9200 - 9750

ALAN WILSON
ATTORNEY GENERAL

November 4, 2014

The Honorable Timothy L. Brown
13th Circuit Family Court Judge, Retired
88 Forest Lane
Greenville, SC 29605

Dear Judge Brown:

Thank you for your letter received on March 11, 2014 requesting the opinion of this Office as to the admissibility of certain evidence relating to computer privacy as well as the privacy of electronic communications in a family court proceeding. Specifically, you state:

> First Question: A husband and wife own [as] a family two mobile phone system[s]. Each has been allowed to use the other's phone and there is no password. One party leaves their phone at home and the other party picks it up and in the process of using it notices texts that relate to questions that might affect custody and matters relating to a possible separation. Since texts can be deleted and not recovered the same as emails the party photo[graphs] the text. Are these photos admissible? Is there any civil or criminal liability?
>
> Second Question: [a] husband and wife own a computer. The jointly owned computer has no password to open and use. The parties have exchanged passwords for accounts. One party [husband] decides to check the deposits in a bank account in the other party's name. That party copies the deposit sheets for several months off the front of the bank records. These records could be subpoenaed but the party wants to see them and is not sure if they are needed before they can be s[upplied]. Are these records admissible? Is there any civil or criminal liability?

To answer your questions, we will provide a framework of the law of electronic communication and computer privacy which we believe the spouses in your hypothetical would use in crafting arguments regarding the admissibility of the photographed text messages and copied electronic bank statements.

Law / Analysis

I. Applicable Federal Law

a. Title III of the Omnibus Crime Control and Safe Streets Act of 1968

While privacy law in the United States has Constitutional origins – the Fourth Amendment protecting people "in their persons, houses, papers, and effects, against unreasonable searches and seizures" – it applies to intrusions by the government and its application is scarce to electronically stored information. Sarah Slater, Storage and Privacy in the Cloud: Enduring Access to Ephemeral Messages, 32 Hastings Comm. & Ent. L.J. 365, 371 (2010); see also Orin S. Kerr, A User's Guide to the Stored Communications Act, and a Legislature's Guide to Amending it, 72 Geo. Wash. L. Rev. 1208, 1209-1213 (2004); see, e.g., City of Ontario v. Quon, 560 U.S. 746, 130 S.Ct. 2619 (2010)

(declining to decide whether a police officer, who brought suit against the city, its police department and police chief alleging the police department wrongfully reviewed text messages sent and received on his department owned and issued pager, had a reasonable expectation of privacy).

This being the case, in response to privacy issues arising from telephone technology, Congress enacted the Federal Communications Act in 1934 and later enhanced privacy protections in 1968 with Title III of the Omnibus Crime Control and Safe Streets Act ("Title III"). Id.; see 47 U.S.C.A. § 605(a) (1934); Pub. L. No. 90-351, 82 Stat. 197, 218-21 (1968). The purpose of Title III, also referenced as the Wiretap Act, was to protect against the threat of abuse to privacy rights while still providing a means to combat organized crime. See S. Rep. No. 90-1097, at 43 (1968).

To effectuate its purpose, Title III afforded protection against interception of "wire or oral" communications, while also permitting law enforcement to gather evidence after judicial authorization of a wiretap warrant upon a showing of probable cause that an individual is, has, or is about to commit a particular offence within the Act. See Pub. L. No. 90-351, 82 Stat. 197, 213, 219 (1968). "Wire" communications encompassed communications transmitted by telephone companies and "oral" communications occurred when talking face-to-face. See Pub. L. No. 90-351, 82 Stat. 197, 212 (1968).

b. The Electronic Communications Privacy Act

Faced with the advancements in technology and new methods of communications, Congress enacted the Electronic Communications Privacy Act ("ECPA") in 1986. See Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C.A. §§ 2510-22, 2701-11, 3121-27). Of relevance to this opinion are what were enacted as Titles I and II of the ECPA. Title I amended the Wiretap Act of 1968 to afford privacy protections to wire, oral, and *electronic* communications intercepted in transmission, and Title II, referred to as the Stored Communications Act ("SCA"), provides protection to stored electronic communications. See 18 U.S.C.A. §§ 2510-22 ("Wiretap Act"); 18 U.S.C.A. §§ 2701-12 ("SCA"). Prior to analysis of the Wiretap Act and the SCA, we note that the electronic communications provisions of the ECPA do not contain an explicit marital exception, and it appears no court has applied one. See Spy vs. Spouse: Regulating Surveillance Software on Shared Marital Computers, 105 Colum. L. Rev. 2097, 2117-18 (Nov. 2005); see, e.g., White v. White, 344 N.J. Super. 211, 217-18, 781 A.2d 85, 89 (N.J. Super. Ct. Ch. Div. 2001) (stating that "the New Jersey Wire Tap Act applies to unauthorized access of electronic communications of one's spouse. . . . ").

i. The Amended Wiretap Act: Privacy of Electronic Communications in Transit

Title I of the ECPA amended the former Wiretap Act by including "electronic communications" among the types of communication protected from interception. Compare Pub. L. No. 90-351, 82 Stat. 197, 213 (1968) with 18 U.S.C.A. § 2511(1).. Currently under the Wiretap Act, it is illegal if any person "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C.A. § 2511(1)(a).[1] In addition to criminal liability, the Wiretap Act also permits private civil action and the recovery of civil damages. See 18 U.S.C.A. § 2520(a).

The Wiretap Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C.A. § 2510(4). In order to "intercept" an "electronic communication," federal courts have

[1] The South Carolina Wiretap Act is modeled after the Federal Wiretap Act. See S.C. Code Ann. § 17-30-10 et seq. Pursuant to S.C. Code Ann. § 17-30-20 (2014) it a felony for a person to "intentionally intercept [ ], attempt[ ] to intercept, or procure[ ] any other person to intercept to attempt to intercept any wire, oral, or electronic communication."

consistently held that electronic communications must be acquired contemporaneously with transmission and are not intercepted within the meaning of the Federal Wiretap Act if they are retrieved from storage. O'Brien v. O'Brien, 899 So.2d 1133, 1136 (Fla. Dist. Ct. App. 2005) (citing Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107 (3d Cir. 2003); Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2003); United States v. Steiger, 318 F.3d 1039 (11th Cir. 2003); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002)). Usually arising in the context of email interception in domestic relations proceedings, application of the Wiretap Act has often resulted in the conclusion that protection is afforded to those emails intercepted in-transit through mechanisms such as spyware, but not when an email is merely stored on the hard drive of one's computer. See supra "Case Law Application."

Damages permitted in association with a civil action under the Wiretap Act are set forth in 18 U.S.C.A. 2520, and the criminal punishments for the various violations within the Act are found in 18 U.S.C.A. § 2511(4)(a) and 18 U.S.C.A. § 2512(1). In addition, the Wiretap Act contains an exclusion of evidence provision, mandating the exclusion of any unlawfully obtained *wire or oral* communication from use as evidence in any proceeding. 18 U.S.C.A. § 2515. Thus, the Federal exclusionary provision does not extend to electronic communications. See id.[2]

ii. The Stored Communications Act: Privacy of Stored Internet Communications

The SCA provides protection to stored communications and punishes "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. . . ." 18 U.S.C.A. § 2701(a)(1)-(2) (emphasis added). "Electronic storage" is defined 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.A. § 2510(17). In addition to criminal liability, the SCA permits civil action pursuant to 18 U.S.C.A § 2707.

The appropriate relief and damages permitted in association with a civil action under the SCA are set forth in 18 U.S.C.A. 2707(b)-(c), and the criminal punishment for unlawful access to stored communications is found in 18 U.S.C.A. § 2701(b). Unlike the Wiretap Act, the SCA does not provide an exclusion of evidence remedy.

iii. Case Law Application

While South Carolina law provides some guidance on application of the SCA, cases decided in other jurisdictions provide additional insight on the application of the Wiretap Act and the SCA in the context of discovery in divorce and child custody proceedings. Although the majority of cases we have uncovered in researching this opinion involve the discovery of email communications, in recent opinions, courts have applied the ECPA in the context of text messaging. We will provide an overview of both below.

Evans v. Evans, 169 N.C. App. 358, 610 S.E.2d 264 (N.C. Ct. App. 2005) involved a divorce and child custody proceeding from which the wife appealed. Among the wife's arguments on appeal were that the trial court committed reversible error by admitting into evidence sexually explicit emails recovered from the hard drive of the family computer that she exchanged with her paramour. Id. at 366,

[2] See S.C. Code Ann. § 17-30-110 (2014) for South Carolina Wiretap Act's exclusionary remedy (stating that unless otherwise provided by federal law, all South Carolina Rules of Evidence Apply and permitting "any aggrieved person" "to move to suppress the contents of any intercepted wire, oral, or electronic communication, or evidence derived therefrom. . . . ").

610 S.E.2d at 270-71. Wife contended that the emails should not have been admitted on the basis that they were illegally intercepted pursuant to 18 U.S.A. § 2511(1)(c) and (d), which prohibit the disclosure or use of any electronic communication intercepted in violation of the ECPA's Wiretap Act. Id. In its analysis, the Evans Court acknowledging that:

> most courts examining this issue have determined that interception under the ECPA must occur contemporaneously with transmission. Here, the e-mails were stored on, and recovered from, the hard drive of the family computer. The e-mails were not intercepted at the time of transmission.

Id. (citations omitted). Thus, finding no violation of the ECPA, the North Carolina Court of Appeals affirmed the trial court's admission of the emails into evidence. Id.

White v. White, 344 N.J. Super. 211, 214-15, 781 A.2d 85, 86-87 (N.J. Super. Ct. Ch. Div. 2001) is also worthy of analysis as it involved a divorce action and custody dispute where husband moved to suppress emails exchanged with his girlfriend stored on the hard drive of the family computer that were offered into evidence by wife. Husband contended wife's access of the emails violated the New Jersey Wiretap Act, and in particular, provisions in the statute mirroring the Federal Stored Communications Act. Id. See N.J.S.A. 2A:156A-27(a) (A person is guilty of a crime . . . if he (1) knowingly accesses without authorization a facility through which an electronic communication service is provided or exceeds an authorization to access that facility, and (2) thereby obtains, alters, or prevents authorized access to wire or electronic communication while the communication is in electronic storage"). Additionally, the Court expanded on whether the emails were "intercepted," and thereby a violation of the Wiretap Act. White v. White, 344 N.J. Super. 211, 222, 781 A.2d 85, 91 (2001).

First, in its analysis of what constitutes "electronic storage," for purposes of New Jersey's version of the SCA, the court expanded on the stages of storage an email enters into in the process of being sent and delivered. Id. at 89-90, 781 A.2d at 219. In short, once an email is sent, it is placed in what is called "temporary" or "immediate" storage and also in "back-up protection" in the event the system crashes prior to completion of transmission of the email. Id. Next, once transmission is complete when the recipient logs on the system and retrieves the email from immediate storage, the email is placed in "post-transmission storage." Id. Finding that husband's emails stored on the family computer's hard drive were emails merely "retrieved by the recipient and then stored" the Court noted that was not the type of storage intended to be protected by the Act. Id. at 90, 781 A.2d at 220. The Court reasoned that:

> [t]he conclusion that the Act does not apply to electronic communications received by the recipient, placed in post-transmission storage, and then accessed by another without authorization, appears to make sense, when one considers the 'strong expectation of privacy with respect to communication in the course of transmission significantly diminishes once transmission is complete.'

Id. (citing Fraser v. Nationwide Mutual Ins. Co., 135 F.Supp.2d 623, 638 (2001), vacated in part on other grounds, 352 F.3d 107 (3rd Cir. 2004)).

The Court also noted that the wife's access to the computer was not "without authorization," a requisite factor under the SCA, reasoning that while she did not regularly use the computer, the term "without authorization" means "using a computer from which one has been prohibited or using another's password or code without permission." Id. at 221, 781 A.2d at 90 (citing Sherman & Co. v. Salton Maxim Housewares, Inc., 94 F.Supp. 2d 817 (E.D. Mich. 2000). Also, it stated that "where a party 'consents to another's access to its computer network, it cannot claim that such access was unauthorized.'" Id., 781

A.2d at 91 (quoting Sherman, 94 F.Supp.2d at 821 (E.D. Mich. 2000)). As the emails were neither in "electronic storage" nor accessed "without authorization" the Court did not find a violation of the N.J. statute nearly identical to the SCA. Id. at 224, 781 A.2d at 92.

Last, in regards to the Wiretap Act, we point out that the Court also found wife did not "intercept" husband's emails due to the impossibility of interception when an email is in post-transmission storage: "[h]ere, the electronic communications has already ceased being in 'electronic storage' as defined by the Act. They were in post-transmission storage-therefore defendant did not intercept them." Id. at 221, 781 A.2d at 91. Thus, finding no "interception" occurred, wife was also not in violation of the Wiretap Act.

In O'Brien v. O'Brien, 899 So.2d 1133, 1134 (Fla. Dist. Ct. App. 2005), wife appealed the trial court's denial of her motion for a rehearing to determine whether it erroneously refused to admit into evidence electronic communications between husband and another woman found on a computer by wife with secretly installed spyware. In its analysis, the court looked to the language of the Florida Security of Communications Act, molded after the Federal Wiretap Act, and noted that "[t]he core of the issue lies in whether the electronic communications were intercepted." Id. at 1135. Concluding that the communications were "intercepted" for purposes of the Act, the Court distinguished between obtaining already stored information on a computer's hard drive with information intercepted contemporaneously with transmission. Id. at 1136-37. Because the spyware wife installed on the computer intercepted the electronic communication contemporaneously with transmission, copied it, and routed the copy to a file in the computer's hard drive, it concluded the electronic communications were intercepted and accessed in violation of the Florida Wiretap Act. Id. at 1137.

Despite wife's violation of the Wiretap Act, the Court noted that, like its Federal counterpart, the Florida Wiretap Act's exclusionary provision only prohibits admission of intercepted *wire or oral communications* into evidence, thereby conspicuously leaving out intercepted "electronic communications." Id. Yet, despite the possible admissibility of the emails, the Florida Court of Appeals upheld the trial court's exclusion of the wrongfully intercepted electronic communications finding that admission of evidence is in the sound discretion of the trial judge that should not be disturbed absent abuse of discretion. Id. at 1137-38 ("Because the evidence was illegally obtained, we conclude that the trial court did not abuse its discretion in refusing to omit it.").

Next, we make note of Jennings v. Jennings, 401 S.C. 1, 736 S.E.2d 242 (2012), decided by our own Supreme Court. Emanating from a domestic dispute, the issue before the court was whether emails between husband and paramour, accessed by wife's daughter-in-law after guessing his password security questions correctly, were held in "electronic storage" thereby affording protection under the Stored Communications Act. Id. at 3, 736 S.E.2d at243. Looking to the definition of "electronic storage" – "(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" – the Court relied on the plain meaning of the word "backup" and "decline[d] to hold that retaining an opened email constitute[d] storing it for backup protection under the Act." Id.at 5-7, 736 S.E.2d at 244-45.[3] While the Court held no claim existed

[3] In a separate concurring opinion, Chief Justice Toal's reasoning parted with the majority opinion:
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 been opened by the recipient, it is in electronic storage.
Jennings v. Jennings, 401 S.C. 1, 12, 736 S.E.2d 242, 248 (2012). Also, Justice Pleicones wrote separately, noting his agreement 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, §

under the SCA because the emails were not in electronic storage, it warned that "this should in no way be read as condoning [daughter-in-laws] behavior." Id. at 7, 736 S.E.2d at 245.

We will now point out recent cases that have applied the ECPA in the context of text messaging. Similar to the "email cases" above, these cases also involve analysis of "interception" and "electronic communications" in the context of the Wiretap Act and consider the term "electronic storage" under the SCA.

First we mention Commonwealth v. Moody, 466 Mass. 196, 993 N.E.2d 715 (Mass. 2013), which clarifies that the Wiretap Act applies to text message communications. One issue before the Court was Defendants' motion to suppress evidence obtained as a result of search warrants issued under the Massachusetts Wiretap Act permitting law enforcement's interception of text messages on Defendants' cell phones. Id. at 207-08, 993 N.E.2d at 723-24. The Moody Court, looking to the Federal Wiretap Act for guidance, clarified that the term "electronic communication" added in 1986 under the ECPA, "plainly includes the transmission of text messages." Id. at 203, 993 N.E.2d at 720. Also of relevance, the Court noted the amendment to the term "intercept" – "the aural *or other* acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" – which it claimed illustrated Congress' intent that the term include "the acquisition of not only the human voice, but also other forms of communication." Id. at 203, 993 N.E.2d at 720. Under this analysis, the Court concluded that the Massachusetts Wiretap Act "provides protection for the electronic transmission of text messages consistent with the protections currently provided in Title III . . . . Id. at 209, 993 N.E.2d at 724.

Next, in Martin v. State, 218 Md.App. 1, 96 A.3d 765 (Md. Ct. Spec. App. 2014), Defendant appealed his attempted murder conviction on the ground that the circuit court erred in denying his motion to suppress text messages retrieved by police from the victim's cell phone, alleging a violation of the Maryland Wiretap Act. In its analysis, the court compared the Maryland Wiretap Act (stating it is unlawful for any person to "willfully *intercept*, endeavor to intercept, or procure any other person to intercept or endeavor to intercept any wire, oral, or *electronic communication*"[4]) to its nearly identical Federal counterpart to determine the appropriate application of the terms "intercept" and "electronic communications." Id. at 15-19, 96 A.3d 765, 773-76 (analyzing Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002); United States v. Steiger, 318 F.3d 1039 (11th Cir. 2003)). As a result, the Court found that:

> [i]n light of the nearly identical definitions of 'intercept' and 'electronic communications' in both the Federal and Maryland Wiretap Acts. . . we shall join the federal courts in construing 'intercept' as requiring 'acquisition contemporaneous with transmission' of the messages. . . 'intercept' does not occur when, conversely, the electronic communication was in storage at the time of acquisition.

Id. at 19, 96 A.3d at 776. Because the text messages on the victim's phone were, "at the time of their seizure already stored in that phone," the Court concluded they were not unlawfully intercepted in violation of the Wiretap Act. Id.

The Martin Court also pointed out that the Maryland Wiretap Statute, like the Federal Wiretap Act, "prohibits interceptions that occur 'through the use of any electronic, mechanical, or other device.'" Id. (citing Md. Code Ann. § 10-401(10)). Since a cell phone is not considered a "device" under the Act,

---

2510(17)(B)" but distinguishing his opinion that because the two types of storage are distinct from one another, an email is protected if it falls under the definition of subsections (A) or (B). Id. at 14, 736 S.E.2d at 248-49.

[4] Md. Code Ann., § 10-402(a)(1) (emphasis added).

as it is specifically excluded by definition, this strengthened the Court's conclusion that the text messages in the victim's cell phone were not covered by the Act. Id.

Last, the Court briefly touched on the Maryland SCA[5], rejecting defendant's argument that it should apply to text messages obtained from the victim's cell phone. Id. at 20, 96 A.3d at 776. It stated that a cell phone "is not a 'facility through which an electronic communication service is provided,' but presumably to the network infrastructure (such as the cell phone tower, its transmitters, and servers and switches), which is managed and operated by cell phone service providers." Id., 96 A.3d at 777. As victim's cell phone was not a "facility" pursuant to the Act, allegations of violation of the Maryland SCA failed, but, for the sake of argument, even if the cell phone was considered a facility, suppression of the text messages would not be mandatory due to the absence of a statutory exclusionary rule under the SCA. Id.

This was the same conclusion reached in Garcia v. City of Laredo, Texas, 702 F.3d 788 (5th Cir. 2012), involving allegations of unauthorized access under the SCA to text messages found on police dispatcher's cell phone leading to her termination. The Garcia Court concluded that the dispatcher's cell phone was not a "facility" within the meaning of the SCA, and even if it was, no proof was provided that the text messages were obtained from "electronic storage." Id. at 793. Alternatively, the text messages were merely stored on the cell phone and were therefore outside the scope of the statute. Id.

c. Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act ("CFAA") is also applicable to your questions relating to computer privacy. Under the CFAA it is a crime to (1) access a computer without authorization and (2) to access a computer by exceeding the authorization given. See 18 U.S.C.A. 1030(a)(2), (c). The CFAA was originally passed in 1984 to prosecute crimes of federal interest. See S. Rep. No. 99-432, at 4 (1986). Since enactment, numerous amendments to the CFAA have been made[6] and, as of 1994, the Act provides for a private cause of action to allow victims to recover damages as a civil remedy against wrongdoers. See 18 U.S.C.A. 1030(g).

Computers covered under the Act have broadened over time. The term "federal interest computer" was replaced with "protected computer" in 1996, and the definition of "protected computer" was expanded in 2008 to include computers "affecting interstate commerce." See 18 U.S.C.A. § 1030(e)(2)(B). Today, a "protected computer" under the Act is any computer or device capable of connecting to the internet. See Cont'l Group, Inc. v. K.W. Prop. Mgmt., LLC, 622 F.Supp.2d 1357, 1370 (S.D. Fla. 2009) ("A connection to the internet is affecting interstate commerce and communication" (quotations omitted)).

Under the CFAA, criminal and civil liability is established when an individual: (1) intentionally access a computer "without authorization" or "exceeds authorized access," and (2) engages in one of seven types of prohibited conduct, including: (1) obtaining national security information, (2) compromising the confidentiality of a computer; (3) trespassing in a Government computer; (4) accessing

---

[5] Maryland's SCA forbids "obtain[ing] . . . access to a wire or electronic communication while it is in electronic storage in an electronic communications system b: (1) [i]ntentionally accessing without authorization a facility through which an electronic communication service is provided; or (2) [i]ntentionally exceeding an authorization to access a facility through which an electronic communication service is provided." Md. Code Ann. § 10-4A-02(a).

[6] The CFAA has been amended in 1986, 1988, 1989, 1990, 1994, 1996, 2001, 2002, and 2008. See U.S. Dept. of Justice, Prosecuting Computer Crimes, at 2 (2007), available at http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf.

a computer to defraud and obtain value; (5) transmission or access that causes damage; (6) trafficking in passwords; and (7) extortion involving threats to damage computer. See 18 U.S.C.A. § 1030(a)(1)-(7).

A private, civil cause of action must involve violations of the statute that constitute a felony under the criminal law. Peter A. Winn, The Guilty Eye: Unauthorized Access, Trespass, and Privacy, 62 Bus. Law. 1395, 1405 (2007). As explained:

> [m]ere unauthorized access alone constitutes a misdemeanor offense, and does not provide a basis for a private claim. The predicate for a civil cause of action, then, is the unauthorized obtaining of private or confidential information, which is used for commercial advantage, private financial gain or to commit any criminal or tortious act. It also includes unauthorized access to particularly sensitive financial and health care records. The private cause of action is limited to SERIOUS invasions of privacy and other tortious acts; there is no private cause of action for any entry into a computer system which simply displeases or annoys the owner of a computer.

Id. (internal quotations omitted) (emphasis in original).

It has been held that whether one is authorized to access a protected computer network under the CFAA should be determined "on the basis of the expected norms of intended use." Global Policy Partners, LLC v. Yessin, 686 F.Supp.2d 632, 636 (2009) (citations omitted). In application, Courts have held that use of another's password to access a website without a website owner's permission may constitute "unauthorized access" under the CFAA. See A.V. ex rel. Vanderhye v. iParadigms, LLC, 562 F.3d 630, 645-46 (4th Cir. 2009); State Analysis, Inc. v. Am. Fin. Assocs., 621 F.Supp. 2d 309, 316 (E.D.Va. 2009).

II. Common Law: Invasion of Privacy

Last, we mention the common law tort of invasion to privacy. Various causes of action can be brought under the common law relating to the right of privacy, however, the cause of action of particular relevance to this opinion is the tort of "intrusion upon seclusion." See Restatement (Second) of Torts § 652A (1977). Under the tort of intrusion upon seclusion, "one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for the invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." Restatement (Second) of Torts, § 652B (1977). The Restatement's comments indicate that,

> [t]he invasion may be by physical intrusion into a place in which the plaintiff has secluded himself . . . [or] [i]t may also be by the use of the defendant's senses, with or without mechanical aids, to oversee or overhear the plaintiff's private affairs, as by looking into his upstairs windows with binoculars or tapping his telephone wires. It may be by some other form of investigation or examination into his private concerns, as by opening his private and personal mail, searching his safe or his wallet, examining his private bank account, or compelling him by a forged court order to permit an inspection of his personal documents.

Id. at cmt. b. Analysis turns on the fact that the intrusion must be "highly offensive to a reasonable person." See, e.g. Froelich v. Werbin, 219 Kan. 461, 464, 548 P.2d 482, 484 (1976). A reasonable person cannot conclude that an intrusion is highly offensive when the actor intrudes onto an area in which the victim has either a limited or no expectation of privacy. White v. White, 344 N.J.Super.211, 222, 781 A.2d 85, 92 (N.J. Super. Ct. Ch. Div. 2008).

In White v. White, also discussed infra in reference to the Wiretap Act and SCA, the Court analyzed one's expectation of privacy in the context of information stored on a computer co-owned by husband and wife. Id. at 222-24, 781 A.2d at 91-92. The Court found no expectation of privacy existed since both parties consented to access by the other. Id. at 223, 781 A.2d at 92. It compared wife's search on the hard drive of the computer to a search through a file cabinet in a room to which the wife had complete access. Id. at 223, 781 A.2d at 91 (discussing Del Presto v. Del Presto, 97 N.J. Super. 446, 456, 235 A.2d 240, 246 (N.J. Super. Ct. App. Div. 1967) that held "having a legitimate reason for being in the files, plaintiff had a right to seize evidence she believed indicated her husband was being unfaithful"). Comparing the case before it to Del Presto, the White Court noted that "rummaging through files in a computer hard drive was "not really" different than rummaging through files in an unlocked file cabinet. Id. at 224, 781 A.2d at 91. Thus, the court held that wife's actions did not intrude upon husband's common law right to seclusion. Id. Other courts have found an expectation of privacy on shared computers as long as the information in question is password protected. See, e.g., Trulock v. Freeh, 275 F.3d 391 (4th Cir. 2001) ("By using a password, Trulock affirmatively intended to exclude Conrad and others from his personal files. . . . Thus, Trulock has a reasonable expectation of privacy in the password-protected computer files and Conrad's authority to consent to the search did not extend to them.").

III. Admissibility

Of the privacy causes of action discussed above, only the Wiretap Act contains an exclusionary remedy. See 18 U.S.C.A. § 2515 ("Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence. . . ."). However, the Wiretap Act's exclusionary remedy only prohibits wrongfully obtained wire or oral communications from evidence, not electronic communications. See id. Thus, even if text messages or email communications (or any other "electronic communication") were obtained in violation of the Wiretap Act, admission into evidence would not be prohibited through the Act.

In regards to the admissibility of text messages, email communications, or other electronically stored information, which would likely be in the form of photographs or copies, several evidentiary obstacles concerning admissibility will have to be overcome. These include establishing relevancy of the communication; authenticating that the communication is what its proponent claims; determining a hearsay exception if the truth of the content of the message is relevant rather than the mere existence of the message; compliance with the original writing or best evidence rule; and weighing the communication's probative versus prejudicial value. See generally Monique C.M. Leathy, Am.Jur.Trials 433, Civil Liability for Text Messaging § 14 (2014). However, even if these obstacles are overcome, court's generally disfavor "self-help discovery" and abiding by the applicable rules of discovery are advised.

Conclusion

While it is our understanding the facts you have presented and the questions you raise in your correspondence are for educational purposes, this Office, as a matter of policy cannot answer hypothetical questions, opine on potential lawsuits, or review factual questions. See Op. S.C. Att'y Gen., 2014 WL 2884612 (June 10, 2014). In keeping with our policy, we are not able to draw specific conclusions on the hypotheticals you raise. Nonetheless, we summarize that the EPCA affords protection to wireless communications, which courts have extended to text message communications. For protection to be afforded under the Wiretap Act, it has been continuously held that communication must be intercepted at transmission, not merely accessed from storage. Furthermore, wrongful interception of wire or oral communications result in exclusion of the evidence from trial, but no such provision exists for electronic communications.

In regards to the Stored Communications Act, courts have held that access must be "without authorization" and obtained from "electronic storage." Moreover, in the realm of text messaging, courts have also held that cell phones are not considered a "facility" within the meaning of the SCA. Even if a court were to hold a cell phone is a facility, arguments can be made that text messages stored on a phone are not in "electronic storage" within the meaning of the Act and also that the SCA does not contain an exclusionary remedy even if a violation of the SCA was found.

Next, the CFAA applies to unauthorized access to a protected computer or exceeding authorized access on a protected computer. In addition, a serious, felonious invasion of privacy must also be present.

Finally, for success on a claim of intrusion to seclusion, the intrusion must be highly offensive to a reasonable person. In other words, a claim will likely fail where the victim has a very limited or no expectation of privacy in the area intruded. The expectation of privacy in a co-owned computer is low; however, privacy expectations increase when files are password protected and the owner of the files has not consented to another's use of the password to access the files.

We hope this analysis proves helpful in answering your inquiries regarding the current law of computer privacy and privacy of electronic communications. Should you have additional questions, please do not hesitate to contact our Office.

Sincerely yours,

Anne Marie Crosswell

Anne Marie Crosswell
Assistant Attorney General

REVIEWED AND APPROVED BY:

Robert D. Cook

Robert D. Cook
Solicitor General