copy stored on a user's own computer. *Crispin* v. *Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 987 (C.D. Cal. 2010); *United States* v. *Weaver*, 636 F. Supp. 2d 769, 770 (C.D. Ill. 2009). Other courts have indicated that, under *Theofel*, opened e-mails stored by web-based providers such as Yahoo *are* protected. *Bailey*, 2008 WL 324156, at *6. This widespread confusion in the district courts accompanying a clear split between courts of last resort further supports granting *certiorari* here. *See* E. Gressman et al., *Supreme Court Practice* § 4.8, at 256-257 (9th ed. 2007).

* * *

The Ninth Circuit's decision in *Theofel* and the South Carolina Supreme Court's decision in this case are in irreconcilable conflict. The Ninth Circuit "reject[ed]" DOJ's traditional interpretation of the SCA, 359 F.3d at 1075; the decision below "adopt[ed]" it, Pet. App. 13a. In South Carolina, e-mails in post-transmission storage can never be in electronic storage under the SCA, Pet. App. 15a, 18a; in the Ninth Circuit, "prior access is irrelevant to whether the messages at issue [a]re in electronic storage." 359 F.3d at 1077. The decision below could not have been clearer in recognizing that it was creating a split; it "advocate[d] a rejection of *Theofel* entirely." Pet. App. 13a.

While it is often advisable for this Court to let issues percolate, this is the rare case in which *certiorari* is justified despite the fact that many appellate courts have not decided the issue. The case presents a pure issue of law, and competing views of

the statute have been fully ventilated by the courts below. The United States has already weighed in on its interpretation of the statute and the existence of a "split" in authority. DOJ Manual 123.

And it may take a long time for the Court to see this issue again: it is not litigated nearly as frequently as its importance warrants. Practically speaking, the most important function of the definition of "electronic storage" is to delimit the scope of the warrant requirement under section 2703. But the SCA—unlike the Fourth Amendment or the Wiretap Act—does not contain a suppression remedy: evidence obtained in violation of the SCA can still be used against an accused in a criminal proceeding. Kerr, *Lifting the Fog*, at 807, 817; *see* 18 U.S.C. §§ 2515, 2518(10)(a), 2712(d). Moreover, the statute only authorizes civil actions against the United States in cases of "willful" violation of the SCA. 18 U.S.C. § 2712(a). Accordingly, criminal defendants have little incentive to litigate violations of the SCA. The dearth of decisions in the United States Courts of Appeals is simply a reflection of the fact that the statute lacks a suppression remedy; it is not an accurate reflection of the SCA's importance.

The Court should not, therefore, let this confusion linger. The question presented is simply too important, and opportunities to answer it too rare. Rather, the Court should resolve "the growing number of conflicting federal and state decisions on this [federal statutory] issue." *St. Martin Evangelical Lutheran Church* v. *South Dakota*, 451 U.S. 772, 780 (1981).

II. THE MEANING OF ELECTRONIC STORAGE IS AN IMPORTANT, RECURRING FEDERAL STATUTORY ISSUE.

The SCA is the basic federal law protecting the privacy of Americans' e-mail, and the definition of electronic storage is a central component of that law. As one treatise has put it, "whether a communication is in electronic storage or not, can be crucial in determining what level of legal process the government must present before acquiring access to stored communications." 1 J. Carr & P. Bellia, *The Law of Electronic Surveillance* § 4:76, at 541 (2012). And yet the courts are in utter disarray over how to interpret that definition.

E-mail is ubiquitous. According to one estimate, 107 *trillion* e-mails were sent worldwide in 2010 alone. Woodrow Hartzog, *Chain-Link Confidentiality*, 46 Ga. L. Rev. 657, 679 n.89 (2012). As of 2009, the four most popular providers of web-based e-mail served 226.4 million users in the United States, accounting for about 73.5% of the population. Kory R. Watson, Note, *Unauthorized Access to Web-Based E-Mail*, 35 S. ILL. U. L.J. 543, 543 (2011). Whether—and under what circumstances—the government can access personal, confidential messages in these hundreds of millions of Americans' email accounts hinges on the outcome of this case.

Were the Court to grant *certiorari*, the consequences of its decision would be felt hundreds of times every day. For example, in the six-month period between January and June of 2012, Google (which operates Gmail, one of the most popular web-based e-mail services) received 7,969 requests from the U.S. government to turn over user data. *See*

Google Transparency Report.[8] Those requests covered 16,281 separate user accounts. *Id.* That amounts to requests for data from almost 90 accounts *per day*—and that is just from Google. The outcome of those requests will often turn on the interpretation of the SCA. And the "number of requests [Google] receives for user account information as part of criminal investigations has increased year after year." *Id.*[9] The question presented in this case will determine whether the government needs a search warrant for many of those requests.

The question is not only vitally important; it also concerns an area of law where there is a special need for uniformity. Customers of e-mail providers are scattered throughout the country. To have the SCA mean different things in different places makes complying with the government's many requests extremely burdensome. Indeed, "[m]any Internet companies * * * acknowledge that access to information is important for fighting crime and terrorism, but say they are dealing with a patchwork of confusing standards that have been interpreted inconsistently by the courts, creating uncertainty." Miguel Heft & Claire Cain Miller, *1986 Privacy Law Is Outrun by Web*, N.Y. Times, Jan. 10, 2011, at A1. That kind of legal uncertainty imposes significant burdens on the entire technology industry.

This uncertainty is amplified by the lack of clarity not only as to what the law is, but also as to what

---

[8] *Available at* http://www.google.com/transparencyreport/userdatarequests/.

[9] *Available at* http://www.google.com/transparencyreport/userdatarequests/US/?p=2012-06.

jurisdiction's law even applies. *United States* v. *Weaver* is illustrative of the confusion. There, the government sought to compel compliance with a subpoena. 636 F. Supp. 2d at 770. The district court, located in the Seventh Circuit, held that it was *not* bound by the Ninth Circuit's decision in *Theofel*, even though Microsoft (the e-mail provider in the case) and its servers were located in the Ninth Circuit. The meaning of the SCA—and the strength of its privacy protections—should not vary based on where the litigation arises, where the individuals accessed their email accounts, whether the email account is a web-based Yahoo account or a software based Outlook account, or where a particular server is located. The kind of dynamic that the Internet presents—especially as we are moving to an era of cloud computing—"creates a strong need for a uniform reading of the statute" everywhere in the Nation. Kerr, *Split with Ninth Circuit*, *supra*.

The current disarray of reasoning and decisions is not only burdensome for companies that provide e-mail services; it is also burdensome to law enforcement. As the Justice Department's manual on searching and seizing electronic evidence states, "[a]gents and prosecutors must apply the various classifications devised by the SCA's drafters to the facts of each case to figure out the proper procedure for obtaining the information sought." DOJ Manual 116. And "the definition of 'electronic storage' is important because * * * contents in 'electronic storage' for less than 181 days can be obtained only with a warrant." *Id.* at 123. Thus it is no surprise that the manual calls the "split between two interpretations of 'electronic storage'" resulting from

Theofel "[u]nfortunate[]." *Id.* The Court should step in to relieve this headache for law enforcement.

Finally, this issue is important to ordinary Americans. E-mail is pervasive in modern life, and the number of communications in the cloud is staggering. Users of Gmail, Hotmail, Yahoo, Dropbox, text messages, and Facebook—just to name a few common providers—could all be affected. Given the uncertain application of the Fourth Amendment, the SCA is the critical source of the "right of the people to be secure" in these domains. *See* U.S. Const. amend. IV. Moreover, Americans must comply with the criminal prohibition of section 2701; the present uncertainty means that whether certain conduct is a crime can turn on the happenstance of geography.

* * *

In short, this statutory interpretation question is poised for review. While the vast majority of Americans use e-mail and other forms of cloud computing, the rules governing how and when private parties and law enforcement can access or disclose these communications are unsettled and conflict from jurisdiction to jurisdiction. This creates tremendous burdens for Internet service providers, law enforcement, and all of us who send and receive emails.

III. THE DECISION BELOW CONTRAVENES THE TEXT AND PURPOSE OF THE STORED COMMUNICATIONS ACT.

Furthermore, the decision below is wrong. It cannot be squared with the text and purpose of the SCA. The majority of Justices below held that subsection (B) of the definition of "electronic storage"

refers only to backups made by e-mail providers for their own administrative purposes. Pet. App. 15a-16a, 18a. There are at least three flaws with this reading.

1. As an initial matter, it is not supported by the plain text of the statute. Subsection (B) covers e-mails stored "for purposes of backup protection." Nothing in the text specifies that the relevant "purpose" is that of the e-mail provider, and the decision below offers no persuasive reason why the definition should be so circumscribed. Rather, "backup protection" plainly refers to the purpose of the user *or* the provider. Moreover, whether or not an e-mail has already been read has no bearing on whether it is a "backup"; if anything, an e-mail is *more* likely to be a backup once it has been read. Finally, subsection (B) does not textually distinguish between "intermediate" and post-transmission storage, as does subsection (A). There is no warrant for importing that limitation into subsection (B). E-mails are often read only minutes after they have been sent; the SCA would be gravely undermined if its privacy protections were so fleeting. Plainly read, subsection (B) does not narrow the scope of electronic storage as the Department of Justice and decision below suggest.

The United States, in *Theofel*, countered that, because subsection (B) refers to storage of "*such* communications," it applies only to communications that already meet the definition of subsection (A) by being in temporary, intermediate storage. Not so. "Subsection (A) identifies a type of communication ('a wire or electronic communication') and a type of storage ('temporary, intermediate storage * * * incidental to the electronic transmission thereof').

The phrase 'such communication' in subsection (B) does not, as a matter of grammar, reference attributes of the type of storage defined in subsection (A)." *Theofel*, 359 F.3d at 1076. The phrase means only that the communication must be of the proper type—wire or electronic, such as an e-mail. The government might have an argument if subsection (B) read "a communication in such storage"; as it is, "'such communication' is nothing more than shorthand for a 'wire or electronic communication.'" *Id.*

2. The second flaw in the decision below is that it renders subsection (B) surplusage. It is a well-established canon of interpretation that a "'statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous, void or insignificant.'" *Corley* v. *United States*, 556 U.S. 303, 314 (2009) (citation omitted). Both the decision below and the DOJ's "traditional interpretation" flout that canon: they "drain[] subsection (B) of independent content." *Theofel*, 359 F.3d at 1076. A backup made by an e-mail provider in the course of transmission would already qualify as "temporary, intermediate storage" under subsection (A). So subsection (B) would add nothing.

3. The third flaw is that the decision below (and the Justice Department's view) results in the anomalous consequence that *non-content* records receive *more* protection than the content of messages sent and received. The government needs either a warrant or a 2703(d) order to compel an e-mail provider to turn over the non-content records of a user. 18 U.S.C. § 2703(c). Under the government's reading of the statute, however, a simple subpoena would suffice to compel production of the contents of e-mails once

they have been read. Non-content records include things like the address of the intended recipient, or the date and time a message was sent. They are similar to the writing on the outside of an envelope. It is inconceivable that Congress, attempting to revitalize the Fourth Amendment, would make it *harder* for the government to read the envelope than the letter.

4. Two Justices below, like the district court in *Weaver*, held that even assuming the correctness of *Theofel*, the definition of "electronic storage" is not applicable to storage by web-based e-mail providers. Rather, it only includes e-mail providers that must be used in conjunction with software like Outlook or Lotus Notes. The reason for the distinction is that "[u]sers of web-based e-mail systems * * * default to saving their message only on the remote system." *Weaver*, 636 F. Supp. 2d at 772. Outlook and similar programs, by contrast, download a copy of an e-mail onto a user's own machine. Since it is possible (the argument goes) that a user of a web-based e-mail service has not downloaded copies of her messages from the provider's server to her own machine, post-transmission copies are not stored "for purposes of backup protection." That is because a backup "presupposes the existence of another copy." Pet. App. 7a.

That argument leads to absurd and unworkable results. *American Tobacco Co.* v. *Patterson*, 456 U.S. 63, 71 (1982) ("Statutes should be interpreted to avoid untenable distinctions and unreasonable results whenever possible."). It would make no sense for the question of whether an e-mail should receive protection to hinge on the use of a program such as Outlook. Indeed, if the only copy of an e-mail were

online, it would be considerably *worse* if someone were to hack into an account to delete it or "prevent[ ] authorized access" to it. 18 U.S.C. § 2701(a). Yet, under the reasoning below, a hacker could do that with impunity under the SCA.

Moreover, the reasoning of these two Justices does not even succeed in protecting law enforcement interests. It would require the government and Internet service providers to ascertain *how* an e-mail user reads her e-mails to know whether a warrant is needed. If she uses Outlook or Lotus Notes (which is perfectly possible with a web-based provider), the government would need a warrant; if not, a subpoena would suffice. But this information would be difficult, if not impossible, for law enforcement to obtain in advance. Additionally, this reading is totally unworkable given the prevalence of smartphones. Many people use web-based e-mail services in conjunction with a handheld device like an iPhone or Blackberry. These devices *do* download copies of e-mails. The government thus would also be forced to determine whether a suspect uses a smartphone, and whether the smartphone still retains a copy of the e-mail being sought, in order to know whether a warrant is required. The uncertainty and strain would increase when an e-mail has multiple recipients and only some have opened the message, or when one recipient opts to "mark" the e-mail as "unread" after reading it. Given these totally unworkable possibilities, the simpler rule is the far better choice: any e-mail in storage by a web-based e-mail provider, read or unread, is in "electronic storage."

Additionally, the ordinary meaning of "backup" does not presuppose the existence of another copy.

The dictionary definition of backup is "a copy of computer data." Merriam-Webster's Collegiate Dictionary (11th ed. 2011). An e-mail stored with a web-based e-mail provider is as much a "copy of computer data" as an e-mail stored by a traditional e-mail server. If one were to write a letter with a carbon copy, the carbon copy would not cease to be a "copy" merely because the recipient threw out the original on arrival. Likewise, an e-mail stored by a web-based e-mail service is a "copy of electronic data" whether or not one uses a program like Outlook to download another copy to a personal computer.

5. Finally, the SCA should be interpreted to cover opened e-mails stored with a web-based provider because of the canon of constitutional avoidance. The U.S. Court of Appeals for the Sixth Circuit in *United States* v. *Warshak*, 631 F.3d 266 (2010), has held that an e-mail user "enjoys a reasonable expectation of privacy in the contents of e-mails" stored by an e-mail provider, and that the government may not compel a provider "to turn over the contents of a subscriber's e-mail without first obtaining a warrant based on probable cause." *Id.* at 288. The Sixth Circuit further held that, "to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional." *Id.* The Petitioner's reading of the statute alleviates the constitutional vulnerabilities of the SCA: all e-mails stored by an e-mail provider can only be accessed pursuant to a warrant based on probable cause, at least for 180 days or fewer.

CONCLUSION

The decision below creates a clear split with the Ninth Circuit on an exceptionally important federal statute. The dizzying array of inconsistent readings of that statute is burdensome to technology companies, law enforcement, and individual citizens trying to keep their private emails private.

The petition for a writ of certiorari should be granted.

Respectfully submitted,

MAX N. PICKELSIMER
CARRIE A. WARNER
WARNER, PAYNE & BLACK, LLP
1531 Blanding Street
Columbia, SC 29201
(803) 799-0554

NEAL KUMAR KATYAL*
JESSICA L. ELLSWORTH
JORDAN ESTES
HOGAN LOVELLS US LLP
555 13th Street, N.W.
Washington, D.C. 20004
(202) 637-5528
neal.katyal@hoganlovells.com

Counsel for Petitioner
**Counsel of Record*

January 2013

APPENDICES

APPENDIX A

THE STATE OF SOUTH CAROLINA
IN THE SUPREME COURT

M. LEE JENNINGS,
Respondent,
v.
GAIL M. JENNINGS, HOLLY BROOME,
BRENDA COOKE, INDIVIDUALLY
AND
BJR INTERNATIONAL DETECTIVE AGENCY, INC.,
OF WHOM HOLLY BROOME IS,
Petitioner.

ON WRIT OF CERTIORARI TO THE COURT OF APPEALS

Appeal from Richland County
L. Casey Manning, Circuit Court Judge

Opinion No. 27177
Heard October 18, 2011 — Filed October 10, 2012

REVERSED: Gary W. Popwell, Jr., of Lee Eadon Isgett & Popwell, of Columbia, for Petitioner. Max N. Pickelsimer and Carrie A. Warner, both of Warner, Payne & Black, of Columbia, for Respondent.

JUSTICE HEARN: Holly Broome was sued civilly for hacking Lee Jennings' Yahoo! e-mail account. The circuit court granted summary judgment in favor of Broome on all claims, including violation of the federal Stored Communications Act (SCA), 18 U.S.C. §§ 2701-12. The court of appeals reversed, finding that the e-mails she obtained from hacking Jennings' account were in electronic storage and thus covered by the SCA. We reverse.

FACTUAL/PROCEDURAL BACKGROUND

The computer hacking at issue here emanated from a domestic dispute. After finding a card for flowers for another woman in her husband's car, Gail Jennings confronted him. Jennings confessed he had fallen in love with someone else, and although he refused to divulge her name, he admitted the two had been corresponding via e-mail for some time. Gail confided this situation to her daughter-in-law, Holly Broome.[1] Broome had previously worked for Jennings and knew he maintained a personal Yahoo! e-mail account. She thereafter accessed his account by guessing the correct answers to his security questions and read the e-mails exchanged between Jennings and his paramour. Broome then printed out copies of the incriminating e-mails and gave them to Thomas Neal, Gail's attorney in the divorce proceedings, and Brenda Cooke, a private investigator Gail hired.

When Jennings discovered his e-mail account had been hacked, he filed suit against Gail, Broome, and Cooke, individually and as shareholder of BJR International Detective Agency, Inc., for invasion of

[1] Broome is married to Gail's son from a previous marriage.

privacy, conspiracy, and violations of the South Carolina Homeland Security Act, South Carolina Code Ann. § 17-30-135 (2010). He later amended his complaint to include an allegation that the defendants violated the SCA. Jennings also moved to add Neal as a defendant. The circuit court denied this motion and granted summary judgment in favor of the defendants on all claims, including the allegations under the SCA. Jennings appealed. The court of appeals affirmed the grant of summary judgment as to Gail, Cooke, and BJR. *Jennings v. Jennings,* 389 S.C. 190, 209, 697 S.E.2d 671, 681 (Ct. App. 2010). However, the court reversed the circuit court's grant of summary judgment in favor of Broome only as to the SCA claim, finding that the e-mails at issue were in "electronic storage" as defined in 18 U.S.C. § 2510(17). *Id* at 198-208, 697 S.E.2d at 675-680. We granted certiorari.

ISSUE PRESENTED

Did the court of appeals err in reversing the circuit court's grant of summary judgment because the e-mails in question were not in "electronic storage" as defined by 18 U.S.C. § 2510?[2]

LAW/ANALYSIS

In arguing the court of appeals erred by holding the e-mails were in electronic storage, Broome contends the court misunderstood the definition of electronic storage under the Act and incorrectly concluded the e-mails had been stored for the purpose of backup protection. We agree.

---

[2] The definitions of section 2510 pertaining to the Wiretap Act are incorporated into the SCA. 18 U.S.0 § 2711(1).

"Determining the proper interpretation of a statute is a question of law, and this Court reviews questions of law de novo." *Town of Summerville v. City of N. Charleston,* 378 S.C. 107, 110, 662 S.E.2d 40, 41 (2008). "Statutory construction must begin with the language of the statute." *Kofa* v. *U.S. Immigration & Naturalization Serv.,* 60 F.3d 1084, 1088 (4th Cir. 1995). "In interpreting statutory language, words are generally given their common and ordinary meaning." *Nat'l Coal. for Students with Disabilities Educ. & Legal Def. Fund v. Allen,* 152 F.3d 283, 288 (4th Cir. 1998). Where the language of the statute is unambiguous, the Court's inquiry is over, and the statute must be applied according to its plain meaning. *Hall v. McCoy,* 89 F. Supp. 2d 742, 745 (W.D. Va. 2000).

Under section 2701(a) of the SCA, anyone who:

> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
>
> (2) intentionally exceeds an authorization to access that facility;
>
> and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

18 U.S.C. § 2701(a). This section thus proscribes the unauthorized accessing of an electronic communication while it is in "electronic storage." The SCA defines "electronic storage" as "(A) any

temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for the purposes of backup protection of such communication." 18 U.S.C. § 2510(17). For Jennings to succeed in his claim against Broome under the SCA, he must prove the e-mails she accessed were in electronic storage as defined in section 2510(17). His argument in this regard extends only to subsection (B) of the Act; Jennings has never argued that the e-mails in questions were in electronic storage pursuant to subsection (A).

The court of appeals agreed with Jennings and held the e-mails were in "electronic storage" because they were stored for backup protection pursuant to subsection (B). Broome argues this conclusion was based upon an improper interpretation of section 2510(17), asserting that the definition of "electronic storage" within the SCA requires that it must be both temporary and intermediate storage incident to transmission of the communication *and* storage for the purposes of backup protection. She therefore contends that an e-mail must meet both subsection (A) and subsection (B) to be covered by the SCA. We acknowledge that this reading is the interpretation espoused by the Department of Justice as the "traditional interpretation" of section 2510(17). However, it has been rejected by the majority of courts in favor of a construction that an e-mail can be in electronic storage if it meets either (A) *or* (B). *See, e.g., Theofel v. Farey-Jones,* 359 F.3d 1066, 1075 (9th Cir. 2004); *Fraser v. Nationwide Mut. Ins. Co.,* 352 F.3d 107, 114 (3d Cir. 2003), *affg in part, vacating in part, and remanding* 135 F. Supp. 2d 623

(E.D. Pa. 2001); *Strategic Wealth Group, LLC v. Canno,* No. 10-0321, 2011 WL 346592, at *3-4 (E.D. Pa. Feb. 4, 2011); *Cornerstone Consultants, Inc. v. Prod. Input Solutions, LLC,* 789 F. Supp. 2d 1029, 1055 (N.D. Iowa 2011); *Shefts v. Petrakis,* No. 10-cv-1104, 2011 WL 5930469, at *5 (C.D. Ill. Nov. 29, 2011); *Crispin v. Christian Audigier, Inc.,* 717 F. Supp. 2d 965, 983 (C.D. Cal. 2010); *U.S. v. Weaver,* 636 F. Supp. 2d 768, 771 (C.D. Ill. 2009); *Flagg v. City of Detroit,* 252 F.R.D. 346, 362 (E.D. Mich. 2008). Because Jennings has only argued his e-mails were in electronic storage pursuant to subsection (B), it is unnecessary for us to determine whether to adopt the traditional interpretation advocated by the Department of Justice or the interpretation recognized by these cases. *See McCall v. Finley,* 294 S.C. 1, 4, 362 S.E.2d 26, 28 (Ct. App. 1987) ("[W]hatever doesn't make any difference, doesn't matter.").

In finding the e-mails were stored for "purposes of backup protection" and thus subject to subsection (B), the court of appeals relied heavily on *Theofel,* a case from the United States Court of Appeals for the Ninth Circuit. In *Theofel,* Integrated Capital Associates (ICA) was involved in commercial litigation with Farey-Jones. *Theofel,* 359 F.3d at 1071. Counsel for Farey-Jones subpoenaed ICA's internet service provider, NetGate, for the production of all e-mails sent or received by anyone at ICA "with no limitation as to time or scope." *Id.* NetGate complied as well as it could with such a voluminous request, but when ICA discovered this disclosure it filed a motion to quash the subpoena and requested the imposition of sanctions. *Id.* Additionally, several of the employees whose e-mails

had been delivered by NetGate filed a civil suit against Farey-Jones for, *inter alia,* violations of the SCA in gaining unauthorized access to communications in electronic storage. *Id.* The court in *Theofel* held that ICA's e-mails which had been received and read, and then left on the server instead of being deleted, could be characterized as being stored "for purposes of backup protection" and therefore kept in electronic storage under subsection (B). *Id* at 1075. We question the reasoning expressed in *Theofel* that such passive inaction can constitute storage for backup protection under the SCA; however, because we believe the plain language of subsection (B) does not apply to the e-mails in question, we reverse the conclusion of the court of appeals that they were in electronic storage under *Theofel.*

After opening them, Jennings left the single copies of his e-mails on the Yahoo! server and apparently did not download them or save another copy of them in any other location. We decline to hold that retaining an opened email constitutes storing it for backup protection under the Act. The ordinary meaning of the word "backup" is "one that serves as a substitute or support." Merriam-Webster Dictionary, http://www.merriam-webster.com/dictionary/backup. Thus, Congress's use of "backup" necessarily presupposes the existence of another copy to which this e-mail would serve as a substitute or support. We see no reason to deviate from the plain, everyday meaning of the word "backup," and conclude that as the single copy of the communication, Jennings' e-mails could not have been stored for backup protection.

Accordingly, we find these e-mails were not in electronic storage. We emphasize that although we reject the contention that Broome's actions give rise to a claim under the SCA, this should in no way be read as condoning her behavior. Instead, we only hold that she is not liable under the SCA because the e-mails in question do not meet the definition of "electronic storage" under the Act.

CONCLUSION

Based on the foregoing, we reverse the court of appeals' opinion and reinstate the circuit court's order granting summary judgment in favor of Broome.

KITTREDGE, J., concurs. TOAL, C.J., concurring in result in a separate opinion in which BEATTY, J., concurs. PLEICONES, J., concurring in result in a separate opinion.

CHIEF JUSTICE TOAL: I concur in result, but write separately to express my concern with Justice Hearn's adoption of the approach taken in *United States v. Weaver,* 636 F. Supp. 2d 769 (C.D. Ill. 2009). I believe the "traditional interpretation" of the Stored Communications Act (SCA), 18 U.S.C. §§ 2701-12 (2000 & Supp. 2011), advanced by the Department of Justice (DOJ), coupled with the fact that Congress never contemplated this new form of technology, provide a sounder basis to reach our decision.

In *Weaver,* the court addressed the government's subpoena of e-mails in a defendant's Hotmail account and whether the e-mails were in "electronic storage," a determination which would dictate whether the government would need to obtain a warrant for the e-mails or whether a trial subpoena was sufficient. 636 F. Supp. 2d at 769-71. *Weaver* held that courts may issue a trial subpoena to compel internet service providers (ISPs) to produce the content of opened e-mails stored by a website provider for 180 days or fewer because such e-mails are not in "electronic storage." *Id* at 71-73. *Weaver* relied on dicta found in *Theofel v. Farey-Jones,* 359 F.3d 1066 (9th Cir. 2004), to conclude that *Theofel's* holding applies only to e-mail systems where users download messages from the ISP's server onto their computers, and that e-mails stored in the cloud should not be considered stored for backup purposes. *Id.* at 72. Similar to *Weaver,* Justice Hearn concludes here that because Jennings left his e-mails on the Yahoo! Server and apparently did not download them from the server or retain a copy of them in any other location, the emails could not be held for "backup protection" within the meaning of the statute.

Justice Hearn relies on the Merriam-Webster Dictionary to argue that the definition of "backup" requires that there must be more than one copy of the email. The exact definition of "backup" varies from dictionary to dictionary. *See, e.g., Webster's Third International Dictionary, Unabridged* 120 (3rd ed. 2002). Assuming for the sake of analysis that the definition of "backup" is "one that serves as a substitute *or support,"* as Justice Hearn contends, this definition would suggest that an email message on an ISP's server could be stored for *support* in the event that the user needs to retrieve it. As such, even if there is no second copy, the email could still constitute "backup protection."

Nevertheless, even if I could interpret "backup" in this matter, in a statute such as this, I am reluctant to read the word "backup" in isolation, but instead the phrase "backup protection" should be viewed in a statutory and historical context. As Professor Kerr explains:

> An understanding of the structure of the SCA indicates that the backup provision of the definition of electronic storage, *see id.* § 2510(17)(B), exists only to ensure that the government cannot make an end-run around the privacy-protecting ECS rules by attempting to access backup copies of unopened e-mails made by the ISP for its administrative purposes. ISPs regularly generate backup copies of their servers in the event of a server crash or other problem, and they often store these copies for the long term. Section 2510(17)(B) provides that backup copies of unopened e-mails are protected by

> the ECS . . . .
>
> There are many statutory signals that support this reading. Several were raised by the United States as amicus and rejected by the *Theofel* court, *see Theofel*, 359 F.3d at 1076-77, but a host of other arguments remain. I think the most obvious statutory signal is the text of 18 U.S.C. § 2704, entitled "Backup Preservation." See 18 U.S.C. § 2704 (2000). Section 2704 makes clear that the SCA uses the phrase "backup copy" in a very technical way to mean a copy made by the service provider for administrative purposes. *See id.* The statutory focus on backup copies in the SCA was likely inspired by the 1985 Office of Technology Assessment report that had helped inspire the passage of the SCA. *See* Office of Tech. Assessment, Federal Government Information Technology: Electronic Surveillance and Civil Liberties (1985). The report highlighted the special privacy threats raised by backup copies, which the report referred to as copies "[r]etained by the [e]lectronic [m]ail [c]ompany for [a]dministrative [p]urposes." *Id.* at 50.

Orin Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It,* 72 Geo. Wash. L. Rev. 1208, 1217 n.61 (2004); *see also Pure Power Boot Camp v. Warrior Fitness Boot Camp,* 587 F. Supp. 2d 548, 555 (S.D.N.Y. 2008) ("The majority of courts which have addressed the issue have determined that e-mail stored on an electronic communication service provider's systems after it has been delivered, as

opposed to e-mail stored on personal computer, is a stored communication subject to the SCA.") (citations omitted).

Furthermore, I am concerned that Justice Hearn's position on "backup protection" potentially leads to illogical results. *Weaver,* itself, concluded that the outcome would be different if a Hotmail user "opt[ed] to connect an e-mail program, such as Microsoft Outlook, to his or her Hotmail account and through it download[ed] messages onto a personal computer." *Id.* Under *Weaver's* rule, the privacy protections of personal e-mail are contingent upon the operation of the e-mail system used.[3] It is not necessary for this Court to rely on *Theofel* dicta, which would lead us

---

[3] *Theofel* stated in dicta, "A remote computing service might be the only place a user stores his messages; in that case, the messages are not stored for backup purposes." 359 F.3d at 1077. Relying on this, *Weaver* distinguished *Theofel* and claimed that it does not apply to web-based e-mail services where e-mails are stored in the cloud. 636 F. Supp. 2d at 771-73. Nevertheless, being stored in the cloud just means that the e-mails are stored on a Yahoo Mail server. *See Accessing Yahoo! Mail* (March 8, 2012), *available at* www.help.yahoo.com/tutorials/. The distinction between being stored on a Yahoo! Mail Server and being stored on the ISP's server in *Theofel* in the context of backup storage is slight in my view. *Compare id. with Theofel,* 359 F.3d at 1070, 1075. In addition, based on its dicta, *Theofel* never explicitly excluded web-based e-mails but spoke of "remote computing service[s]." Some courts, including our court of appeals, have concluded that web-based e-mail services like Yahoo! provide both electronic communication services (ECS) and remote computing service (RCS) making it problematic to rely on *Theofel's* dicta to exclude web-based e-mails as *Weaver* has done. *See, e.g., In re Application of the U.S. for a Search Warrant, for Contents of Elec. Mail and for an Order Directing a Provider of Elec. Commc'n Servs. to Not Disclose the Existence of the Search Warrant,* 665 F. Supp. 2d 1210, 1214 (D. Or. 2009).

down the precarious path of saying that if one uses Microsoft Outlook for e-mail, one will be protected, but if one uses Yahoo! Mail for e-mail, there is no protection. *Griffin v. Oceanic Contractors, Inc.,* 458 U.S. 564, 575, 102 S. Ct. 3245, 3252 (1982) (holding "interpretations of a statute which would produce absurd results are to be avoided if alternative interpretations consistent with the legislative purpose are available."); *see also Hodges v. Rainey,* 341 S.C. 79, 91, 533 S.E.2d 578, 584 (2000) (citation omitted) ("However plain the ordinary meaning of the words used in a statute may be, the courts will reject that meaning when to accept it would lead to a result so plainly absurd that it could not possibly have been intended by the Legislature . . . .").

Instead, I advocate a rejection of *Theofel* entirely and the adoption of the "traditional interpretation" of the SCA, which tracks the statutory language and comports with legislative history. *Prosecuting Computer Crimes,* DOJML Comment 9-3.000, 5 Department of Justice Manual (Supp. 2011-13) *[hereinafter* DOJML Comment 9-3.000]; *see also* Kerr, *supra,* at 1216-18 (advocating the traditional approach and arguing that "the Ninth Circuit's analysis in *[Theofel]* is quite implausible and hard to square with the statutory text"). Under this approach, the term "electronic storage" has a narrow, statutorily defined meaning. DOJML Comment 9-3.000. It does not simply mean storage of information by electronic means. Rather section 2510(17) provides:

> (17) "electronic storage" means—
>
> > (A) any temporary, intermediate storage of a wire or electronic

> communication incidental to the electronic transmission thereof; *and*
>
> **(B)** any storage of such communication by an electronic communication service for purposes of backup protection of such communication;

18 U.S.C. § 2510(17) (Supp. 2011) (emphasis added).

I disagree with Justice Hearn's position that an e-mail is covered under section 2701(a) of the SCA if it meets the criteria of "either subsection (A) *or* subsection (B)." (emphasis in original). Plainly read, the definition of electronic storage encompasses both subsections A and B. I do not rely on Broome's over-analysis of the word "such" in the phrase "such communication" to reach this conclusion. Rather, I turn to the structure of the statutory text and also to the unambiguous use of the conjunctive "and." Both subsections A and B are subsumed under section 17, which starts out with the phrase "'electronic storage' means—," suggesting that the definition of electronic storage encompasses both subsections A and B. Furthermore, subsections A and B are connected by the conjunctive "and" indicating that they must be read together. *See Bruesewitz v. Wyeth LLC,* 562 U.S. ____, 131 S. Ct. 1068, 1078 (2011) (noting that "linking independent ideas is the job of a coordinating junction like 'and"). Had Congress intended two alternative definitions for electronic storage then it would have used the disjunctive particle "or" in place of "and." *See, e.g., Reiter v. Sonotone Corp.,* 442 U.S. 330, 339, 99 S. Ct. 2326,

2331 (1979) ("Canons of construction ordinarily suggest that terms connected by a disjunctive be given separate meanings, unless the context dictates otherwise."); *K & A Acquisition Group, LLC v. Island Pointe, LLC,* 383 S.C. 563, 580, 682 S.E.2d 252, 261 (2009) (The "use of the word 'or' in a statute 'is a disjunctive particle that marks an alternative."). Justice Hearn's approach would delete a word and insert a new one into the statutory text, effectively writing out subsection A from the definition of electronic storage.

Thus, in my view, electronic storage refers only to temporary storage, made in the course of transmission, by an ECS provider, *and* to backups of such intermediate communications. Under this interpretation, if an e-mail has been received by a recipient's service provider but has not yet been opened by the recipient, it is in electronic storage. *Steve Jackson Games, Inc. v. United States Secret Serv.,* 36 F.3d 457, 461 (5th Cir. 1994) (holding that e-mail which had been sent to a bulletin board but not read by intended recipients was "in 'electronic storage"). When the recipient opens the e-mail, however, the communication reaches its final destination. DOJML Comment 9-3.000. If the recipient chooses to retain a copy of the e-mail on the service provider's system, the retained copy is no longer in electronic storage because it is no longer in "temporary, intermediate storage . . . incidental to . . . electronic transmission." *Fraser v. Nationwide Mut. Ins. Co.,* 135 F. Supp. 2d 623, 635-36 (E.D. Pa. 2001), *affd in part* 352 F.3d 107, 114 (3d Cir. 2004) (upholding district court's ruling on other grounds); *In re Doubleclick Inc. Privacy Litigation,* 154 F. Supp. 2d 497, 511-13 (S.D.N.Y. 2001) (emphasizing

that electronic storage should have a narrow interpretation based on statutory language and legislative intent and holding that cookies fall outside of the definition of electronic storage because of their "long-term residence on plaintiffs' hard drives").

In this case, the circuit court judge found that the e-mails were "received, opened and read by [Jennings] . . . ." Because the e-mails were already opened by Jennings when they were retrieved and printed out by Broome, they reached their final destination and fell outside the scope of the definition of electronic storage under the statute, which requires the e-mails to be in "temporary, intermediate storage . . . incidental to the electronic transmission thereof." 18 U.S.C. § 2510(17).

Much of the difficulty in applying the SCA to cases such as this arises because of the discrepancy between current technology and the technology available in 1986 when the SCA was first enacted. When the SCA was enacted, the process of network communication was still in its infancy; the World Wide Web, and the Internet as we know it, did not arrive until 1990. William Jeremy Robison, *Free At What Cost?: Cloud Computing Privacy Under the Stored Communications Act,* 98 Geo. L.J. 1195, 1198 (2010). An examination of how the Senate viewed e-mails in 1986 indicates just how strikingly different the technology was compared to the present:

> Electronic mail is a form of communication by which private correspondence is transmitted over public and private telephone lines. In its most common form, messages are typed into a computer terminal, and then transmitted over

> telephone lines to a recipient computer operated by an electronic mail company. If the intended addressee subscribes to the service, the message is stored by the company's computer "mail box" until the subscriber calls the company to retrieve its mail, which is then routed over the telephone system to the recipient's computer. If the addressee is not a subscriber to the service, the electronic mail company can put the message onto paper and then deposit it in the normal postal system.

S. Rep. No. 99-541, at 7 (1986). Viewing the statutory language of the SCA in this context, the traditional definition of electronic storage becomes more reasonable. The SCA is ill-fitted to address many modern day issues, but it is this Court's duty to interpret, not legislate. Moreover, I agree with Justice Hearn that it is prudent to limit our analysis to the language before us and give the language its literal meaning. However, I believe doing so requires us to adopt the traditional interpretation of 18 U.S.C. § 2510(17) rather than rely on the reasoning advanced by *United States v. Weaver.* 636 F. Supp. 2d at 769-73. Jennings and similarly situated plaintiffs are not foreclosed from seeking redress by alternative theories, but under the SCA, Broome's actions do not give rise to a claim because the e-mails in question do not meet the definition of electronic storage.

BEATTY, J., concurs.

JUSTICE PLEICONES: I concur in result. I agree with Chief Justice Toal that "electronic storage" under the Stored Communications Act (SCA) refers to temporary storage of communications during the course of transmission, 18 U.S.C. § 2510(17)(A), and to backups of those communications, § 2510(17)(B). However, I view these two types of storage as necessarily distinct from one another: one is temporary and incidental to transmission; the other is a secondary copy created for backup purposes by the service provider.[4] Therefore, an e-mail is protected if it falls under the definition of either subsection (A) or (B). It does not end the inquiry to find that the e-mails at issue were not in temporary storage during the course of transmission (subsection (A)). Accordingly, because the e-mails in this case were also not copies made by Jennings's service provider for purposes of backup (subsection (B)), they were not protected by the SCA.[5] I therefore concur in result.

---

[4] The "backup" covered by subsection (B) is a copy made by the service provider to back up its own servers. It does not include an original e-mail that has been transmitted to the recipient and remains on the provider's server after the recipient has opened or downloaded it. *See Orin Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It,* 72 Geo. Wash. L. Rev. 1208, 1217 n.61 (2004), quoted by Chief Justice Toal, *supra* (noting the technical meaning of "backup copy" as used in the SCA); *Powerex Corp. v. Reliant Energy Services, Inc.,* 551 U.S. 224, 232 (2007) ("A standard principle of statutory construction provides that identical words and phrases within the same statute should normally be given the same meaning.").

[5] Thus, I agree with Justice Hearn that we must interpret the language of subsection (B) and with her conclusion that the e-mails in this case were not protected.

APPENDIX B

THE STATE OF SOUTH CAROLINA
IN THE COURT OF APPEALS

M. LEE JENNINGS,
Appellant,

v.

GAIL M. JENNINGS, HOLLY BROOME,
BRENDA COOKE, INDIVIDUALLY
AND
BJR INTERNATIONAL DETECTIVE AGENCY, INC.,
Respondent.

Appeal from Richland County
L. Casey Manning, Circuit Court Judge

Opinion No. 4711
Heard April 15, 2010 — Filed July 14, 2010

AFFIRMED IN PART, REVERSED IN PART, AND REMANDED

Max N. Pickelsimer and Carrie A. Warner, both of Columbia, for Appellant.

Deborah Harrison Sheffield, Richard Giles Whiting,

Gary W. Popwell, Jr. and John K. Koon, all of Columbia, for Respondents.

GEATHERS, J.: In this appeal, M. Lee Jennings (Husband) contends that the circuit court erred by granting Respondents' motions for summary judgment as to his cause of action for a violation of the Stored Communications Act, 18 U.S.C. §§ 2701-2712 (2006). Husband also argues that the circuit court erred by denying his motion to amend his complaint to add Thomas Neal (Neal) as a party defendant. We affirm in part, reverse in part, and remand for further proceedings.

FACTS/PROCEDURAL HISTORY

On June 21, 2006, Husband's wife, Gail Jennings (Wife), discovered a card for flowers in her car. Suspecting the flowers were not for her, Wife questioned Husband, who had recently borrowed her car, about the card. To Wife's dismay, Husband informed Wife that he had bought the flowers for another woman, with whom he had fallen in love. Although Husband refused to tell Wife the woman's full name, he mentioned that he had been corresponding with her via email at his office. That same day, the couple separated.

A few days later, Wife's daughter-in-law, Holly Broome (Broome), visited Wife at her home.

Wife, who was extremely upset, told Broome about the separation and the conversation she had had with Husband. The next day, Broome, who had previously worked for Husband, logged onto

Husband's Yahoo account from her personal computer by changing Husband's password. Broome proceeded to read emails that had been sent between Husband and his girlfriend. After reading a few of the emails, Broome called Wife, who came over to Broome's home. Broome printed the emails, and she and Wife made copies of them. They then gave one set of the emails to Neal, Wife's divorce attorney, and another set to Brenda Cooke (Cooke), a private investigator from the BJR International Detective Agency, Inc. (BJR) whom Wife had hired.

Broome subsequently logged onto Husband's Yahoo account on five or six additional occasions. Information she obtained about Husband's girlfriend as a result was communicated to Neal and Cooke. According to Broome, she never accessed any of Husband's unopened emails.

On June 29, 2006, Wife initiated an action in family court for divorce and separate support and maintenance. During the course of that litigation, which is still pending, Husband learned that Broome had accessed emails from his Yahoo account and that copies of those emails had been disseminated to Cooke and BJR.

In February 2007, Husband commenced this action against Wife, Broome, Cooke, and BJR, alleging causes of action for invasion of privacy (publicizing of private affairs and wrongful intrusion), conspiracy to intercept and disseminate private electronic communications, and violation of the South Carolina Homeland Security Act, S.C. Code Ann. §§ 17-30-10 to -145 (Supp. 2009) (HSA). The parties filed cross-motions for summary judgment in May 2007.

In June 2007, Husband filed a motion to amend his complaint, which was granted pursuant to a Consent Order to Amend issued July 13, 2007. Later that July, Husband filed his amended complaint, adding allegations of violations of the following statutes: (i) the South Carolina Computer Crime Act (CCA), S.C. Code Ann. §§ 16-16-10 to -40 (2003 & Supp. 2009); (ii) Title I of the Federal Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2510-2522 (2006); and (ill) Title II of the ECPA, 18 U.S.C. §§ 2701-2712 (2006), which is separately known as the Stored Communications Act (SCA).

In February 2008, Wife and Broome each moved again for summary judgment. Thereafter, Husband filed a motion to amend his complaint a second time. Among other things, Husband sought to add Neal as a party defendant.

A hearing regarding the parties' summary judgment motions and Husband's motion to amend his complaint was held in June 2008. At that hearing, Husband voluntarily withdrew his causes of action arising under the HSA, the CCA and Title I of the ECPA, as well as his cause of action for conspiracy.

By an order filed September 24, 2008, the circuit court granted Respondents' motions for summary judgment as to Husband's remaining causes of action, and it denied Husband's motion to amend his complaint. With regard to Husband's claim under section 2701 of the SCA, the circuit court held that Husband had failed to allege all of the elements necessary for a cause of action. Additionally, the circuit court found that Husband was not entitled to

relief under section 2701 because the emails at issue were not in "electronic storage" as that term is defined in 18 U.S.C. § 2510(17) (2006). Furthermore, the circuit court ruled that, even if the emails were in electronic storage, Husband could not recover against Wife or Cooke because their actions did not constitute a violation of section 2701.

Husband subsequently filed a motion to reconsider, which was denied by the circuit court. This appeal followed.

ISSUES ON APPEAL

1. Did the circuit court err in granting Respondents' motions for summary judgment on Husband's cause of action for a violation of the SCA on the ground that Husband failed to allege all of the elements necessary to successfully plead a cause of action under 18 U.S.C. § 2701 (2006)?

2. Did the circuit court err in granting Respondents' motions for summary judgment on Husband's cause of action for a violation of the SCA on the ground that the emails were not in "electronic storage" as defined in 18 U.S.C. § 2510(17) (2006)?

3. Did the circuit court err by not allowing Husband to amend his complaint to add Neal as a party defendant?

STANDARD OF REVIEW

This court reviews the grant of a summary judgment motion under the same standard applied by the trial court under Rule 56(c), SCRCP. *Jackson*

v. Bermuda Sands, Inc., 383 S.C. 11, 14 n.2, 677 S.E.2d 612, 614 n.2 (Ct. App. 2009). Rule 56(c), SCRCP, provides that summary judgment shall be granted where "the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to a judgment as a matter of law." In ascertaining whether any triable issue of fact exists, the evidence and all inferences which can be reasonably drawn from the evidence must be viewed in the light most favorable to the non-moving party. *Belton v. Cincinnati Ins. Co.*, 360 S.C. 575, 578, 602 S.E.2d 389, 391 (2004).

A motion to amend a pleading is normally addressed to the sound discretion of the trial court. *Porter Bros., Inc. v. Specialty Welding Co.,* 286 S.C. 39, 41, 331 S.E.2d 783, 784 (Ct. App. 1985). The trial court's decision will not be overturned "without an abuse of discretion or unless manifest injustice has occurred." *Berry v. McLeod*, 328 S.C. 435, 450, 492 S.E.2d 794, 802 (Ct. App. 1997). The discretion afforded to the trial court in granting or denying an amendment "is so broad that it will rarely be disturbed on appeal." *Porter Bros.,* 286 S.C. at 41, 331 S.E.2d at 784.

DISCUSSION

I. Did the circuit court err in determining that Husband failed to allege all of the elements of a cause of action under section 2701 of the SCA?

Section 2701(a) of the SCA provides:

> Except as provided in subsection (c) of this section whoever—
>
> > (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
> >
> > (2) intentionally exceeds an authorization to access that facility;
> >
> > > *and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such* system shall be punished as provided in subsection (b) of this section.

18 U.S.C. § 2701(a) (2006) (emphasis added).

Husband contends that the circuit court erred by determining that he failed to allege all of the elements of a cause of action under Section 2701. We agree.

Here, the circuit court held that the allegations in Appellant's complaint were "fatally incomplete" because Appellant failed to specifically contend that Respondents "obtain[ed], alter[ed], or prevent[ed] authorized access to a wire or electronic communication while it [was] in electronic storage." Because the circuit court's ruling focused upon Appellant's complaint, it appears that the circuit court treated Respondents' motions for summary judgment as motions to dismiss under Rule 12(b)(6),

SCRCP.[1] However, the requirements for granting summary judgment are obviously different than the requirements for granting a Rule 12(b)(6) motion to dismiss. For instance, in ruling on a Rule 12(b)(6) motion, the court is confined to the complaint. See *Berry*, 328 S.C. at 441, 492 S.E.2d at 797 ("A Rule 12(b)(6) motion to dismiss for failure to state a cause of action must be resolved by the trial judge based *solely* on the allegations established in the complaint.") (emphasis added). In contrast, in ruling on a summary judgment motion, "a court must consider *everything* in the record-pleadings, depositions, interrogatories, admissions on file, affidavits, etc." *Gilmore v. Ivey*, 290 S.C. 53, 58, 348 S.E.2d 180, 183 (Ct. App. 1986).

In the present case, Husband introduced evidence showing that Broome logged onto Husband's Yahoo email account without authorization by changing

---

[1] Rule 12(b)(6), SCRCP, provides that "failure to state facts sufficient to constitute a cause of action" is a defense in a civil action. Here, there is no evidence in the record that any of the Respondents filed a motion to dismiss pursuant to Rule 12(b)(6), SCRCP. Moreover, even if Respondents had done so, the circuit court's consideration of matters outside of the pleadings would have converted such a motion into a summary judgment motion. *See* Rule 12(b), SCRCP ("If, on a motion asserting the defense numbered (6) to dismiss for failure of the pleading to state facts sufficient to constitute a cause of action, matters outside the pleading are presented to and not excluded by the Court, the motion shall be treated as one for summary judgment and disposed of as provided in Rule 56, and all parties shall be given reasonable opportunity to present all material made pertinent to such a motion by Rule 56."); *Berry*, 328 S.C. at 441-42, 492 S.E.2d at 798 (holding that, by considering matters outside of the pleadings, the trial court converted a Rule 12(b)(6) motion to dismiss into a summary judgment motion).

Husband's password. He also presented evidence that Broome, without Husband's consent, read and printed emails that were stored in Husband's Yahoo email account. Importantly, at least one court has held that comparable proof was sufficient to withstand a summary judgment motion in a section 2701 action. See *Fischer v. Mt. Olive Lutheran Church, Inc.*, 207 F. Supp. 2d 914, 924-26 (W.D. Wis. 2002) (denying summary judgment to defendants in a cause of action for a violation of section 2701 where evidence was presented to show that defendants logged onto plaintiffs Hotmail account without authorization and printed plaintiffs emails). Because the circuit court was ruling on motions for summary judgment, it was required to consider the evidence presented by Husband. Accordingly, we conclude that the circuit court erred by granting summary judgment to Respondents based merely upon the fact that Husband failed to expressly allege in his complaint that Respondents "obtain[ed], alter[ed], or prevent[ed] authorized access to a wire or electronic communication while it [was] in electronic storage." See 18 U.S.C. § 2701(a) (2006).

II. Did the circuit court err in holding that the emails were not in "electronic storage" as contemplated by 18 U.S.C. § 2510(17)?

By its terms, section 2701(a) applies only to communications that are in "electronic storage." See 18 U.S.C. § 2701(a) (2006). Section 2510(17) defines "electronic storage" as:

> (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission

> thereof; and
>
> (B) any storage of such communication by an *electronic communication service* for purposes of *backup protection* of such communication.

18 U.S.C. § 2510(17) (2006) (emphasis added).[2] In the present case, Husband contends that the emails in question fell within subsection (B) of section 2510(17) and that the circuit court therefore erred by holding that the emails were not in "electronic storage."[3] We agree.

In its decision, the circuit court held that the emails in question fell outside the scope of section 2510(17)(B) because: (i) they were not stored by an "electronic communication service" (ECS); and (ii) they were not stored "for purposes of backup protection." As discussed below, we find that the circuit court erred in reaching those conclusions.

---

[2] The definitions set forth in section 2510 have been incorporated into the SCA. *See* 18 U.S.C. § 2711(1) (2006).

[3] Several courts have held that the application of subsection (A) of section 2510(17) is limited to communications that have not yet been accessed by their intended recipient. *See, e.g.*, In re *DoubleClick, Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 512 (S.D.N.Y. 2001) ("[I]t appears that [section 2510(17)(A)] is specifically targeted at communications temporarily stored by electronic communications services incident to their transmission—for example, when an email service stores a message until the addressee downloads it."); *United States v. Weaver*, 636 F. Supp. 2d 769, 771 (C.D. III. 2009) ("Because the emails here have been opened, they are not in temporary, intermediate storage incidental to electronic transmission."). Here, as noted above, Broome testified that she never accessed any of Husband's unopened emails.

A. Were the emails stored by an ECS?

An ECS is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15) (2006). In the present case, the circuit court denied recovery to Husband based in part on its finding that "Plaintiff has not asserted or provided evidence from which to conclude he is an 'electronic communication service." Although we agree with the circuit court that Husband is not an ECS, the circuit court framed the issue incorrectly. Specifically, the circuit court should have addressed whether Yahoo was an ECS, rather than whether Husband was an ECS. Here, the emails in question were stored on servers operated by Yahoo. Therefore, the emails were stored "by" Yahoo. *See Quon v. Arch Wireless Operating Co., Inc.,* 529 F.3d 892, 901 (9th Cir. 2008) ("By archiving the text messages on its server, Arch Wireless certainly was 'storing' the messages."), *rev'd on other grounds sub nom. City of Ontario v. Quon*, No. 08-1332, 2010 WL 2400087 (U.S. June 17, 2010). Although any emails stored by Husband on the hard drive of his computer would not be covered by the SCA,[4] in this case, Broome did not access the emails in question from Husband's hard drive. Instead, she logged directly onto Yahoo's system and retrieved the emails from there. Accordingly, the relevant issue

---

[4] *See, e.g.*, *Hilderman v. Enea TekSci, Inc.*, 551 F. Supp. 2d 1183, 1204-05 (S.D. Cal. 2008) (holding that emails stored by employee on hard drive of company-issued laptop were not in "electronic storage" as contemplated by the SCA); *In re DoubleClick*, 154 F. Supp. 2d at 511-13 (holding that computer programs known as "cookies" placed by internet advertising corporation on the hard drives of plaintiffs' computers were not in "electronic storage").

here is whether Yahoo constitutes an ECS.

Turning to that question, we hold that Yahoo is an ECS. Yahoo unquestionably provides its users with the ability to send or receive electronic communications. Any doubt regarding whether Yahoo constitutes an ECS is removed by the SCA's legislative history, which provides that "electronic mail companies are providers of electronic communication services." S. Rep. No. 99-541, at 14 (1986); *see also* H.R. Rep. No. 99-647, at 63 (1986) ("An 'electronic mail' service . . . would be subject to Section 2701.").[5]

Wife, however, contends that Yahoo was acting as a "remote computing service" (RCS), rather than an ECS, at the time that the emails were accessed. RCS is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2) (2006).[6] The term refers to "the processing or

---

[5] Federal courts have looked to legislative history such as House and Senate Reports in interpreting the SCA. *See, e.g., Fischer*, 207 F. Supp. 2d at 925-26 (citing Senate Report); In re *Nat'l Sec. Agency Telecomms. Records Wig.*, 483 F.Supp.2d 934, 939 (N.D. Cal. 2007) (citing House and Senate Reports). Additionally, in construing federal statutes, the South Carolina Supreme Court has reviewed congressional reports to glean legislative intent. *See White v. S.C. Tax Comm'n*, 253 S.C. 79, 85-86, 169 S.E.2d 143, 145-46 (1969) ("Clearly demonstrative of the intent and purpose of Congress in enacting what is now Code Section 2056(b)(4) is the following quotation from Senate Report No. 1013.").

[6] An "electronic communications system" is "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

storage of data by an off-site third party." *Quon,* 529 F.3d at 901; *see also* 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, 1213-14 (2004) (describing customers of RCS as those that "paid to have remote computers store extra files or process large amounts of data").

In the present case, it is questionable whether Yahoo was providing RCS with respect to the emails in question. For instance, in *Quon*, the Ninth Circuit held that Arch Wireless, a company providing text messaging services to the city of Ontario, was not an RCS and that Arch Wireless therefore violated the SCA when it disclosed to the city the contents of text messages sent by city employees. *Quon*, 529 F.3d at 900-034.[7] Nonetheless, even if Yahoo was acting as an RCS with respect to the emails at issue, there is no question that Yahoo was also acting as an ECS with regard to those same emails. Husband's account was still active, and Husband retained the ability to send (forward) any of the emails at issue to someone else. Notably, the House Report for the SCA indicates that, in such situations, the communications would still be protected under section 2701. See H.R. Rep. No. 99-647, at 63 (1986)

---

electronic storage of such communications." 18 U.S.C. § 2510(14) (2006).

[7] This holding was not on review in the U.S. Supreme Court's recent City of Ontario decision in which the Court reversed a portion of *Quon*. See *City of Ontario*, 2010 WL 2400087, at *7 (noting that "[t]he petition for certiorari filed by Arch Wireless challenging the Ninth Circuit's ruling that Arch Wireless violated the SCA was denied"). Rather, the issue addressed in *City of Ontario* was whether the city violated the Fourth Amendment by reviewing the text messages. Id. at *4.

("[T]o the extent that a remote computing service is provided through an Electric Communication Service, then such service is also protected [under section 2701].").

Because Yahoo was providing ECS with respect to the emails at issue, this case is distinguishable from *Flagg v. City of Detroit,* 252 F.R.D. 346 (E.D. Mich. 2008), a case relied upon by Respondents. In that case, the court addressed whether text messages stored by a non-party service provider on behalf of the city of Detroit were discoverable in a civil action brought against the city. *Id.* at 347. The city claimed that disclosure of the text messages by the service provider was barred by section 2702(a) of the SCA, which prohibits RCS entities from knowingly divulging communications maintained on their systems and ECS entities from knowingly divulging communications that are in "electronic storage" on their systems. *Id.* at 349. The court disagreed with the city, finding that the service provider was acting as an RCS with respect to the text messages and that the city, as the "subscriber," could therefore give its consent to the disclosure of the messages under an exception set forth in section 2702(b)(3). *Id.* at 363.[8]

---

[8] Section 2702(b)(3) provides: "A provider described in subsection (a) may divulge the contents of a communication . . 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." 18 U.S.C. § 2702(b)(3) (2006). Although, in *Flagg*, the city did not want to give its consent, the court concluded that the city, as a party to the action, was "both able *and obligated* to give its consent" so that the city could comply with a request for the production of the text messages under Rule 34 of the Federal Rules of Civil Procedure. 252 F.R.D. at 363 (emphasis added).

The court gave the following explanation for its conclusion that the service provider was acting as an RCS:

> [T]he ECS/RCS inquiry in this case turns upon the characterization of the service that SkyTel *presently* provides to the City, pursuant to which the company is being called upon to retrieve text messages from an archive of communications sent and received by City employees in years past using SkyTel text messaging devices. . . . SkyTel is no longer providing, and has long since ceased to provide, a text messaging service to the City of Detroit—the City, by its own admission, discontinued this service in 2004, and the text messaging devices issued by SkyTel are no longer in use. The Court finds, therefore, that the archive maintained by SkyTel constitutes "computer storage," and that the company's maintenance of this archive on behalf of the City is a "remote computing service" as defined under the SCA.

Id. at 362-63.

Here, unlike the situation in *Flagg*, Yahoo was providing email services to Husband at the time the emails at issue were accessed. Accordingly, *Flagg* is distinguishable from the present case.

B. Were the emails being stored "for purposes of backup protection"?

As noted above, to fall within section 2510(17)(B), a communication must not only be stored by an ECS, it

must also be stored "for purposes of backup protection." In *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004), the Ninth Circuit addressed whether previously delivered emails held by an internet service provider (ISP) were stored "for purposes of backup protection" as contemplated by section 2510(17)(B). The court concluded that they were, explaining:

> An obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again—if, for example, the message is accidentally erased from the user's own computer. The ISP copy of the message functions as a "backup" for the user. Notably, nothing in the Act requires that the backup protection be for the benefit of the ISP rather than the user. Storage under these circumstances thus literally falls within the statutory definition.

Id. at 1075.

Like the Ninth Circuit, we believe that one of the purposes of storing a backup copy of an email message on an ISP's server after it has been opened is so that the message is available in the event that the user needs to retrieve it again. In the present case, the previously opened emails were stored on Yahoo's servers so that, if necessary, Husband could access them again. Accordingly, we hold that the emails in question were stored "for purposes of backup protection" as contemplated by section 2510(17)(B).

Respondents nonetheless contend that, because Husband has not claimed that he saved the emails anywhere else, the storage of his emails could not have been for the purposes of backup protection. However, courts interpreting section 2701 have issued rulings that would seem to allow Husband's cause of action in this case. See *Cardinal Health 414, Inc. v. Adams*, 582 F. Supp. 2d 967, 976 (M.D. Tenn. 2008) ("[W]here the facts indisputably present a case of an individual logging onto another's e-mail account without permission and reviewing the material therein, a summary judgment finding of an SCA violation is appropriate."); *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548, 555 (S.D.N.Y. 2008) ("The majority of courts which have addressed the issue have determined that e-mail stored on an electronic communication service provider's systems after it has been delivered, as opposed to e-mail stored on a personal computer, is a stored communication subject to the SCA."); *Fischer*, 207 F. Supp. 2d at 925-26 (rejecting argument that emails stored on Hotmail's system were not in "electronic storage").

Furthermore, we do not find Respondents' argument to be convincing. Under Respondents' construction of the SCA, the unauthorized access of a person's emails from an ECS would be unlawful if the person had previously saved his emails somewhere else, but would be perfectly lawful if the person had not done so. However, such an interpretation would lead to strange results. For instance, a person whose emails were stored solely with an ECS would generally suffer greater harm if someone "alter[ed]" or "prevent[ed] authorized

access" to his ECS-stored emails than a person who had saved his emails in additional locations. Yet, under Respondents' construction of the SCA, only the person in the latter position would be protected. We do not believe that this was what Congress intended.

Indeed, the legislative history of the SCA supports the conclusion that Congress intended for the SCA to apply to the conduct Broome engaged in here. For instance, both the House and Senate Reports state that section 2701 "addresses the growing problem of unauthorized persons deliberately gaining access to, and sometimes tampering with, electronic or wire communications that are not intended to be available to the public." H.R. Rep. No. 99-647, at 62 (1986); S. Rep. No. 99-541, at 35 (1986). Additionally, the Senate Report provides the following illustration of what conduct would constitute a violation of section 2701:

> For example, a computer mail facility authorizes a subscriber to access information in their portion of the facilities storage. Accessing the storage of other subscribers without specific authorization to do so would be a violation of [section 2701].

S. Rep. No. 99-541, at 36. Here, Broome has admitted that she accessed and read, without authorization, Husband's emails that were stored on Yahoo's system. The legislative history of the SCA indicates that Congress intended that such conduct would constitute a violation of section 2701.

C. Does the SCA apply to emails in a "post-transmission" state?

Respondents also argue for affirmance of the circuit court's decision on the ground that the emails in question were not in "electronic storage" as contemplated by section 2510(17) because they were in a "post-transmission" state. In making this argument, Respondents rely upon *Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623 (E.D. Pa. 2001), *affd on other grounds*, 352 F.3d 107 (3rd Cir. 2003). In *Fraser*, the court addressed whether an employer violated the SCA when it accessed emails of its employee that were stored on the employer's server. *Id.* at 632. The court held that there was no violation because the emails were in "post-transmission" storage, meaning that they had already been retrieved by the intended recipient. Id. at 636. The court concluded that the SCA "provides protection only for messages while they are in the course of transmission." *Id.*

However, the district court's decision in Fraser was subsequently appealed to the Third Circuit, which affirmed on different grounds. See *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107 (3rd Cir. 2003). Specifically, the Third Circuit held that the employer's actions fell within the exception set forth in section 2701(c)(1) because the employer administered the email system and thus was acting as the ECS.[9] *Id.* at 114-15. Importantly, in reaching that result, the Third Circuit expressed skepticism regarding the district court's ruling that the emails were not in electronic storage, stating:

---

[9] Section 2701(c)(1) provides: "Subsection (a) of this section does not apply with respect to conduct authorized . . . by the person or entity providing a wire or electronic communications service." 18 U.S.C. § 2701(c)(1) (2006).

> [A]ccording to the District Court, the e-mail was in a state it described as "post-transmission storage." We agree that Fraser's e-mail was not in temporary, intermediate storage. But to us it seems questionable that the transmissions were not in backup storage—a term that neither the statute nor the legislative history defines. Therefore, while we affirm the District Court, we do so through a different analytical path, *assuming without deciding that the e-mail in question was in backup storage*.

Id. at 114 (emphasis added).

Moreover, in *Theofel*, the Ninth Circuit declined to follow the district court's holding in *Fraser*, reasoning:

> In contrast to subsection (A), subsection (B) [of section 2510(17)] does not distinguish between intermediate and post-transmission storage. Indeed, *Fraser's* interpretation renders subsection (B) essentially superfluous, since temporary backup storage pending transmission would already seem to qualify as "temporary, intermediate storage" within the meaning of subsection (A). *By its plain terms, subsection (B) applies to backup storage regardless of whether it is intermediate or post-transmission*.

Theofel, 359 F.3d at 1075-76 (emphasis added). Similarly, in *Quon v. Arch Wireless Operating Co., Inc.*, 309 F. Supp. 2d 1204 (C.D. Cal. 2004), the court rejected the contention that the SCA did not apply to

emails in a "post-transmission" state, explaining: "Part (B) [of section 2510(17)] states that the storage must be 'for the purpose of backup protection.' Backup protection clearly may be needed after transmission." *Id.* at 1208. For the foregoing reasons, we decline to follow the district court's decision in *Fraser*.

Respondents further claim that the legislative history of the SCA supports their position. Specifically, they point to a section of the applicable House Report that states that email messages stored by an RCS should "continue to be covered by section 2702(a)(2)" if left on the server after they were accessed by the user. *See* H.R. Rep. No. 99-647, at 65 (1986). Respondents appear to contend that this passage demonstrates that Congress intended for opened emails to be covered under section 2702(a)(2), as opposed to section 2701. In *Theofel*, the Ninth Circuit rejected a similar argument, explaining:

> The cited discussion [from the House Report] addresses provisions relating to remote computing services. We do not read it to address whether the electronic storage provisions also apply. The committee's statement that section 2702(a)(2) would "continue" to cover e-mail upon access supports our reading. If section 2702(a)(2) applies to e-mail even before access, the committee could not have been identifying an exclusive source of protection, since even the government concedes that unopened e-mail is protected by the electronic storage provisions. 359 F.3d at 1077 (citations omitted).

We agree with the Ninth Circuit's analysis in *Theofel*. In our view, it would be too much of a stretch to conclude that the above-referenced passage from the House Report demonstrates that Congress did not intend for section 2701 to apply to opened emails.

D. Did the circuit court err by granting summary judgment to Wife, Cooke, and BJR?

Alternatively, Wife, Cooke and BJR contend that, even if the emails were in "electronic storage," the circuit court's grant of summary judgment as to them should be affirmed because they did not engage in a violation of section 2701. We agree.

In its order granting summary judgment to Respondents, the circuit court held that "regardless of this Court's findings as to whether any violation of 18 USC § 2701 occurred, Plaintiff cannot obtain any relief or recovery against Defendant Jennings or Defendant Cooke, as Defendant Jennings and Defendant Cooke are not persons who potentially engaged in such alleged violation." Because Husband has not specifically challenged that ruling, it is the law of the case and requires affirmance. *See Buckner v. Preferred Mut. Ins. Co.*, 255 S.C. 159, 160-61, 177 S.E.2d 544, 544 (1970) (holding that an unappealed ruling is the law of the case).

Moreover, we conclude that the circuit court's ruling on this issue was not erroneous. As noted above, Husband claims that Respondents violated section 2701. In order to violate section 2701, a person or entity must, among other things, intentionally access without authorization, or

intentionally exceed an authorization to access, a facility through which an electronic communication service is provided. *See* 18 U.S.C. § 2701(a) (2006). Civil causes of action for violations of the SCA may be brought pursuant to section 2707(a), which provides:

> Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, *which engaged in that violation* such relief as may be appropriate.

18 U.S.C. § 2707(a) (2006) (emphasis added).

Importantly, section 2707 extends civil liability only to "the person or entity . . which engaged in [the] violation." 18 U.S.C. § 2707(a) (2006); *Tucker v. Waddell*, 83 F.3d 688, 691 (4th Cir. 1996). Here, there is no evidence that Wife, Cooke, or BJR accessed Husband's email account. Although Wife disclosed some of Husband's emails to Cooke and BJR, who allegedly used the emails to obtain additional information about Husband's affair, the SCA does not punish such conduct. *See Cardinal Health*, 582 F. Supp. 2d at 976 ("While [the] SCA punishes the act of accessing a 'facility through which an electronic communication service is provided' in an unauthorized manner, the SCA does not punish disclosing and using the information obtained therefrom."). Accordingly, the circuit court

did not err by granting summary judgment to Wife, Cooke, and BJR. *See Fischer,* 207 F. Supp. 2d at 926 (granting summary judgment to defendants who did not access plaintiffs email accounts); *Cardinal Health*, 582 F. Supp. 2d at 977-79 (same); *see also Freeman v. DirecTV, Inc.*, 457 F.3d 1001 (9th Cir. 2006) (holding that civil liability under section 2707 does not extend to those who aid, abet, or conspire with a person or entity engaging in a violation of section 2702); *Doe v. GTE Corp.*, 347 F.3d 655 (7th Cir. 2003) (holding that an ISP was not liable under sections 2511 and 2520 of the ECPA for aiding and abetting defendants who intercepted and disclosed oral communications).

III. Did the circuit court err by denying Husband's motion to amend his complaint to add Neal as a party defendant?

Finally, Husband contends that the circuit court erred by not allowing him to amend his complaint a second time to add Neal as a party defendant. We disagree.

Rule 15(a), SCRCP, sets forth the standard for granting motions to amend a pleading. It provides in pertinent part:

> A party may amend his pleading once as a matter of course at any time before or within 30 days after a responsive pleading is served or, if the pleading is one to which no responsive pleading is required and the action has not been placed upon the trial roster, he may so amend it at any time within 30 days after it is served. *Otherwise a party may*

> *amend his pleading only by leave of court or by written consent of the adverse party; and leave shall be freely given when justice so requires and does not prejudice any other party*.

Rule 15(a), SCRCP (emphasis added). Although leave to amend should generally be "freely given," this court has held that it may be denied where the proposed amendment would be futile. *See Higgins v. Med. Univ. of S.C.*, 326 S.C. 592, 604-05, 486 S.E.2d 269, 275 (Ct. App. 1997).

Here, Husband has not alleged that Neal accessed Husband's email account. Therefore, because liability under the SCA extends only to those who actually engaged in a violation of that act, adding Neal as a party defendant would have been futile. Like Wife, Cooke, and BJR, Neal would have been entitled to summary judgment if he had been added as a defendant. Accordingly, we conclude that the circuit court did not err in refusing to grant Husband leave to amend his complaint to add Neal as a party defendant.

CONCLUSION

For the foregoing reasons, we affirm the circuit court's grant of summary judgment as to Wife, Cooke, and BJR, as well as the circuit court's denial of Husband's motion to amend his complaint to add Neal as a party defendant. Additionally, we reverse the circuit court's grant of summary judgment as to Broome and remand the case for further proceedings. Accordingly, the circuit's court's decision is

AFFIRMED IN PART, REVERSED IN PART, and

REMANDED.

PIEPER, J., and CURETON, A.J., concur.

APPENDIX C

COURT OF COMMON PLEAS OF SOUTH CAROLINA,
FIFTH JUDICIAL CIRCUIT.
RICHLAND COUNTY

M. LEE JENNINGS,
Plaintiff,

v.

GAIL M. JENNINGS, HOLLY BROOME, BRENDA COOKE, INDIVIDUALLY,
AND
BJR INTERNATIONAL DETECTIVE AGENCY, INC.,
Defendants.

No. 07-CP-40-1125.

September 23, 2008.

Order Granting Defendants' Motion for Summary Judgment and Denying Plaintiff's Motion to Amend Complaint

L. Casey Manning, Chief Administrative Judge.

This matter was before me for hearing on June 19, 2008 pursuant to the Defendants Motions for Summary Judgment and the Plaintiffs Motion to Amend the Complaint to add an additional party defendant and an additional cause of action for damage to his business. All parties were present and represented by their respective counsel.

During the hearing, counsel for the Plaintiff

stipulated that the causes of action under the South Carolina Homeland Security Act, §17-30-10, et seq., S.C. Code Ann. (1976, as amended); the South Carolina Computer Crime Act, §16-16-10, et seq., S.C. Code Ann. (1976, as amended); and the Federal Electronic Communications Privacy Act, 18 U.S.C., §§2510-2520, et. seq., are no longer being pursued by the Plaintiff as it was stipulated that there was no interception of the emails in question by the Defendants. He also stipulated that the Plaintiff was no longer pursuing his fourth cause of action for conspiracy which the Complaint referenced as improperly intercepting the Plaintiff's private electronic communications.

Therefore, the issues before the Court on Defendants' Motions for Summary Judgment were the Plaintiffs cause of action alleging violation of the Federal Stored Communications Act, 18 U.S.C., §§2701-2712 under the First Cause of Action, the Common Law Invasion of Privacy Claim (publicizing private affairs) under the Second Cause of Action, the Common Law Invasion of Privacy Claim (wrongful intrusion) under the Third Cause of Action, and the Plaintiffs Motion to amend his Complaint to add an additional party defendant and add an additional cause of action for damage to his business.

Upon review of the pleadings and the evidence in the record, the depositions submitted at the hearing and the arguments of counsel, I make the following Findings of Fact and Conclusions of Law.

FINDINGS OF FACT

1. The Plaintiff, Lee Jennings, is the husband of the

Defendant Gail Jennings. The Defendant Holly Broome is the daughter-in-law of the Defendant Gail Jennings and the step daughter-in-law of the Plaintiff Lee Jennings.

2. Gail Jennings and Lee Jennings separated on June 21, 2006 when the Plaintiff told Gail that he had fallen in love with someone else, who was also married. The Plaintiff told Gail Jennings that he had been corresponding with the woman with whom he had fallen in love via email, but he would not tell her the woman's name.

3. Defendant Gail Jennings told Defendant Holly Broome about the separation when Holly and her husband came over to Defendant Jennings' house on Saturday, June 24, 2006, and explained that the Plaintiff had told her that he had fallen in love with someone else and that they had been corresponding by email after Defendant Jennings had found a card for flowers in Plaintiff Jennings' car and realized the flowers were not for her. Defendant Gail Jennings was extremely upset.

4. The next day Defendant Broome, using her computer at her home, went onto the Plaintiffs Yahoo email account and changed his password, therefore giving her access to the saved emails which Mr. Jennings had received and not deleted, and had sent and not deleted. She printed emails which the Plaintiff had sent to his girlfriend, and which his girlfriend had sent to him. The Defendant Broome subsequently went on the email account several more times and printed out other emails which Plaintiff had sent his girlfriend, and which his girlfriend had sent him and which had been opened

and saved by Plaintiff Jennings.

5. Defendant Broome and Defendant Jennings made three copies of the emails, which Defendant Broome had printed and gave one to Plaintiffs domestic attorney and one to Defendant Cooke, the private investigator hired by Defendant Jennings and Defendant Jennings kept one copy.

6. Family Court litigation was initiated in the summer of 2006 by Defendant Gail Jennings. That litigation is still pending. There is no evidence in the record that the emails between the Plaintiff and his girlfriend, which had been printed by Defendant Broome, were ever filed with the Family Court and those emails have not been filed with this Court.

7. The parties consented to amendment of the Summons and Complaint of the Plaintiff to add additional causes of action and the Amended Summons and Complaint was filed on July 25, 2007.

8. There is no evidence in the record that the emails in question which were sent between the Plaintiff and his girlfriend and saved by the Plaintiff were temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof, nor is there any evidence that they were stored by an electronic communication service for purposes of back-up protection of those communications. The emails were saved on Plaintiffs personal account where they were kept at Plaintiffs discretion.

9. The Plaintiff learned that the emails in question had been accessed without his permission on or about January 3, 2007. He saw a counselor in June,

2007.

10. The Plaintiff's business has not suffered since his discovery that his saved emails had been printed and he started counseling.

CONCLUSIONS OF LAW

1. Plaintiff's Motion for Summary Judgment as to the First Cause of Action alleging violations of §16-16-10, et seq., S.C. Code Ann. (1976, as amended); §17-30-10, et seq., §16-16-10, et seq., 18 U.S.C., §§2510-2520, et. seq., and Plaintiffs Fourth Cause of Action for conspiracy to intercept and disseminate the Plaintiffs electronic communications is granted as to those causes of action as it was stipulated at the hearing that there was no interception of Plaintiffs emails under the statutes and that none of the Defendants had been convicted under §16-16-10, et seq. As was stipulated, since there was no interception then there was no conspiracy to intercept the Plaintiffs emails and there is no evidence in the record that interception of Plaintiff's emails were ever contemplated or attempted by Defendants.

2. Under the cause of action for public disclosure of private facts, one essential element of recovery is publicity. It is publicity, as opposed to publication, that gives rise to a cause of action for invasion of privacy. Communication to a single individual or to a small group of people, absent a breach of contract, trust or other confidential relationship, will not give rise to liability. *Rycroft v. Gaddy,* 281 S.C. 119, 314 S.E.2d 39 (S.C. App. 1984). No evidence has been presented showing that the emails in question were disclosed to the public or were the subject of

publicity. No evidence has been presented which shows that the Defendants mentioned the emails in any Family Court pleading or proceeding, or entered emails in question into the record in either the Family Court proceeding or this proceeding. Therefore, there has been no publicity attendant to the emails in question and summary judgment is therefore granted for the Defendants as to Plaintiffs Second Cause of Action.

3. Plaintiffs Third Cause of Action alleges invasion of privacy on the basis of wrongful intrusion. When a plaintiff bases an action for invasion of privacy on intrusion alone, bringing forth no evidence of public disclosure, it is incumbent upon him to show a blatant and shocking disregard of his rights and serious mental or physical injury, or humiliation to himself resulting therefrom. *Rycroft, supra, citing, Shorter v. Retail Credit Co.,* 251 F. Supp. 329 (D.S.C. 1966). The right of privacy protects only the ordinary sensibilities of an individual and not super sensitiveness. It is relative to the customs of the time and place, and it is determined by the norm of the ordinary man. Protection afforded by law must be restricted to the ordinary sensibilities and cannot extend to super sensitiveness or agoraphobia. In order to constitute an invasion of the right of privacy, an act must be of such a nature as a reasonable man can see might and probably would cause mental distress and injury to anyone possessed of ordinary feelings and intelligence, situated in like circumstances as the complainant; and this question is to some extent one of law. *Meetze v. The Associated Press,* 230 S.C. 330, 95 S.E.2d 606 (1956); *citing* 41 Am. Jur., Privacy, §12. As there has been no publication of the emails in question, it is

incumbent upon the Plaintiff to show serious mental or physical injury or humiliation to himself. *Rycroft, supra.*

The Plaintiff had already admitted to the Defendant Jennings that he had fallen in love with another woman and that they had been emailing each other. He would not provide Defendant Jennings with the woman's name. The Plaintiff and Defendant Jennings then separated. The question then becomes whether an ordinary man of ordinary sensibilities, having informed his wife that he had fallen in love with someone else with whom he had been corresponding via email and separated from his wife, would be so shocked and humiliated by his wife or another family member on her behalf snooping to try to find out the identity of the girlfriend and/or the nature of the relationship between the Plaintiff and his girlfriend so as to suffer serious mental or physical injury or humiliation. As aforestated, Family Court litigation is on-going concerning this matter and the identity of the Plaintiffs girlfriend would certainly have been revealed via discovery in the Family Court litigation. While it is certainly preferable that everyone mind their own business and not snoop into other family members' correspondence, via email or otherwise, given the specific facts and circumstances and the record in this case, I find that the ordinary husband with ordinary sensibilities would not be so shocked and outraged under the particular facts and circumstances of this case so as to suffer severe mental or physical injury, or severe humiliation when a family member, in this particular case Defendant Broome, having accessed his emails without permission and discovered the identity of his

girlfriend and the nature of their relationship, provided that information to Plaintiffs wife. This is especially true in light of the fact that the Plaintiff had informed Defendant Jennings that he had been corresponding with his girlfriend via email and chose to save the emails which had passed between him and his girlfriend when he could have deleted them at any time.

Furthermore, there is no evidence in the record that Defendant Jennings or Defendant Cook, individually or d/b/a BJR International Detective Agency, Inc. ever accessed Plaintiffs email account.

Therefore, summary judgment is hereby granted to the Defendants on Plaintiffs Third Cause of Action.

4. Plaintiff has asserted a cause of action under 18 USC § 2701(a) of the Stored Communications Act, alleging that Defendant "intentionally access[ed] without authorization a facility through which an electronic communication service is provided." Amended Complaint, Paragraph 16. While this language has been taken directly from the statute, it is a fatally incomplete description of the elements of § 2701 which give rise to a cause of action. There are other elements that must be satisfied to impute liability because the statute goes on to read: "and thereby obtains, alters, or prevents authorized access to a wire or electronic communication *while it is in electronic storage* in such system" [emphasis added]. The term "electronic storage" is defined in the statute. 18 USC § 2510(17) of the Act clearly defines "electronic storage" to be "(A) any *temporary, intermediate storage* of a wire or electronic communication *incidental to the electronic*

transmission thereof; and (B) any storage of such communication *by an electronic communication service for purposes of backup protection* of such communication" [emphasis added]. Therefore, Plaintiff has failed to allege all the elements of the cause of action under the statute. Furthermore, Plaintiff has not alleged any facts or provided any evidence that tends to establish that any e-mail in question was in "electronic storage" for purposes of the statute. This Court finds that no recovery or relief can be obtained by Plaintiff under this statute because the e-mails in question were not in "electronic storage" as defined by the clear language of the statute. The e-mails distributed to Defendant Jennings were those discovered by Defendant Broome, having been received, opened and read by the Plaintiff and then "saved" by the Plaintiff on his personal account or those sent by the Plaintiff and then "saved" by the Plaintiff, again in his personal account.

The e-mails that are at issue in this action were in a post-transmission, stored state. Thus, they fall outside the scope of the 18 USC § 2510(17) definition of "electronic storage." Under § 2510(17)(A) the e-mails were in neither "temporary" nor "intermediate storage" that is "incidental to the electronic transmission thereof." In fact, the e-mails had already been transmitted and had reached their final destination where they would be preserved indefinitely (presumably until Plaintiff deletes them), preventing any finding that they were in "temporary, intermediate storage." Nor could they be "incidental to the electronic transmission thereof," because they were the principal e-mails that were actually transmitted. As such, they fail all aspects of

the 18 USC §2510(17)(A) definition of "electronic storage."

The e-mails also fall outside the scope of 18 USC § 2510(17)(B) because the e-mails were not stored "by an electronic communication service for purposes of backup protection." Plaintiff has not asserted or provided evidence from which to conclude he is an "electronic communication service;" his personal storage of the e-mails is not within the scope of § 2510(17)(B). Plaintiff has also failed to assert or offer evidence that the e-mails were being stored by such an electronic communication service "for purposes of backup protection." *Id.* Indeed, there is every reason to believe that the e-mails accessed by Defendant Broome were the original and principal transmissions that were stored in Plaintiffs own account, not any sort of backup system controlled and managed by the electronic communications service (in this case, the Internet Service Provider: Yahoo). In other words, since the e-mails in question were stored on Plaintiff's personal account and could have been deleted by Plaintiff at any time, they can hardly be considered part of any "backup protection" system operated "by an electronic communication service." *Id.*

The cardinal rule of statutory interpretation is to ascertain and effectuate the intention of the legislature. *Hodges v. Rainey,* 341 S.C. 79, 85, 533 S.E.2d 578, 581 (2000). When a statute's terms are clear and unambiguous on their face, there is no room for statutory construction and a court must apply the statute according to its literal meaning. *Paschal v. State Election Commission,* 317 S.C. 434, 436, 454 S.E.2d 890, 892 (1995); *Carolina Power &*

Light Co. v. City of Bennettsville, 314 S.C. 137, 139, 442 S.E.2d 177, 179 (1994). Words must be given their plain and ordinary meaning without resort to subtle or forced construction to limit or expand the statute's operation. *Paschal,* 437, 892; *Bryant v. City of Charleston,* 295 S.C. 408, 368 S.E.2d 899 (1988); *State v. Blackmon,* 304 S.C. 270, 273, 403 S.E.2d 660, 662 (1991). While these rules of statutory construction are axiomatic, they are critical with respect to the interpretation of "electronic storage" from 18 USC § 2510(17)(B) in the context of 18 USC § 2701, especially when considering the other provisions of the Stored Communications Act.

The first requirement of § 2510(17)(B) is that the storage of the communication be "by an electronic communications service." Although one may argue that the interpretation of the word "by" could be ambiguous, its meaning becomes crystal clear when considered with the rest of the provision and the other provisions of the Stored Communications Act. The phrase is intended to denote at whose discretion or instruction the communication is maintained rather than merely where the communication is maintained, since it is already a given that the communication is stored within an electronic communication service's facility. 18 USC § 2701. § 2510(17)(B) goes on to read that the storage by the electronic communication service must be "for purposes of backup protection of such communication," indicating a specific purpose behind the electronic communication service's storage of an electronic communication. 18 USC § 2704, which is also part of the Stored Communications Act, is the statute that governs "backup preservation" by service providers, and states the instances in which

the government may require such service providers to backup documents, which is basically to perpetually preserve them in case the subscriber erases them from his principal account. An inference that this is exactly the type of "backup protection" referenced in § 2510(17)(B) is most reasonable, and affords meaning to the entire language of the statute without expanding it's operation beyond Congressional intent. In fact, were the language "for purposes of backup protection" to pertain to the Plaintiffs personal intent, it would render that language meaningless, because almost anything could be considered backup with such an amorphous and expansionary interpretation. Furthermore, if the court were to construe the phrase "by an electronic communications service" to mean that the communication preservation could be at the direction or discretion of the subscriber, then the language "for purposes of backup protection" would likewise be meaningless and unnecessary, since the subscriber could claim his preservation was for any purpose and almost any preservation could be considered "backup." This would be a forced interpretation of the statute that would ignore its plain meaning as well as other provisions of the Act, which provides a more specific and practical meaning. The statute was not intended to protect any and all personal electronic communication storage on internet service providers by individuals, or it would have been written that way; it was intended to protect subscribers from the inherently peculiar operations of such internet service providers from computer hackers, such as when an internet service provider is directed by the government under 18 USC § 2704 to indefinitely backup certain electronic

communications or when they choose to do so for other reasons.

Plaintiff has failed to assert any basis for concluding the e-mails obtained by Defendant Broome met either definition of "electronic storage" in § 2510(17) of the Act. In fact, Plaintiffs basis for recovery, described in his Amended Complaint Paragraph 7, is that Defendant Broome has "illegally accessed Plaintiffs private e-mail address without his permission." Storage of e-mails by Plaintiff on his personal e-mail account by definition falls outside the scope of § 2510(17). The e-mails in question can most accurately be classified as in the personal long-term storage of the e-mail client; they are neither incidental to the transmission of the communication nor are they maintained by the electronic communication service for backup protection. Therefore, there is no basis for finding a violation of 18 USC § 2701 and therefore summary judgment as to this cause of action is also granted.

Finally, regardless of this Court's findings as to whether any violation of 18 USC §2701 occurred, Plaintiff cannot obtain any relief or recovery against Defendant Jennings or Defendant Cooke, as Defendant Jennings and Defendant Cooke are not persons who potentially engaged in such alleged violation. 18 USC § 2707(a). The Fourth Circuit has considered a circumstance similar to the case at bar and ruled that the plain language of the statute only authorizes a cause of action against the "person or entity... which engaged in that violation." *Id. See Tucker v. Waddell,* 83 F.3d 688, at 691 (4th Cir.1996) ("Persons aggrieved by violations of the [§ 2707 of the Electronic Communications Privacy] Act can only

assert a cause of action against the person or entity that 'engaged in that violation.' "). Plaintiff has not asserted or provided any basis that Defendant Jennings or Defendant Cooke engaged in a violation of the Stored Communications Act, he merely asserts in Paragraph 7 of his Amended Complaint that Defendant Broome accessed his private e-mail account; thus, the cause of action against Defendant Jennings and Defendant Cooke under 18 USC § 2707 is dismissed as a matter of law.

5. As the Complaint has already been amended once and as this Court has granted summary judgment to the Defendants on the causes of action listed above, the Plaintiff's Motion for amendment of the Complaint to add an additional party defendant and allege damage to his business is denied.

AND IT IS SO ORDERED.

<<signature>>
L. CASEY MANNING
Chief Administrative Judge
Fifth Judicial Circuit
Columbia, South Carolina

Sept. 23, 2008.

APPENDIX D

THE STORED COMMUNICATIONS ACT

18 USC § 2701—Unlawful access to stored communications

(a) OFFENSE.—Except as provided in subsection (c) of this section whoever—

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

(b) PUNISHMENT.—The punishment for an offense under subsection (a) of this section is—

(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State—

(A) a fine under this title or imprisonment for not more than 5 years, or both, in the case of a first offense under this

subparagraph; and

(B) a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph; and

(2) in any other case—

(A) a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section.

(c) EXCEPTIONS.— Subsection (a) of this section does not apply with respect to conduct authorized—

(1) by the person or entity providing a wire or electronic communications service;

(2) by a user of that service with respect to a communication of or intended for that user; or

(3) in section 2703, 2704 or 2518 of this title.

18 USC § 2702 - Voluntary disclosure of customer communications or records

(a) PROHIBITIONS.—Except as provided in subsection (b) or (c)—

(1) 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; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, 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; and

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

(b) EXCEPTIONS FOR DISCLOSURE OF COMMUNICATIONS.— A provider described in subsection (a) may divulge the contents of a communication—

(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 this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;

(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

[(B) Repealed. Pub. L. 108–21, title V, § 508(b)(1)(A),Apr. 30, 2003, 117 Stat. 684]

(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.

(c) EXCEPTIONS FOR DISCLOSURE OF CUSTOMER RECORDS.— A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))—

(1) as otherwise authorized in section 2703;

(2) with the lawful consent of the customer or subscriber;

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the

emergency;

(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A; or

(6) to any person other than a governmental entity.

(d) REPORTING OF EMERGENCY DISCLOSURES.— On an annual basis, the Attorney General shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report containing—

(1) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (b)(8); and

(2) a summary of the basis for disclosure in those instances where—

(A) voluntary disclosures under subsection (b)(8) were made to the Department of Justice; and

(B) the investigation pertaining to those disclosures was closed without the filing of criminal charges.

18 USC § 2703 - Required disclosure of customer communications or records

(a) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE.— A governmental entity may require the disclosure

by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN A REMOTE COMPUTING SERVICE.—

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent

jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, 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.

(c) RECORDS CONCERNING ELECTRONIC COMMUNICATION SERVICE OR REMOTE COMPUTING SERVICE.—

(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure;

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) REQUIREMENTS FOR COURT ORDER.— A court order for disclosure under subsection (b) or (c) may be issued by any court that is a 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. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) NO CAUSE OF ACTION AGAINST A PROVIDER DISCLOSING INFORMATION UNDER THIS CHAPTER.— No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

(f) REQUIREMENT TO PRESERVE EVIDENCE.—

(1) IN GENERAL.— A provider of wire or electronic communication services or a remote computing service, upon the request of a

governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) PERIOD OF RETENTION.— Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

(g) PRESENCE OF OFFICER NOT REQUIRED.— Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

18 USC § 2705 - Delayed notice

(a) DELAY OF NOTIFICATION.—

(1) A governmental entity acting under section 2703 (b) of this title may—

(A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703 (b) of this title for a period not to exceed ninety days, if the court determines that there is reason to believe that notification of the

existence of the court order may have an adverse result described in paragraph (2) of this subsection; or

(B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703 (b) of this title for a period not to exceed ninety days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.

(2) An adverse result for the purposes of paragraph (1) of this subsection is—

(A) endangering the life or physical safety of an individual;

(B) flight from prosecution;

(C) destruction of or tampering with evidence;

(D) intimidation of potential witnesses; or

(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(3) The governmental entity shall maintain a true copy of certification under paragraph (1)(B).

(4) Extensions of the delay of notification provided in section 2703 of up to ninety days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) of this section.

(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first-class mail to, the customer or subscriber a copy of the process or request together with notice that—

(A) states with reasonable specificity the nature of the law enforcement inquiry; and

(B) informs such customer or subscriber—

(i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;

(ii) that notification of such customer or subscriber was delayed;

(iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and

(iv) which provision of this chapter allowed

such delay.

(6) As used in this subsection, the term "supervisory official" means the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney's headquarters or regional office.

(b) PRECLUSION OF NOTICE TO SUBJECT OF GOVERNMENTAL ACCESS.— A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703 (b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—

(1) endangering the life or physical safety of an individual;

(2) flight from prosecution;

(3) destruction of or tampering with evidence;

(4) intimidation of potential witnesses; or

(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

18 USC § 2707 - Civil action

(a) CAUSE OF ACTION.— Except as provided in section 2703 (e), any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

(b) RELIEF.— In a civil action under this section, appropriate relief includes—

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c); and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) DAMAGES.— The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000. If the violation is willful or intentional, the court may assess punitive damages. In the case of a

successful action to enforce liability under this section, the court may assess the costs of the action, together with reasonable attorney fees determined by the court.

(d) ADMINISTRATIVE DISCIPLINE.— If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(e) DEFENSE.— A good faith reliance on—

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization (including a request of a governmental entity under section 2703 (f) of this title);

(2) a request of an investigative or law enforcement officer under section 2518 (7) of this title; or

(3) a good faith determination that section 2511 (3) of this title permitted the conduct complained of;

is a complete defense to any civil or criminal action brought under this chapter or any other law.

(f) LIMITATION.— A civil action under this section may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

(g) IMPROPER DISCLOSURE.— Any willful disclosure of a "record", as that term is defined in section 552a (a) of title 5, United States Code, obtained by an investigative or law enforcement officer, or a governmental entity, pursuant to section 2703 of this title, or from a device installed pursuant to section 3123 or 3125 of this title, that is not a disclosure made in the proper performance of the official functions of the officer or governmental entity making the disclosure, is a violation of this chapter. This provision shall not apply to information previously lawfully disclosed (prior to the commencement of any civil or administrative proceeding under this chapter) to the public by a Federal, State, or local governmental entity or by the plaintiff in a civil action under this chapter.

18 USC § 2711 - Definitions for chapter

As used in this chapter—

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section;

(2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system;

(3) the term "court of competent jurisdiction" includes—

(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that—

(i) has jurisdiction over the offense being investigated;

(ii) is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or

(iii) is acting on a request for foreign assistance pursuant to section 3512 of this title; or

(B) a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants; and

(4) the term "governmental entity" means a department or agency of the United States or any State or political subdivision thereof.