NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
14 N.C. J.L. & TECH. ON. 205 (2013)

STEALING GLANCES: ELECTRONIC COMMUNICATIONS PRIVACY AND THE NECESSITY FOR NEW LEGISLATION IN THE DIGITAL AGE

Laura Arredondo-Santisteban*

Electronic communication technology has seamlessly woven itself into the fabric of individuals' daily lives. Technology's rapid evolution and continuous advancement has made it possible for more people to enjoy access to devices that facilitate electronic communications. Technology's progression, however, is starkly contrasted against the law's inability to keep pace. Garcia v. City of Laredo *highlights the gap in protection that certain electronic communication technologies suffer under the Stored Communications Act. Although the Act was envisioned by Congress to provide greater protection for future forms of communication, courts' narrow interpretations of the privacy protections and the lack of any major revisions have resulted in the need for new legislation to better serve Congress's original purpose.*

I. INTRODUCTION

If someone breaks into your house and steals your diary, under the law he or she can be prosecuted. Logic reasons then, that if someone breaks into your locker, steals your cell phone, and downloads your pictures, you should also be able to prosecute him or her. What if the text messages and photos on your phone were shown to your boss, who then fires you for an inappropriate work relationship? You would want be able to press charges against the person who unlawfully accessed your personal text messages. Unfortunately, this was not the case for Fannie Garcia.[1] She was

* J.D. Candidate, University of North Carolina School of Law, Class of 2014. I would like to thank the Board and Staff of the *North Carolina Journal of Law & Technology* for all of the assistance they have provided me and Professor Anne Klinefelter for her guidance.

[1] *See* Garcia v. City of Laredo, 702 F.3d 788 (5th Cir. 2012).

unable to prosecute a fellow co-worker's wife, who took her cell phone, viewed its contents, and then showed them to Garcia's employers.[2]

Garcia could not take advantage of the Stored Communications Act ("SCA"), which is aimed at protecting "electronic communications" in storage.[3] The SCA provides substantive criminal prohibitions for offenses involving unauthorized access of such stored communications.[4] The SCA sets strict guidelines regarding access and receipt of electronic communications by service providers, government officials, and private actors.[5] Violators are subject to criminal penalties of up to ten years imprisonment, as well as civil damages.[6]

The number of computers connected to the Internet has steadily increased from less than 90,000 in 1989 to 1 million in 1993 and over 9 million in 1996.[7] As communication technology became more widely accessible to the general population and more portable, people began to take more personal information outside the home.[8] However, such communications were not guaranteed protection against unauthorized access.[9] Currently, the SCA provides little protection due to its antiquated view of technology, courts' narrow interpretations, and its lack of substantive updates.[10] The SCA was established in an effort to provide greater protection to newer forms of communication, resulting from advances in "computer and telecommunications technolog[y]."[11] However, the SCA has not been amended to update its scope and treatment of

---

[2] *See id.* at 790.

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

[4] *See id.* § 2701(b).

[5] *See id.* § 2701.

[6] *See id.* § 2701(b).

[7] Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1294 (2004).

[8] *See infra* Part IV.

[9] *See* Garcia v. City of Laredo, 702 F.3d 788, 793 (5th Cir. 2012).

[10] *See infra* Part V.

[11] S. REP. NO. 99-541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555.

technology since it was enacted in the 1980s.[12] Consequently, as technology has continued to advance, the law has remained stunted in its conception of technology's functions and its use by individuals.[13]

The SCA was envisioned by Congress to extend protections to new and future forms of electronic communication.[14] Congress recognized the need for protection as more individuals used new and developing forms of electronic communications in their personal and work lives.[15] This Recent Development addresses a gap in protection that exists under the Stored Communications Act, which no longer satisfies Congress's intent to extend protection to new technology. Part II of this Recent Development discusses the history and progression of information privacy law in the United States. Part III analyzes the SCA's purpose and the congressional intent behind its enactment. Part IV analyzes the current state of Internet and telecommunications technology, as compared to the state of technology at the time of the SCA's adoption in 1986. Next, Part V looks at various courts' interpretations and applications of the SCA as compared to how the Fifth Circuit framed the SCA in *Garcia v. City of Laredo*.[16] Part VI emphasizes the need for new legislation that expands protections to include future forms of communications technology. Specifically, it proposes that legislation should create broad principles that establish privacy protections, which can be adapted as technology continues to progress.

II. PRIVACY LAW: A BRIEF HISTORY

"Privacy . . . is a concept in disarray."[17] Unlike other areas of law, privacy law has not developed in a systemic or traceable fashion. This is due, in part, to the difficulty scholars, philosophers, and jurists have had at conceptualizing the notion of

[12] Solove, *supra* note 7, at 1293.
[13] *Id.*
[14] *See* S. REP. NO. 99-541, at 5.
[15] *Id.*
[16] 702 F.3d 788 (5th Cir. 2012).
[17] DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 1 (2008).

privacy.[18] Privacy law encompasses a wide-ranging body of law that includes common law, constitutional law, and statutory law.[19]

In the late nineteenth century, privacy concerns became social and political issues.[20] Not only were newspapers being widely circulated, but also the press had become increasingly sensational.[21] Technological advancements, such as Kodak's release of the snap camera, posed privacy concerns by making it easier for the general public to document life events.[22] In 1890, Justice Samuel Warren and Justice Louis Brandeis published *The Right to Privacy*, in which they articulated the need for the law to recognize and provide protection for individual privacy.[23] They noted that the common law had always served to protect individuals' person and property and that it could be reworked and reinterpreted to protect privacy interests as well.[24]

Over the years, states began to adopt or recognize privacy torts, such as public disclosure of private facts,[25] intrusion upon seclusion,[26] false light,[27] appropriation,[28] defamation,[29] and infliction of emotional distress.[30] These torts allowed individuals to take civil action and

---

[18] *Id.* at 2.

[19] DANIEL J. SOLOVE, MARC ROTENBERG & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 9 (Erwin Chemerinksy et al. eds., 2nd ed. 2006).

[20] *Id.*

[21] *Id.*

[22] *Id.* at 10.

[23] *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890).

[24] *Id.* at 213.

[25] RESTATEMENT (SECOND) OF TORTS § 652D (1977) (creating a cause of action for someone who publicly discloses a private matter that is "highly offensive to a reasonable person and is not of legitimate concern to the public").

[26] *Id.* § 652B (providing a remedy when a person intrudes upon the solitude or seclusion of another or his private affairs or concerns).

[27] *Id.* § 652E (creating a cause of action when one publicly discloses a matter that places a person in a false light that is "highly offensive to the reasonable person").

[28] *Id.* § 652C (providing a remedy against one who appropriates to his own use or benefit the name or likeness of another).

[29] *Id.* § 558.

[30] *Id.* § 46 (providing a remedy when "one by extreme and outrageous conduct intentionally or recklessly causes severe emotional distress to another").

receive damages for privacy intrusions in certain circumstances. Where courts failed to recognize a right, state legislatures worked quickly to adopt laws to ensure future protection.[31]

Beginning in the 1960s and 1970s, "privacy [re]emerged as a central political and social concern," particularly due to the introduction of new technology, such as the computer.[32] Growing concern about the ability of computers and other electronic surveillance devices to collect information about citizens prompted Congress to focus its attention on privacy and information collection.[33] Consequently, Congress passed various laws protecting privacy in different sectors of industry and the economy. Some of Congress's most notable privacy legislation includes the Family Educational Rights and Privacy Act of 1974 ("FERPA")[34] and the Video Privacy Protection Act of 1988.[35]

Apart from Congress's enactment of statutory privacy laws, the Federal Constitution has also been interpreted to protect certain privacy rights.[36] In 1965, the Supreme Court decided *Griswold v.*

---

[31] *See* Paul Czarnota, *The Right of Publicity in New York and California: A Critical Analysis*, 19 VILL. SPORTS & ENT. L.J. 481, 487 (2012). For example, after the New York Court of Appeals refused to recognize a common law right for invasion of privacy in *Roberson v. Rochester Folding Box Co.*, the New York legislature quickly expressed its disapproval and responded by enacting a statute targeting such behavior. *See id.* The statute made it a misdemeanor for a "person, firm or corporation that uses for advertising purposes, or for the purposes of trade, the name, portrait or picture of any living person without having first obtained written consent of such person." N.Y. CIV. RIGHTS LAW § 50 (McKinney 2009).

[32] SOLOVE, ROTENBERG, & SCHWARTZ, *supra* note 19, at 35.

[33] WILLIS H.WARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS 1 (1973), *available at* http://www.rand.org/content/dam/rand/pubs/papers/2008/P5077.pdf.

[34] Educational Amendments of 1974, Pub. L. No. 93-380, § 513, 88 Stat. 484, 571–78 (1974) (codified as amended at 20 U.S.C. § 1232g(b) (2006) (protecting the privacy of school records)).

[35] *See* Video Privacy Protection Act, Pub. L. No. 100-618, 102 Stat. 3195 (1988) (codified as amended at 18 U.S.C. § 2710–2712 (2006) (protecting individuals' videotape rental information)).

[36] *See, e.g.*, McIntyre v. Ohio Election Comm'n, 514 U.S. 334 (1995). The First Amendment's protection of speech and the right of association have been interpreted to safeguard against intrusions by the government compelling people

Connecticut,[37] a landmark case recognizing that individuals have a constitutional right to privacy.[38] The Supreme Court found that legislation, which inserted the government into the affairs of marital unions, intruded upon the fundamental nature of privacy that is located within other freedoms protected by the Bill of Rights.[39] The Court in *Griswold* specifically recognized privacy, for the first time, as a right held by the people against the government.

Griswold was influential in recognizing individuals' right to privacy for their life decisions, but under the "state action doctrine," the right of privacy is protected from intrusions by government actors, not private actors.[40] The Supreme Court's holdings in the *Civil Rights Cases*[41] are largely credited for establishing the need for state action for the Constitution to apply.[42] "[T]he Constitution does not purport to determine how one *person*

---

to disclose their identities or the groups to which they belong. *See id.* at 462; *see also* NAACP v. Alabama, 357 U.S. 449, 462 (1985) ("It is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute . . . an . . . effective restraint of freedom of association . . . . This court has recognized the vital relationship between freedom to associate and privacy in one's associations."). The Third Amendment prevents the government from requiring people to house soldiers in their homes, and protects individuals' right to privacy in their home from government intrusion. U.S. CONST. amend. III. The Fourth Amendment's protection against unreasonable searches and seizures is viewed as an implicit privacy protection of individuals to remain secure in their "persons . . . and effects." U.S. CONST. amend. IV. The Fifth Amendment's privilege against self-incrimination protects individual privacy by prohibiting the government from forcing individuals to testify against themselves under certain circumstances. U.S. CONST. amend. V.

[37] 381 U.S. 479 (1965).

[38] *See id.* at 484. Finding unconstitutional a Connecticut statute that made it a crime for any person to use any form of contraception for the purpose of preventing pregnancy, the Court stated "specific guarantees in the Bill of Rights have penumbras, formed from emanations of those guarantees that give them life and substance. Various guarantees create zones of privacy." *Id.*

[39] *See id.*

[40] *See* Wilson R. Huhn, *The State Action Doctrine and the Principle of Democratic Choice*, 34 HOFSTRA L. REV. 1379, 1388–89 (2006).

[41] 109 U.S. 3, 10–11 (1883).

[42] G. Sidney Buchanan et al., *State Action and the Public/Private Distinction*, 123 HARV. L. REV. 1248, 1256 (2010).

is to treat another. So far as the Constitution is concerned, one individual may steal the possessions of another, assault another person, even commit murder, and it is not in violation of the Constitution."[43] Consequently, invasion by a private actor of individual rights is simply a private wrong, which must be left "to the laws of the State for redress."[44]

In 1921, the Supreme Court reinforced the private action distinction and held that the Fourth Amendment does not apply to the actions of private individuals.[45] Individuals' right to be free from unreasonable searches and seizures pertains only to government searches.[46] In *Burdeau v. McDowell*,[47] the Court held that "[the Fourth Amendment's] origin and history clearly show that it was intended as a restraint upon the activities of sovereign authority, and was not intended to be a limitation upon other than governmental agencies."[48] The Supreme Court reaffirmed its holding in *Burdeau* years later in *United States v. Jacobsen*.[49] It stated that Fourth Amendment protection proscribes only government action and that "it is wholly inapplicable 'to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.' "[50]

The Supreme Court's holdings in *Burdeau* and *Jacobsen* reinforce this "private search doctrine," which establishes that the right of the people to be free from unreasonable searches and seizures proscribes only government action.[51] Under the private search doctrine, the Fourth Amendment does not govern searches conducted by private actors, so long as their actions do not

---

[43] Huhn, *supra* note 40, at 1388.
[44] *Civil Rights Cases*, 109 U.S. at 17.
[45] Burdeau v. McDowell, 256 U.S. 465, 475 (1921).
[46] *See id.*
[47] 256 U.S. 465 (1921).
[48] *Id.* at 475.
[49] 466 U.S. 109 (1984).
[50] *Id.* at 113–14 (quoting Walter v. United States, 447 U.S. 649, 662 (1980) (Blackmun, J., dissenting)).
[51] *See Walter*, 477 U.S. at 662 (Blackmun, J., dissenting).

constitute state action.[52] Consequently, evidence of adultery obtained by a private party who enters into his separated wife's apartment without her consent is not subject to a motion to suppress on the ground that it had been illegally obtained under the Fourth Amendment.[53] The evidence is admissible without Fourth Amendment concern because the husband was neither a state actor nor acting on behalf of the state.[54]

III. STORED COMMUNICATIONS ACT

Wrongful searches and seizures by private actors may not violate the Fourth Amendment, but individuals are free to pursue actions against intrusions by private actors under any applicable tort, criminal, or statutory law. Before 1986, the United States Code did not provide protection for communications stored in large electronic data banks or remote computing operations because such technologies had either not been invented or were only beginning to develop and had hardly become widespread.[55] But, due to the "dramatic changes in new computer and telecommunications technologies," Congress was compelled to protect new technological forms of communication.[56] Congress expressed concern that advances in communications and computer technologies resulted in comparable advances in surveillance techniques, "making it possible for overzealous law enforcement agencies, industrial spies and private parties to intercept the personal or proprietary communications of others . . . ."[57]

While the Fourth Amendment generally provides strong privacy protections in the home against unreasonable searches and seizures by the government, Congress recognized that access to information obtained and stored on Internet networks no longer required a physical intrusion by the government into a person's

[52] *See* Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971).
[53] *See* Sackler v. Sackler, 229 N.Y.S.2d 61, 62, 64 (1962).
[54] *Id.* at 64–65.
[55] *See* Garcia v. City of Laredo, 702 F.3d 788, 791 (5th Cir. 2012).
[56] S. REP. NO. 99-541, at 1 (1986).
[57] *Id.* at 3.

"home."[58] Computers are not only used by large businesses to store and process information but are also used by private citizens as recordkeeping systems.[59] Citizens increased use of new communications technologies made it possible for the government and other private actors to easily access individuals' electronic communications without violating the Fourth Amendment because "there was no searching, no seizure of anything tangible, and no physical trespass."[60]

Under the "third party records doctrine,"[61] information that is lawfully held by third parties can be obtained by law enforcement through subpoena or other means of legal discovery, without the requirement of a search warrant.[62] In *United States v. Miller*,[63] the Supreme Court held that because the defendant voluntarily shared information in the form of deposit slips with his bank, a third party, he had no expectation of privacy under the Fourth Amendment and the police did not need a warrant to obtain the information.[64]

The Internet's structure requires communications to pass through remote third party servers.[65] Congress recognized that current law provided little protection from unauthorized access to the information transmitted through new technologies.[66] In voicing the necessity behind protecting citizens' private electronic communications, Congress stated:

> A letter sent by first class mail is afforded a high level of protection against unauthorized opening . . . . Voice communications transmitted via common carrier are protected . . . .
>
> But there are no comparable Federal statutory standards to protect the privacy and security of communications transmitted by new

---

[58] *See id.* at 2.
[59] *See id.* at 3.
[60] *Id.* at 2.
[61] *See* United States v. Miller, 425 U.S. 435, 443 (1976); *see also* Smith v. Maryland, 442 U.S. 735, 743–44 (1979).
[62] *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1210 (2004).
[63] 425 U.S. 435 (1976).
[64] *See id.* at 443.
[65] *See* Kerr, *supra* note 62, at 1209–10.
[66] *See* S. REP. NO. 99-541, at 3 (1986).

> noncommon carrier communications services or new forms of telecommunications and computer technology.[67]

Congress noted that the lack of clear standards not only discouraged potential users from using new communication systems but also that it exposed law enforcement to liability and posed a danger to the admissibility of evidence.[68] As a result, Congress adopted the Stored Communications Act to ensure that the law advanced along with technology and to protect the privacy of private citizens.[69]

Various federal attempts at regulating electronic surveillance preceded the SCA's adoption.[70] In 1928, the Supreme Court, in a controversial opinion, declared that wiretapping did not constitute a search and did not violate the Fourth Amendment.[71] In response, Congress enacted the Federal Communications Act of 1934, which prohibited the unauthorized interception of communications and the publication of intercepted communications.[72] In 1968, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[73] which required federal agents to obtain a warrant before wiretapping.[74] In 1986, Congress passed the Electronic Communications Privacy Act ("ECPA") in an attempt to modernize the federal wiretap laws and to extend application of federal electronic surveillance law to private individuals and entities, as well as government officials.[75] The SCA,[76] also known

---

[67] *Id.* at 5.

[68] *Id.*

[69] *See id.*

[70] *See* Communications Act of 1934, ch. 652, 48 Stat. 1064, 1103 (1934) (codified as amended at 47 U.S.C. § 605 (2006)); Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 197, 211–25 (1968) (codified as amended at 18 U.S.C. §§ 2510–2520 (2006)).

[71] *See* Olmstead v. United States, 277 U.S. 438, 465 (1928).

[72] *See* 47 U.S.C. § 605.

[73] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 197, 211–25 (1968) (codified as amended at 18 U.S.C. §§ 2510–2520 (2006)).

[74] *See* 18 U.S.C. § 2516.

[75] SOLOVE, ROTENBERG, & SCHWARTZ, *supra* note 19, at 265–71.

[76] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, tit. II, 100 Stat. 1848, 1860–68 (1986) (codified as amended at 18 U.S.C. §§ 2701–2712 (2006)).

as Title II of the Electronic Communication Privacy Act, was one of three Acts that made up the ECPA and created a set of privacy protections for electronic information held by network and service providers for access by government and private actors of electronic information held by network and service providers.[77] Apart from the SCA, the ECPA also consisted of the Wiretap Act[78] and the Pen Register Act.[79] The ECPA, in its entirety, governs wire, oral, and electronic communications.[80] However, the SCA's scope is limited to regulating only stored electronic communications. In relevant part, section 2701 of the SCA states that 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 . . . .[81]

The SCA protects citizens' electronic communications from unauthorized access by government officials and private parties.[82] The SCA makes it a criminal offense to access wire and electronic communications, while in temporary or backup storage, without authorization.[83] The SCA forbids the disclosure of contents of stored electronic communications by service providers without the consent of the creator or recipient of the communication.[84] Punishment for violations can consist of a minimum fine of $1,000 per violation and incarceration for up to six months.[85] If the government seeks access to communications that are in storage for more than 180 days, it may obtain access by subpoena or court order.[86]

---

[77] Kerr, *supra* note 62, at 1212–13.
[78] *See* Electronic Communications Privacy Act tit. I, 100 Stat. at 1848–59.
[79] *See id.* at tit. III, 100 Stat. at 1868–73 (codified as amended at 18 U.S.C. §§ 3121–3127.
[80] Solove, *supra* note 7, at 1279.
[81] 18 U.S.C. § 2701.
[82] *See id.*
[83] *Id.* at § 2701(a) – (b).
[84] *Id.* at § 2702(a).
[85] *Id.* at § 2701(b).
[86] *Id.* at § 2703(a).

Congress emphasized that the provision directed at both government and private parties addressed 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."[87] While the statute defines various key words and pairings,[88] notably absent from the definitions section is the definition for what constitutes "facility" for electronic communication.[89] This is most likely because at the time the legislation was drafted, technology did not allow for Congress to conceptualize any "facility" other than network service providers with the capability of providing and storing electronic communications. When the SCA was adopted, network service providers, such as ISPs, were the focal points of the legislation.[90] This was due, in part, to the way in which technology was used at that time. In the 1980's, computers utilized third party network service providers to send and receive communications, like e-mail, and to outsource computing tasks that involved large amounts of data.[91] However, ordinary network users were unable to store large amounts of information on their own personal computers or networks. Users had to pay network service providers for sending and receiving such communications and for electronic storage on the provider's servers.[92] As a result, while Congress envisioned a law that would "advance with technology,"[93] it crafted the SCA to reflect the understandings and operation of computer networks as of 1986.[94]

---

[87] S. REP. NO. 99-541, at 35 (1986).

[88] *See, e.g.*, 18 U.S.C. § 2510(17) (2006) (defining "electronic storage" to include "(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").

[89] *See* Garcia v. City of Laredo, 702 F.3d 788, 792 (5th Cir. 2012).

[90] *See* Kerr, *supra* note 62, at 1213.

[91] *See id.* at 1213–14.

[92] *Id.*

[93] *See* S. REP. NO. 99-541, at 5 (1986).

[94] Kerr, *supra* note 62, at 1214.

IV. TECHNOLOGY TODAY

Technology has evolved greatly since the SCA's adoption in 1986. Currently, Gmail[95] offers its users 10 gigabytes of free storage for e-mail messages and attachments.[96] The concept of e-mail has evolved from a simple text-only message to a massive storage facility where users can send and receive documents, photos, and videos and keep them in storage for later access.[97]

When Congress envisioned protections for electronic communications, e-mail's storage capabilities were greatly limited.[98] As more households obtained Internet access in the home, online communication among Americans increased.[99] In 2010, the Pew Research Center reported that sixty-six percent of American adults have a broadband Internet connection at home.[100] The increase in access to wireless Internet, or Wi-Fi, meant that the ability to communicate across online networks is no longer limited to a cable or Ethernet-line connection in the home. Currently, approximately seventy-four percent of adults use the Internet, with fifty-five percent of adults connecting wirelessly to the Internet.[101]

Internet access, however, is no longer solely limited to an online connection through a laptop computer.[102] As technology has

---

[95] GMAIL, http://www.gmail.com (last visited Mar. 7, 2013).

[96] *Your Storage Limit*, GMAIL, http://support.google.com/mail/bin/answer.py?hl=en&answer=6558 (last visited Mar. 7, 2013).

[97] *See* Ian Peter, *The History of Email*, NETHISTORY, http://www.nethistory.info/History%20of%20the%20Internet/email.html (last visited May 24, 2013).

[98] *See* Lucas Mearian, *Scientists Calculate Total Data Stored to Date: 295+ Exabytes*, COMPUTERWORLD (Feb. 14, 2011, 6:00 AM), http://www.computerworld.com/s/article/9209158/Scientists_calculate_total_data_stored_to_date_295_exabytes.

[99] *See id.*

[100] AARON SMITH, PEW RESEARCH CTR., HOME BROADBAND 2010 5 (2010), *available at* www.pewinternet.org/~/media//Files/Reports/2010/Home%20broadband%202010.pdf.

[101] LEE RAINIE, PEW RESEARCH CTR., INTERNET, BROADBAND, AND CELL PHONE STATISTICS 1 (2010), *available at* http://www.pewinternet.org/~/media//Files/Reports/2010/PIP_December09_update.pdf.

[102] *See* KATHRYN ZICKUHR & AARON SMITH, PEW RESEARCH CTR., *DIGITAL DIFFERENCES* 2 (2012), *available at* http://pewinternet.org/~/media//Files/Reports/2012/PIP_Digital_differences_041312.pdf.

improved, so have the ways in which people are able to connect to the Internet. Tablets and smart phones with Internet access allow people to go online wirelessly without a traditional computer.[103] "Currently, 88% of American adults have a cell phone, 57% have a laptop, 19% own an e-book reader, and 19% have a tablet computer; about six in ten adults (63%) go online wirelessly with one of those devices."[104]

Apart from increasing and facilitating access to the Internet, devices like tablets and smartphones now have increased memory capabilities that allow users to store more information on their hard drives. According to Apple,[105] the most recent version of their iPhone can contain up to sixty-four gigabytes of data.[106] It has the ability to film and store videos, save pictures, and send and receive text messages; all in a device that weighs less than four ounces.[107] With these devices, electronic and online communication is not limited to e-mail and text messages. As of December 2012, sixty-seven percent of online adults use and participate in social networking sites, with the majority of online adults using Facebook and Twitter, respectively.[108] These social networking sites allow users to post information to select groups of members, as well as the ability send private messages to other users.[109]

Consequently, technology has not only facilitated electronic communication but also has made it possible to communicate electronically outside the home. Texting and messaging services allow users to send and receive brief electronic messages between

---

[103] *See id.*

[104] *Id.*

[105] APPLE, http://www.Apple.com (last visited Mar. 7, 2013).

[106] *iPhone*, APPLE, http://www.apple.com/iphone/specs.html (last visited Jan. 26, 2013).

[107] *Id.*

[108] MAEVE DUGGAN & JOANNA BRENNER, PEW RESEARCH CTR., THE DEMOGRAPHICS OF SOCIAL MEDIA USERS—2012 2 (2013), *available at* http://pewinternet.org/~/media//Files/Reports/2013/PIP_SocialMediaUsers.pdf. *See* FACEBOOK, http://www.facebook.com (last visited Mar. 7, 2013); TWITTER, http://www.twitter.com (last visited Mar. 7, 2013).

[109] *See* Michael Hirschorn, *About Facebook*, THE ATLANTIC (Oct. 1, 2007, 12:00 PM), http://www.theatlantic.com/magazine/archive/2007/10/about-facebook/306181.

mobile phones over a phone network.[110] Currently, eighty percent of cell phone owners use their phones to send and receive text messages from other mobile users.[111] Cell phone companies, such as Verizon Wireless and AT&T, have evolved from simple phone service providers, to providing mobile broadband services, such as 3G (third generation) networks.[112] Through these services, mobile phone users are able to access the Internet and download data at high speeds.[113]

V. *GARCIA V. CITY OF LAREDO* & STORED COMMUNICATION ACT CASES

Laws should strive to set guiding principles which can be easily applied across a broad spectrum of technology and should not attempt to fix legal understandings to technology's current functions. When Senator Patrick Leahy addressed Congress about the necessity of the SCA, he argued that existing law had not kept up with technology and that new legislation was necessary to keep pace with technological advancements.[114] The problem with laws centered on particular forms of technology is that such legislation is quickly rendered ineffective and outdated as technology changes.

In *Garcia*, Fannie Garcia was terminated from her job after a co-worker's wife removed her personal cell phone from a locker at work and shared its contents with Garcia's employer.[115] The contents stored on her cell phone included personal text messages, videos, and photos, which were subsequently downloaded and used to

---

[110] MAEVE DUGGAN & LEE RAINIE, PEW RESEARCH CTR., CELL PHONE ACTIVITIES 2012 5 (2012), *available at* http://www.pewinternet.org/~/media//Files/Reports/2012/PIP_CellActivities_11.25.pdf.

[111] *Id.*

[112] *See* AT&T, http://www.att.com (last visited Mar. 7, 2013); VERIZON WIRELESS, http://www.verizonwireless.com (last visited Mar. 7, 2013).

[113] *See* INT'L TELECOMM. UNION, THE WORLD IN 2011: ICT FACTS AND FIGURES (2011), *available at* http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf.

[114] S. REP. NO. 99-541, at 3–4 (1986).

[115] Garcia v. City of Laredo, 702 F.3d 788, 790 (5th Cir. 2012).

support an accusation that she had violated the rules and regulations of her employment.[116]

On appeal, Garcia argued that the SCA protected all text-messages and data stored on her personal phone.[117] In her brief, Garcia stated that both the statute's language and legislative history evince Congress's intent for the statute to be broadly construed to protect new and evolving communications.[118] Consequently, she argued that her cell phone was a "facility" under the meaning of the SCA in which electronic communication was kept in electronic storage in the form of text messages and other data.[119] Garcia argued that cell phones act much like freight cars that are used to ship physical goods from one place to another, or power lines that transmit electricity from one source to another.[120]

The Fifth Circuit disagreed with Garcia's classification of facility and cited the Eleventh Circuit, stating that the SCA applies to information stored with phone companies and ISPs but not to information stored directly on a personal computer's hard drive or a cell phone.[121] In dismissing Garcia's claim for SCA-protection, the Fifth Circuit agreed with the district court's reasoning in *Freedom Banc Mortgage Services v. O'Harra*[122] that "the relevant 'facilities' that the SCA is designed to protect are not computers that *enable* the use of an electronic communication service, but instead are facilities that are *operated by* electronic communication service providers and used to store and maintain electronic storage."[123] In *Garcia*, the court stated that "[a]n individual's personal cell phone does not *provide* an electronic communication

---

[116] *Id.*

[117] *Id.* at 791.

[118] Brief of Appellant at 25, *Garcia*, 702 F.3d 788 (No. 11-41118).

[119] *Id.* ("[A] common cell phone from which a user subscribes to an electronic communications service, such as Verizon or Cricket[,] is [a] . . . 'facility' in which electronic communication is kept in electronic storage.").

[120] *See id.*

[121] *See Garcia*, 702 F.3d at 792–93 (discussing United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003)).

[122] Freedom Banc Mortg. Servs., Inc. v. O'Harra, No. 2:11-cv-01073, 2012 U.S. Dist. LEXIS 125734 (S.D. Ohio Sept. 5, 2012).

[123] *Id.* at *23 (emphasis added).

service just because the device enables use of electronic communications services."[124] The court justified its reasoning by relying on the Senate's 1986 report.[125] It noted that nowhere in the legislative reports did Congress mention individual computers, nor did it mention extending SCA protection to communications stored in personal computers.[126] By refusing to classify a cell phone or personal computer as a "facility," the court stated it was merely reading the statute consistently with the legislative history.[127]

Garcia failed to provide any evidence that the defendants directly obtained any information from the cell phone company or network.[128] Consequently, the court found that the text messages and photos accessed from her phone fell outside the scope of the SCA.[129] The court stated that regardless of whether Garcia's phone could be construed as a facility, the text messages and other data accessed by defendants were not in "electronic storage"[130] as defined by the Act.[131] The court stated that, because Garcia was not an "electronic communication service"[132] provider, such as an ISP or phone company, the information stored on her personal cell phone could not be considered to be in electronic storage under the SCA.[133] According to the court, electronic communications should only be considered in "electronic storage" when stored by an electronic communication service provider, not a recipient of such

[124] *Garcia*, 702 F.3d at 793.
[125] *See id.*
[126] *Id.*
[127] *See id.* at 793.
[128] *Id.* at 793.
[129] *Id.*
[130] 18 U.S.C. § 2510(17) (2006) (defining 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").
[131] *Garcia*, 702 F.3d at 793.
[132] 18 U.S.C. § 2510(15) ("Electronic communication service means any service which provides to users thereof the ability to send or receive wire or electronic communications.").
[133] *Garcia*, 702 F.3d at 793.

services.[134] "Thus, information that an Internet provider stores to its servers or information stored with a telephone company . . . are examples of protected electronic storage under the statute."[135]

The Fifth Circuit's decision in *Garcia* was not unique. The court relied on several cases from other jurisdictions, which all similarly held that information downloaded and located solely on a personal computer's hard drive does not fall within the scope of the SCA.[136] Recent court cases that have interpreted the SCA have struggled to uniformly apply its rigid framework to modern technology.[137] When the SCA was enacted, users were unable to keep opened e-mail sitting on the server for long periods of time because of limited storage space capability.[138] Congress crafted the SCA to reflect how the e-mail system operated at that time and wrote the law to protect electronic communications in storage with network service providers.[139]

Many courts continue to apply the 1980's understanding of the SCA.[140] These courts argue that that opened e-mails, remaining on

---

[134] *Id.*

[135] *Id.*

[136] *See* Freedom Banc Mortg. Servs., Inc. v. O'Harra, No. 2:11-cv-01073, 2012 U.S. Dist. LEXIS 125734, at *22 (S.D. Ohio Sept. 5, 2012); s*ee also* Hilderman v. Enea TekSci, Inc., 551 F. Supp. 2d 1183, 1205 (S.D. Cal. 2008) ("E-mails stored on the laptop computer are not in 'temporary, intermediate storage.' Furthermore, these e-mails on the laptop are not stored 'by an electronic communication service for purposes of backup protection' as required by subsection (B)."); Bailey v. Bailey, No. 07-11672, 2008 U.S. Dist. LEXIS 8565, at *17 (E.D. Mich. Feb. 6, 2008) ("Stored Communications Act protection does not extend to emails and messages stored only on Plaintiff's personal computer.").

[137] *See* United States v. Steiger, 318 F.3d 1039, 1047–52 (11th Cir. 2003); *see also In re* iPhone Application Litig., 844 F. Supp. 2d. 1040, 1056–60 (N.D. Cal. 2012); *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 510 (S.D.N.Y. 2001). *But see* Expert Janitorial, LLC, v. Williams, No. 3:09-CV-283, 2010 WL 908740, at *4–5 (E.D. Tenn. Mar. 12, 2010); Chance v. Ave. A, Inc., 165 F. Supp. 2d 1153, 1161 (W.D. Wash. 2001).

[138] *See* Solove, *supra* note 7, at 1283.

[139] *See id.* at 1293–95.

[140] *See* Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114 (3d Cir. 2003) (unwilling to define backup storage to mean e-mails kept on the server); *see also* Jennings v. Jennings, 736 S.E.2d 242, 245 (S.C. 2012) (reasoning that e-mails,

an ISP's server, no longer fall within the purview of the SCA because they are no longer considered to be in "temporary, intermediate"[141] electronic storage or to be for the "purpose of backup protection."[142] In *Fraser v. Nationwide Mutual Insurance Co.*,[143] the Third Circuit granted summary judgment in favor of defendant Nationwide, and held that the SCA did not apply to an employer's search of an employee's e-mail because the e-mails had already been read by the employee and were no longer in "temporary, intermediate storage."[144]

Similarly, the Supreme Court of South Carolina reversed an appellate court's finding that a relative of respondent's wife violated the SCA when she hacked into his e-mail and printed out incriminating copies as evidence against him in divorce proceedings.[145] The court, in *Jennings v. Jennings*,[146] declined to extend SCA protection to an opened e-mail that remained on a server after being read.[147] "We question the reasoning . . . that such passive inaction can constitute storage for backup protection under the SCA . . . ."[148]

However, in 2004, the Ninth Circuit took a different approach in *Theofel v. Farey-Jones.*[149] It concluded that all e-mails on a server are protected under electronic communication service rules, regardless of whether an e-mail had been accessed.[150] A year later, in *United States v. Councilman*,[151] the First Circuit followed the same line of reasoning and stated that "Congress sought to ensure that the messages and by-product files that are left behind after

---

once read and kept on the server, no longer qualify as being in electronic storage under the SCA).

[141] *See* 18 U.S.C. § 2510(17) (2006).

[142] *See Jennings*, 736 S.E.2d at 245.

[143] 352 F.3d 107 (3d Cir. 2003).

[144] *Id.* at 114.

[145] *Jennings*, 736 S.E.2d at 243, 245.

[146] *Id.* at 242.

[147] *Id.* at 245.

[148] *Id.*

[149] 359 F.3d 1066, 1075 (9th Cir. 2004).

[150] *See id.* at 1077 ("[P]rior access is irrelevant to whether the messages at issue were in electronic storage.").

[151] 418 F.3d 67 (1st Cir. 2005).

transmission, as well as messages stored in a user's mailbox, are protected from unauthorized access."[152] The First Circuit rejected the argument that an e-mail ceases to be an electronic communication under the SCA when the message "resides in transient electronic storage."[153]

Variation exists among the courts as they decide how to grant SCA protection to the different stages of communication technology. Some courts have begun to interpret the SCA to protect e-mails that users have read and kept on the server.[154] One court found that a person who directly logs in to a user's three e-mail accounts from the same computer and obtains copies of his or her e-mails is "access[ing] three separate electronic communication services."[155] Some courts, however, have been explicit in exempting e-mails and messages that are only stored on a computer hard drive from SCA protection.[156] These courts hold that, in order to receive SCA protection, a copy of the message must remain on the server.[157]

Some courts, like the Ninth Circuit in *Theofel* and the First Circuit in *Councilman*, have not found it difficult to extend SCA protection to situations involving unauthorized access to opened e-mail remaining on a server.[158] But the same cannot be said when courts are requested to extend SCA protection to electronic communications stored in other media, like cell phone applications

---

[152] *Id.* at 77.

[153] *See id.* at 79.

[154] *See, e.g.*, Bailey v. Bailey, No. 07-11672, 2008 U.S. Dist. LEXIS 8565, at *17 (E.D. Mich. Feb. 6, 2008) (finding that "[t]he fact that Plaintiff may have already read the emails and messages . . . [that remained on the server] does not take them out of the purview of the Stored Communications Act.").

[155] Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 556 (S.D.N.Y. 2008).

[156] *Bailey*, 2008 U.S. Dist. LEXIS 8565, at *17 ("However, as a point of clarification, Stored Communications Act protection does not extend to emails and messages stored only on Plaintiff's personal computer.").

[157] *Id.*

[158] *Councilman*, 418 F.3d at 77; Theofel v. Farey-Jones, 359 F.3d 1066, 1077 (9th Cir. 2004); *see also Pure Power Boot Camp*, 587 F. Supp. 2d at 556; *Bailey*, 2008 U.S. Dist. LEXIS 8565, at *17.

or text-messages.[159] These courts have refused to broadly interpret SCA provisions to extend protection to non-e-mail forms of communication, despite the fact that research shows the usage of devices with the capabilities to communicate electronically have increased.[160] As in *Garcia*, people are now saving their electronic communications to mobile devices and PDAs.[161] Mobile phone technology, however, typically operates differently from e-mail. Once the electronic communication is received by the intended device, it is no longer considered to be in storage with the service provider under the SCA.[162] Therefore, technology involving communications that download directly to a user's device are difficult to protect under the SCA.

Cases that have attempted to obtain SCA-protection for non-e-mail communications have largely been unsuccessful.[163] In *In re iPhone Application Litigation*,[164] a district court refused to classify iPhones or other iOS devices as a "facility through which an electronic communication service is provided."[165] The iPhone plaintiffs alleged that Apple,[166] iPhone's manufacturer, and other

---

[159] *See* United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003); *see also In re* iPhone Application Litig., 844 F. Supp. 2d. 1040, 1058 (N.D. Cal. 2012) ("Plaintiffs fail to state a claim under the SCA because their iOS devices do not constitute 'facilit[ies] through which an electronic communication service is provided.' "); *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 510–11 (S.D.N.Y. 2001) ("The cookies' long-term residence on plaintiffs' hard drives places them outside of § 2510(17)'s definition of 'electronic storage' and hence, [the SCA's] protection.").

[160] *See* DUGGAN & RAINIE, *supra* note 110, at 5.

[161] *See* Garcia v. City of Laredo, 702 F.3d 788, 788 (5th Cir. 2012).

[162] *See* Puneet Gupta, *Short Message Service: What, How and Where?*, WIRELESS DEVELOPER NETWORK, http://www.wirelessdevnet.com/channels/sms/features/sms.html (last visited Mar. 7, 2013).

[163] *See Steiger*, 318 F.3d at 1049 (stating the "non-applicability of the SCA to hacking into personal computers"); *see also In re iPhone*, 844 F. Supp. 2d. at 1057 (declining to consider "an individual's computer, laptop, or mobile device" as a facility); *In re DoubleClick*, 154 F. Supp. 2d at 514 (S.D.N.Y. 2001) ("[A]ll of plaintiffs' communications accessed by DoubleClick fall under § 2701(c)(2)'s exception or outside [the SCA] and, accordingly, are not actionable.").

[164] 844 F. Supp. 2d. 1040 (N.D. Cal. 2012).

[165] *Id.* at 1057; *see* 18 U.S.C. § 2701(a)(1) (2006).

[166] APPLE, http://www.Apple.com (last visited Mar. 7, 2013).

mobile industry defendants violated their privacy rights under the SCA by unlawfully allowing third party applications to collect and use their personal information without their knowledge or consent.[167] The court found that classifying plaintiffs' iPhones as facilities would "render other parts of the [SCA] illogical."[168]

Similarly, in *In re DoubleClick Inc. Privacy Litigation*,[169] another district court was also unwilling to classify plaintiffs' personal computers as "facilities" for the purpose of challenging an Internet advertising corporation's placement of computer programs, or "cookies,"[170] on plaintiffs' computer hard drives.[171] The court held that the placement of "cookies" on plaintiffs' computers fell outside the scope of protection under the SCA.[172] Relying upon legislative history, the court found the lack of reference to personal computers indicated that the SCA "deals only with facilities operated by electronic communication services such as 'electronic bulletin boards' and 'computer mail facility[ies]' . . . . It makes no mention of individual users' computers . . . ."[173] Regardless of whether Congress failed to take adequate account of basic property and privacy notions when enacting the SCA, the court held it could not ignore the plain meaning of the statute when determining SCA protection.[174]

Apart from those district courts, the Eleventh Circuit in *United States v. Steiger*,[175] also refused to classify a personal computer as a "facility" under the SCA, stating:

---

[167] *In re iPhone*, 844 F. Supp. 2d. at 1048–49.

[168] *Id.* at 1058.

[169] 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

[170] A "cookie" is defined as "a small file or part of a file stored on a World Wide Web user's computer, created and subsequently read by a Web site server, and containing personal information (as a user identification code, customized preferences, or a record of pages visited)." *Cookie*, MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary/cookie (last visited Mar. 29, 2013).

[171] *See In re DoubleClick*, 154 F. Supp. 2d at 512.

[172] *Id.* at 512 ("DoubleClick's cookies fall outside § 2510(17)'s definition of electronic storage and, hence, § 2701's scope.").

[173] *Id.* at 512.

[174] *See id.* at 509.

[175] 318 F.3d 1039 (11th Cir. 2003).

> [T]he SCA clearly applies, for example, to information stored with a phone company, Internet Service Provider (ISP), or electronic bulletin board system (BBS).
>
> The SCA, however, does not appear to apply to the source's hacking into Steiger's computer to download images and identifying information stored on his hard-drive because there is no evidence to suggest that Steiger's computer maintained any "electronic communication service . . . ."[176]

Few cases exist in which courts have refused to dismiss complaints where the argument is that personal computers are "facilities" under the SCA.[177] However, courts presiding in those cases typically render their decisions on procedural grounds, or on other limited grounds, such as whether or not to grant summary judgment.[178] As a result, those courts, when conducting an analysis of whether or not such a device is a facility under the SCA, have not provided in-depth reasoning or analysis of the law, as noted by the court in *In re iPhone*.[179] *Chance v. Avenue A, Inc.*,[180] represents one of the few cases in which a court refused to grant summary judgment, concluding that "modern computers, which serve as a conduit for the web server's communication to Avenue A, are facilities covered under the [SCA]."[181] In rendering its decision against summary judgment, the court noted that while the SCA was enacted "to cover . . . mid-1980s technological facilities," the

---

[176] *Id.* at 1049 (quoting 18 U.S.C. § 2510(15) (2006)).

[177] *See* Chance v. Ave. A, Inc., 165 F. Supp. 2d 1153, 1161 (W.D. Wash. 2001); *see also* Expert Janitorial, LLC, v. Williams, No. 3:09-CV-283, 2010 WL 908740, at *5 (E.D. Tenn. Mar. 12, 2010) ("[F]or the purposes of a motion to dismiss, plaintiff's allegations that the email accounts, user-names, and passwords were stored on plaintiff's computers . . . are sufficient allegations to assert a claim under § 2701 of the SCA."); *In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1275 n.3 (C.D. Cal. 2001).

[178] *See Expert Janitorial*, 2010 WL 908740, *10; *see also In re Intuit*, 138 F. Supp. 2d at 1275 n.3 ("Defendant does brief the issue whether a computer would qualify as a 'facility' for the purposes of Section 2701 for the first time in its reply brief, but this court does not consider arguments raised anew for the first time in a reply brief . . . .").

[179] *See In re* iPhone Application Litig., 844 F. Supp. 2d. 1040, 1058 (N.D. Cal. 2012).

[180] 165 F. Supp. 2d 1153 (W.D. Wash. 2001).

[181] *Id.* at 1161.

computer has now become the "focal point of Internet communications."[182]

Similar to *Chance*, the court in *Expert Janitorial, LLC v. Williams*[183] refused to dismiss plaintiff's claim that defendants violated the SCA when they accessed the e-mail accounts and passwords of plaintiff's employees through plaintiff's computer.[184] Defendants argued that Plaintiff's allegations regarding their access to employee e-mail accounts were insufficient to state a claim under the SCA because the plaintiff was not an electronic communication provider or a facility through which an electronic communication service was provided.[185] The court refused to dismiss the claim and stated that the SCA "does not require that a plaintiff's computers or workplace be a 'facility' through which an electronic communication is provided."[186]

In *Expert Janitorial*, the court cited to *Becker v. Toca*[187] to find that, in certain situations, personal computers may constitute facilities under the SCA.[188] In *Becker*, the plaintiff alleged that the defendant had violated the SCA when she intentionally sent a computer virus to the plaintiff's and the plaintiff's employees' computers for the purpose of obtaining financial information and passwords.[189] Defendant argued that the SCA did not apply in that situation because the plaintiff's computers were not "facility[ies] through which an electronic communication service is provided."[190] The court argued that it would be "premature and speculative" to dismiss the claim due to the fact that "the computers may qualify as [facilities] because the Plaintiff does allege that he used the

---

[182] *Id.* at 1160.
[183] No. 3:09-CV-283, 2010 WL 908740 (E.D. Tenn. Mar. 12, 2010).
[184] *Id.* at *5.
[185] *Id.* at *4.
[186] *Id.* at *5 (stating that the "plaintiff's allegations that the email accounts, user-names, and passwords were stored on plaintiff's computers and that defendants knowingly accessed this stored information without authorization are sufficient allegations to assert a claim under § 2701 of the SCA").
[187] No. 07-7202, 2008 WL 4443050 (E.D. La. Sept. 26, 2008).
[188] *Expert Janitorial*, 2010 WL 908740 at *5.
[189] *Becker*, WL 4443050, at *1.
[190] *Id.*

computers to run his business."[191] Thus, a few courts have entertained the possibility that computers, and in theory other PDA-like devices, are facilities and can receive SCA protection. The courts' decisions in those cases, however, lack substantial precedential and analytical support to guide future courts tackling similar issues.

VI. *GARCIA*'S IMPLICATIONS AND SOLUTIONS

According to the interpretation of the majority of courts, a person may receive protection under the SCA against unauthorized hacking and downloading of their e-mails in storage with an Internet or network service provider.[192] However, under this interpretation, SCA-protection will not be given for unauthorized hacking and downloading of text messages that are stored on a cell phone.[193] The Fifth Circuit's ruling in *Garcia* highlights the current gap in the law.[194] When courts narrowly read the SCA to apply solely to facilities operated by services, like ISPs or telephone companies, other electronic communications do not fall within its protection. This hole in the law is particularly disconcerting in the private action context, where private actors are the ones conducting the searches. As noted earlier, the Fourth Amendment's protections against unlawful searches and seizures do not extend to private actors.[195] Independent statutory protection is necessary to ensure that private actors are unable to obtain access to private electronic communications without authorization.[196] Congress recognized this need when it enacted section 2701 of the SCA.[197] It noted that before the SCA's adoption, the legal atmosphere provided little

---

[191] *Id.* at *4.

[192] *See generally* Bailey v. Bailey, No. 07-11672, 2008 U.S. Dist. LEXIS 8565 (E.D. Mich. Feb. 6, 2008) (holding that emails stored on a server fall under the protection of the SCA).

[193] *See* Garcia v. City of Laredo, 702 F.3d 788, 792–93 (5th Cir. 2012).

[194] *See id.*

[195] *See supra* Part II.

[196] *See* Burdeau v. McDowell, 256 U.S. 465, 475 (1921).

[197] *See* S. REP. NO. 99-541, at 3 (1986) ("Thus, the information may be open to possible wrongful use and public disclosure by law enforcement authorities as well as unauthorized private parties. The provider of these services can do little under current law to resist access to communications.").

ability to resist unapproved access by private parties to individuals' electronic communications.[198] Consequently, Congress purposely made section 2701 a criminal provision to "address[ ] 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."[199]

The SCA has not been substantively amended or updated since its creation in the 1980's.[200] At the time of the SCA's adoption, approximately 7.9 percent of households in the United States owned a home computer,[201] contrasted with the three quarters of Americans who currently own a desktop computer or laptop computer.[202] People are now storing more than just phone numbers in their cell phones and are taking that information with them outside of the home and into the workplace.[203] As a result, the ability of private actors to access other individuals' electronic communications has risen with the advancements that have created devices that permit people to electronically communicate in public places outside the home.

Garcia exemplifies the problem that private actors face when new forms of electronic communication are not protected under the SCA. As new ways are developed to allow individuals to communicate electronically, and such means of communication become popular, the necessity to expand the scope of what is protected under the SCA becomes imperative. Currently, the majority of courts, including the Fifth Circuit in *Garcia*, narrowly interpret the SCA to only apply to facilities and operations as they

---

[198] *Id.*

[199] *Id.* at 35.

[200] Solove, *supra* note 7, at 1293 ("While ECPA has been amended between 1986 and 2001 . . . 'subsequent changes have merely nibbled around the edges of the law.' ").

[201] ROBERT KOMINKSI & ERIC NEWBURGER, ACCESS DENIED: CHANGES IN COMPUTER OWNERSHIP AND USE: 1984–1997 5 (1999), *available at* http://nslab.ee.ntu.edu.tw/courses/summer00/overview/confpap99.pdf.

[202] AARON SMITH, PEW RESEARCH CTR., AMERICANS AND THEIR GADGETS 2 (2010), *available at* http://www.pewinternet.org/~/media/Files/Reports/2010/PIP-Americans%20and%20their%20Gadgets.pdf.

[203] *See* Garcia v. City of Laredo, 702 F.3d 788, 790 (5th Cir. 2012).

existed at the time of the SCA's adoption.[204] Such an interpretation leaves courts with an antiquated law that is unable to adequately protect current and future forms of electronic communication from unauthorized access by private actors.

Courts' failure to interpret the SCA in the current technological atmosphere coupled with Congress's lack of amendments updating the SCA are particularly disconcerting when placed in an employment setting. When the private actor conducting the search is an employer, the danger includes divulging personal information and possible termination from employment.[205] In *Garcia*, the information revealed from her cell phone was not only extremely private and involved an on-and-off relationship with a fellow co-worker, but it also led to her being fired.[206] Under the Fifth Circuit's reading of the SCA, however, little recourse exists for those in Fannie Garcia's position.[207]

Different states may provide tort-like causes of action for situations involving unwanted accessing of private electronic communications, in which individuals may seek civil remedies.[208] Such causes of action may include common law tort actions, like trespass to chattels, invasion of privacy, and perhaps conversion.[209] Unlike tort actions, the SCA is unique because it not only provides a unified federal law across the states, but it also imposes criminal liability on individuals who violate its terms.[210] The imposition of criminal liabilities is notable because it indicates that Congress acknowledged the danger that such unauthorized access could pose to individuals.[211] Congress, as a result, deliberately included criminal provisions in the SCA to deter unwanted acts of intrusion.[212]

---

[204] *See supra* Part V.
[205] *See Garcia*, 702 F.3d at 790.
[206] Brief of the Appellant at 3–15, *Garcia*, 702 F.3d 788 (No. 11-41118).
[207] *See Garcia*, 702 F.3d at 791–93.
[208] *See supra* Part II.
[209] *See supra* Part II.
[210] *See* 18 U.S.C. § 2701(b) (2006).
[211] *See* S. REP. NO. 99-541, at 5 (1986) (discussing fears that a failure to increase protection as technology advances would result in the erosion of individual privacy rights).
[212] *See* 18 U.S.C. § 2701(b).

The SCA is an important piece of legislation. Protection against unwanted intrusion into individuals' electronic communications through service providers remains an important objective. However, there are currently many new ways for individuals to communicate electronically that do not involve communications being stored by network service providers.[213] Limiting protection to communications based on where they are located quickly renders the SCA ineffective. It also ignores Congress's intent for enacting the legislation in the first place—to protect communications that use new technology.[214] Had Congress been able to identify how new technology was to be used and assimilated into everyday culture, it would have protected communications on PDAs, cell phones, and future devices. This can be ascertained in Senate reports accompanying the SCA's proposal analyzing the protection afforded to mail and telephone conversations as a reason for extending protection to newer modes of communication.[215] This indicates that Congress intended for the SCA to eliminate "[t]his gap [that] results in legal uncertainty" by creating protection for new forms of communication.[216]

The problem shown in *Garcia* and other cases that involve new technology indicates that, contrary to Congress's intention, the SCA has not been interpreted to encompass all new forms of communications technology. The idea that someone can prosecute someone for breaking into their locker and taking their diary but is unable to prosecute someone for breaking into their cell phone and accessing their text messages does not seem to coincide with Congress's intent for the SCA. As more and more people begin using and relying on devices to communicate electronically with one another, the threat posed by unauthorized access to electronic communications is no longer largely from the government. Unauthorized access to electronic communications can now result from an angry co-worker,[217] an ex-spouse,[218] or an employer.[219]

---

[213] Modern forms of communication include text messaging, e-mail, Facebook and Twitter messages.

[214] *See* S. REP. NO. 99-541, at 5.

[215] *Id.*

[216] *Id.*

[217] Garcia v. City of Laredo, 702 F.3d 788, 790 (5th Cir. 2012).

The reality is that after-the-fact tort claims, such as invasion of privacy, do not carry the same disincentive against unlawfully accessing those communications as do criminal penalties.

Some scholars argue that the SCA has the ability to encompass newer and upcoming forms of technology through broad interpretation by the courts.[220] While a broad interpretation of the SCA could encompass situations like *Garcia*, the majority of courts have shown an unwillingness to push the statute's boundaries when it comes to including other types of communication.[221] A new federal statute that explicitly permits courts to grant privacy protections to newer forms of communication would eliminate courts' concerns of departing from the SCA's plain meaning.[222] It would also create national uniformity where none currently exists.

Ideally, new legislation should be enacted that protects against the unauthorized access of electronic communications regardless of where or how the communications are stored. New legislation should not limit protection to communications generated or stored in specific types of media but instead should be crafted to better encapsulate future forms of communication and data sharing. Currently, the SCA focuses on the "stored" aspect of electronic communications

---

[218] *See* Bailey v. Bailey, No. 07-11672, 2008 U.S. Dist. LEXIS 8565, at *2–3 (E.D. Mich. Feb. 6, 2008).

[219] *See* Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 552 (S.D.N.Y. 2008).

[220] *See* Ariana R. Levinson, *Toward a Cohesive Interpretation of the Electronic Communications Privacy Act for the Electronic Monitoring of Employees*, 114 W. VA. L. REV. 461, 461 (2012).

[221] *See In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 511 (S.D.N.Y. 2001) (holding that cookies stored on a plaintiff's computer are not in "electronic storage" for the purposes of the SCA); *see also In re* iPhone Application Litig., 844 F. Supp. 2d. 1040, 1059 (N.D. Cal. 2012) (holding that location data on an iPhone is not in "electronic storage" for the purposes of the SCA).

[222] *In re DoubleClick*, 154 F. Supp. 2d at 513 ("This plain language controls in the absence of any legislative history suggesting that Congress intended it to cover conduct like DoubleClick's.").

as a prerequisite for receiving protection.[223] However, whether information communicated electronically is in "electronic storage"[224] should not rely on any temporal elements. Technological advancements have made it possible to save information in digital form for long, and often indefinite, periods of time.[225] As a result, limiting protection to electronic communications only if they are in "temporary, intermediate storage"[226] no longer serves a valuable purpose for determining what electronic information should or should not receive protection under the law. New legislation is necessary to build off of Congress's expressed intent of not only extending protections for new forms of communications that have resulted due to technological expansion but also to have the law advance with technology.[227]

In creating the SCA, Congress recognized the importance of protecting citizens' privacy.[228] It created the SCA to encourage citizens and businesses to use and participate in these new forms of technology without the fear of being exposed to fewer privacy protections.[229] The creation of new legislation, which indiscriminately protects all electronic communications from unauthorized access, would continue to follow that legislative intent.

Recently, states have recognized the lack of protection certain online communications receive under the current law and have adopted legislation as a means of offering greater protection.[230] Several states, such as Michigan, have enacted laws that ban employers from requesting employees' and job applicants' social

---

[223] 18 U.S.C. § 2701(a) (2006) (prohibiting unauthorized "access to wire or electronic communication while in electronic storage" with a facility).

[224] *Id.* § 2510(17) (defining "electronic storage" as "any temporary, intermediate storage of an electronic communication").

[225] *See iPhone*, *supra* note 106.

[226] 18 U.S.C. § 2510(17).

[227] S. REP. NO. 99-541, at 5 (1986).

[228] *Id.*

[229] *Id.*

[230] *See* H.R. 5523, 96th Leg., Reg. Sess. (Mich. 2012), *available at* http://www.legislature.mi.gov/documents/2011-2012/publicact/pdf/2012-PA-0478.pdf; *see also* H.R. 5684, 112th Cong. (2012), *available at* http://www.gpo.gov/fdsys/pkg/BILLS-112hr5684ih/pdf/BILLS-112hr5684ih.pdf.

media and electronic passwords.[231] These password laws parallel the federal Password Protection Act,[232] a bill recently introduced in Congress that would make employers' requests or coercions for employees to turn over their personal social media and online account passwords illegal.[233] These Acts, both at the state and federal levels, indicate that governments recognize the need to protect individuals' online interactions. The laws, however, deal with only a small area of electronic communication. Such laws only typically prohibit employers from compelling or coercing individuals to turn over computer passwords "for the purposes of employing, promoting or terminating employment."[234] While they are an important step towards offering greater communication privacy, these laws do not address situations like those in *Garcia* in which a password was not needed to access the stored communications.[235]

Uniformity is still nonexistent for electronic communication protection, which leaves victims like Fannie Garcia with inadequate legal recourse. A uniform federal approach should encompass the password protection statutes that have currently been adopted by several states and expand upon those protections to include other forms of access to stored communications. Federal legislation should act as a prohibition against all unauthorized access, regardless of whether a password was requested or demanded for access. Only through broadly defining the law's umbrella of protection and not limiting its scope to specific types of technology will Congress's intention when it enacted the SCA in 1986 be fully realized.[236]

VII. CONCLUSION

---

[231] *See* H.R. 5523.
[232] *See* H.R. 5684.
[233] *Id.* § 2(a)(2)
[234] *Id.* § 2(8)(A).
[235] *See* Garcia v. City of Laredo, 702 F.3d 788, 790 (5th Cir. 2012); *see also* Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 555–56 (S.D.N.Y. 2008).
[236] *See* S. REP. NO. 99-541, at 5 (1986).

The idea that you can prosecute a person for stealing your important papers and effects, but you have fewer abilities to do so if the information stolen was in electronic format seems inconsistent. Under the Fifth Circuit's ruling in *Garcia v. City of Laredo* and the holdings of other courts across the country, that is just the case. Congress, by enacting the SCA, wanted to fill a legal gap that left individuals' electronic communication with little privacy protections under current laws. However, its intent at extending and offering privacy protections to newer electronic communications has been thwarted due to legislative drafting that left SCA-protection stuck in the 1980's. *Garcia*, *In re iPhone*, *In re DoubleClick*, and similar cases indicate the presence of a legal gap, which has left certain electronic and telecommunications vulnerable to unwanted access and exposure.

A new and uniform statutory approach is necessary in order to more adequately ensure that all new and current forms of electronic communication are protected. New legislation should not attempt to fix the law based on current understandings and uses of technology. Instead, it should create guiding principles that continue to remain applicable as technology rapidly changes. Unlike the SCA, and courts' current interpretation of the word "facility," new legislation should not limit protection based on where or how electronic communications are stored. Currently, there exist proposals to amend the Electronic Communications' Privacy Act, including certain portions of the SCA.[237] However, the proposed amendment does little to rectify the gap created by the SCA's antiquated understandings of how electronic communications technology is current used.[238] The Amendment ignores the dangers posed by unauthorized access from private actors[239] and instead focuses on access to electronic communications

---

[237] *See* Matt Sledge, *ECPA Amendment Passes, as Senate Judiciary Votes to Require Warrant for Email Snooping*, THE HUFFINGTON POST (Nov. 29, 2012, 1:10 PM), http://www.huffingtonpost.com/2012/11/29/ecpa-electronic-communications-privacy-act_n_2211889.html.

[238] *See* H.R. 2471, 112th Cong. § 203 (2012), *available at* http://www.judiciary.senate.gov/legislation/upload/Leahy-Substitute-HR-2471.pdf.

[239] *See id.*

by law enforcement.[240] While updating the requirements for access by law enforcement is an important objective, situations like *Garcia* continue to receive little legislative attention. In order to protect people like Fannie Garcia, legislation should encompass all aspects of electronic communications, including elements like online password protection.

Privacy is the "most comprehensive of rights and the most valued by civilized men."[241] If we hold these words to be true, laws should be adapted and updated as technology advances to ensure continued protection of such a valued societal right.

[240] *Id.* (amending the SCA to require law enforcement to obtain a search warrant before "requir[ing] the disclosure by a provider of electronic communication service or remote computing service of the contents of a wire or electronic communication that is in electronic storage with or otherwise stored, held, or maintained by the provider").

[241] Olmstead v. United States, 277 U.S. 438, 478 (1928).

14 N.C. J.L. & TECH. ON. 205, 238
Updating the Stored Communications Act