PRIVACY LIABILITY FOR DATA BREACH AND REMEDIES

PIERRE GROSDIDIER, *Houston*
Haynes and Boone, LLP

State Bar of Texas
FAMILY LAW & TECHNOLOGY:
Keeping Your Family Law Practice in Pace with the Latest Technological Advances
December 8-9, 2016
Austin

CHAPTER 16

Pierre Grosdidier
Haynes and Boone, LLP
1221 McKinney Street, Suite 2100
Houston, TX 77010
713.547.2272

BIOGRAPHICAL INFORMATION

Education

B.Eng., Chemical Engineering, McGill University, 1980, with distinction
Ph.D., Chemical Engineering, California Institute of Technology, 1986
J.D., University of Texas at Austin School of Law, 2007, with honors

Professional Activities

Pierre Grosdidier worked as a consulting engineer for 18 years before becoming a lawyer. He now leverages his engineering, computer, and business background to litigate cases that involve complex technical and commercial disputes. Pierre is at ease with the most complex technologies whether in the energy, construction, computer, or manufacturing industries. He has represented clients in lawsuits and arbitrations that arose from construction defects, industrial accidents, environmental contamination, oil and gas drilling operations, engineering services projects, computer and software projects, copyright and software copyright infringements, computer piracy, and trade secret thefts. Pierre's litigation experience also includes claims under the Stored Communications Act and the Computer Fraud and Abuse Act, including one where the defendant planted a "time bomb" in his employer's computer system. Pierre leverages his software and project management experience to efficiently organize and lead complex ESI preservation, collection, and review projects. He is a prolific writer.

Selected Publications

- *Data Breaches, Big Data, and FTC Oversight*, presenter, InfraGard Health Care SIG, Sept. 1, 2016.
- *Admissibility and Authentication of Electronic Evidence*, presenter, 2016 State Bar of Texas Annual Meeting, June 17, 2016.
- *A Modern Whodunit: Non-compliant DMCA § 512 'Takedown' Notifications Might Prevent a Copyright Owner from Learning an Alleged Infringer's Identity,* State Bar of Texas, Computer and Technology Section's Circuits Newsletter, September 2, 2015.
- *Three Threshold Questions Every Attorney Must Answer before Filing a Computer Fraud Claim,* Excerpted from Circuits – Newsletter of the Computer & Technology Section Summer 2015.
- *Don't Look To SCA in BYOD-Termination Remote Wipe Cases*, Law360, Mar. 17, 2015.
- *When Employees Leave with Electronic Files: The CFAA's Eclectic Damage and Loss Case Law Illustrated*, co-author, Bloomberg BNA Electronic Commerce & Law Report, May 21, 2014.
- *When Hacking an Email Account Doesn't Violate the SCA*, Law360, Dec. 11, 2013; updated Nov. 3, 2016.
- *Pitfalls Await Those Who Do Not Think Through TTLA Claims*, guest author, Law360, Oct. 15, 2013.
- *Choose Your Friends – and Privacy Settings – Wisely*, guest author, Law360, October 2, 2013.
- *The Danger With Time Bombs - Can Your Software Vendor Lock Up Your Software so That You Have to Buy an Upgrade? Maybe not,* ControlGlobal.com, October 2011 (Updated, Oct. 1, 2015).

See all P. Grosdidier's publications at http://www.haynesboone.com/people/g/grosdidier-phd-pierre
Disclosure: parts of this article are based on material drawn from some of the above publications.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes and Rules

Other Authorities

PRIVACY LIABILITY FOR DATA BREACH AND REMEDIES

I. INTRODUCTION

The term “data breach” usually brings to mind the much-publicized capture of vast quantities of consumer information from retail vendors (*e.g.*, Target, Windham), on-line service providers (*e.g.*, Yahoo!), or social media sites (*e.g.*, Ashley Madison). Hackers’ motives are presumably as diverse as the hackers themselves, but clearly include obtaining marketable information, such as credit card numbers and intellectual property, or embarrassing consumers, as in the Ashley Madison breach. Recent events also show that motives now possibly include political agendas with media reports that foreign hackers may even attempt to influence U.S. elections. Of course all this activity is criminal. “Guccifer,” the Romanian hacker involved in the disclosure of Hillary Clinton’s private email server when she served as Secretary of State, was extradited from his home country and recently sentenced to 52 month of prison after a plea bargain.[1]

This picture of data breaches is accurate, but incomplete. Data breaches occur on a small scale as well. The mere unauthorized access of a lone computer, web-based email account, social media account, or even cell phone is a data breach. In a family law context, such breaches typically occur when an estranged spouse accesses his or her soon-to-be ex’s emails or cell phone without the ex’s knowledge or consent. The motive in these cases is usually to try to expose infidelity, or to get a step up in a divorce or custody proceeding, or both. Although far less likely to be criminally prosecuted, such conduct is civilly actionable under a variety of tort theories and statutory provisions. This article discusses the statutory claims that a victim can assert against his or her snooping spouse, or ex-spouse, under the Computer Fraud and Abuse Act (18 U.S.C. § 1030, the “CFAA”), the Stored Communications Act (18 U.S.C. §§ 2701–2711, the “SCA”), and the Texas Harmful Access by Computer Act (Tex. Civ. Prac. & Rem. Code Chap. 143, the “HACA”). As noted, victims can also assert other tort claims such as invasion of privacy or intentional infliction of emotional distress, for example. But these claims are not within the scope of this article.[2]

Plaintiff’s counsel is instinctively tempted to assert CFAA and SCA claims in data breach cases, if only based on the statutes’ strength and name recognition, especially the CFAA’s. This temptation also seems to prevail in family law cases, such as when a dejected or rejected spouse snoops into the other’s personal emails or phone. The statutory language’s complexity and the case law’s sparseness (in Texas) and fragmentation (nationwide) invite caution, however. The CFAA is a criminal statute with a narrowly defined civil cause of action and a high $5,000 loss threshold. Absent *bona fide* pecuniary harm to a family business, a family law plaintiff will struggle to meet this threshold.

The SCA is a 1986, dawn-of-Internet, statute intended for email technology that has since greatly evolved. To some extent, today’s email technology must be shoe-horned into the SCA’s 1986 language. The SCA’s language is narrow and difficult, and its case law is fragmented, as is the CFAA’s. Both statutes, therefore, invite dismissal motion practice when pleaded. As everyone knows motion practice is expensive, especially in federal court. The prospect of defending weak CFAA or SCA claims in expensive dismissal proceedings should temper any inclination to assert these claims in family law cases.

Texas, like all other states, has enacted a broadly-worded criminal statute to deal with unauthorized computer access.[3] This statute, Texas Penal Code Chapter 33, Computer Crimes, was strengthened in 2015

[1] *See* http://www.reuters.com/article/us-usa-cyber-guccifer-idUSKCN1175FB.

[2] Also, no cause of action stands under the Fourth Amendment against a person who searched another’s emails, computer, or cell phone. The U.S. Supreme Court has long held that the Fourth Amendment does not apply to private searches, even unreasonable ones. *United States v. Jacobsen*, 466 U.S. 109, 113 (1984).

[3] *See* http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx.

with language intended to address violations of contractual computer-use agreements, *inter alia*.[4] The HACA provides a civil cause of action to any "person who is injured or whose property has been injured as a result of a" Penal Code Chapter 33 violation, provided that the wrongdoer acted "knowingly or intentionally."[5] The HACA is a powerful tool for victims of computer crimes. It is not bridled by the CFAA's $5,000 loss threshold, nor by the SCA's narrow and convoluted language.

The take-away for family law counsel dealing with an intra-spousal data breach is to carefully think through the merits of asserting CFAA and SCA claims to assess whether the chances of surviving a motion to dismiss justify the requisite effort and expense. Counsel can almost always fall back on a simpler and no-less-effective HACA claim—provided the plaintiff satisfies the injury element of the claim.

II. CLAIMS UNDER THE CFAA

A. Key elements of a CFAA civil claim

The CFAA is a broadly-worded criminal statute that proscribes unauthorized access to protected computers, or access that exceeds authorization. "Protected computers" include computers that are "used in or affecting interstate or foreign commerce or communication."[6] Under this broad definition, any computer that is connected to Internet is a protected computer under the CFAA.[7] Since most home computers are now connected to Internet for email and web surfing, it follows that these computers are subject to the CFAA. Likewise, a cell phone, even if used only for calls and text messages, is a computer under 18 U.S.C. § 1030(e).[8]

The statute also provides a victim with a private cause of action.[9] The CFAA's § 1030(g) is often a civil plaintiff's go-to federal statute in cases of unauthorized computer access. As the discussion below shows, its suitability in family law disputes hinges largely on whether the defendant's conduct involves monetary harm, to a family business, for example.

Two threshold issues govern CFAA claims.[10] The first is whether the defendant's conduct constitutes "unauthorized access." This issue is unsettled and depends on whether the forum Circuit Court of Appeals construes "unauthorized access" broadly or narrowly. The second issue is whether the plaintiff has the requisite statutory damage or loss, or both. The answer to this important question depends on the forum district court and the facts of the case (few Circuit Court decisions directly address the issue, and the case law is fragmented).

[4] Acts 2015, 84th Leg., R.S., Ch. 154 (H.B. 896), Sec. 1, eff. Sept. 1, 2015; *id*., R.S., Ch. 1251 (H.B. 1396), Sec. 23, eff. Sept. 1, 2015.

[5] Tex. Civ. Prac. & Rem. Code § 143.001(a).

[6] 18 U.S.C. § 1030(e)(2)(B). The CFAA distinguishes between "computers" and "protected computers." There is no need to dwell on this distinction for the purpose of this article.

[7] *See United States v. Nosal*, 676 F.3d 854, 859 (9th Cir. 2012) (the CFAA's "broadest provision is subsection 1030(a)(2)(C), which makes it a crime to exceed authorized access of a computer connected to the Internet *without* any culpable intent.") (emphasis in original); *Merritt Hawkins & Assocs., LLC v. Gresham*, 948 F. Supp. 2d 671, 673–74 (N.D. Tex. 2013) (citing cases) ("In the CFAA, Congress defines a protected computer as a computer that is used in or affecting interstate or foreign commerce or communication. . . . Pleading specific facts that the defendant accessed a computer connected to the internet is sufficient to establish that the accessed computer was 'protected.'").

[8] *United States v. Kramer*, 631 F.3d 900, 902–03 (8th Cir. 2011) ("The language of 18 U.S.C. § 1030(e)(1) is exceedingly broad. . . . This definition captures any device that makes use of a [sic] electronic data processor, examples of which are legion. . . . Therefore we conclude that cellular phones are not excluded by this language.").

[9] 18 U.S.C § 1030(g).

[10] For additional details on this topic, *see* Pierre Grosdidier, *Three Threshold Questions Every Attorney Must Answer before Filing a Computer Fraud Claim*, excerpted from Circuits – Newsletter of the Computer & Technology Section Summer 2015.

B. Unauthorized access under the CFAA

The CFAA's § 1030(a) bars at least seven types of activities, several of which involve government or financial institution computers. These prohibited activities are improbable grounds for claims in private civil litigation. Most civil CFAA claims between private parties arise under §§ 1030(a)(2)(C) (obtaining information from any protected computer), (a)(4) (accessing a protected computer intending to defraud), or (a)(5) (causing damage to a protected computer). In family law litigation, one would expect, and the case law generally shows, that "obtaining information" without authorization, or by exceeding authorized access, is the most likely ground for a CFAA claim against a snooping spouse.

The CFAA does not define unauthorized access (it only defines "exceeds authorized access"), and courts of appeals are split on whether to construe the term "unauthorized" broadly or narrowly. Access that circumvents a password is almost always unauthorized. Access would be unauthorized, for example, if a spouse accessed the other spouse's web-based email account after securing the password through surreptitiously installed keylogger software on the family computer.[11] The issue is less clear when spouses voluntarily shared each other's email account passwords. Is such access unauthorized even though a spouse proceeded with a password provided freely by the other spouse at a time of greater spousal harmony (assuming the other spouse did not change password at the onset of marital discord)? Circuit Courts are famously split on this issue.

The Fifth Circuit construed "unauthorized access" broadly. In *United States v. John*, a criminal case, the Fifth Circuit held that an employee exceeded authorized access when the employee accessed a system in violation of his or her employer's computer-use policy using an otherwise valid password.[12] John worked in a bank and passed on computer-stored customer account information to a relative, who used the information to orchestrate frauds. John had attended bank training programs that delineated the limits of her authority to use the bank's computer systems and customer information. A trial court found her guilty of "exceeding authorized access to a protected computer in violation of 18 U.S.C. §§ 1030(a)(2)(A) and (C)." The Fifth Circuit upheld the conviction, reasoning in part that "when an employee knows that the purpose for which she is accessing information in a computer is both in violation of an employer's policies and is part of an illegal scheme, it would be 'proper' to conclude that such conduct 'exceeds authorized access' within the meaning of § 1030(a)(2)." By analogy, a spouse who leverages the other spouse's password in a manner unintended by the other spouse might be vulnerable to a CFAA claim under *John* on the ground that such use exceeded the user's authorization. The spouse might argue, for example, that she shared her cell phone password with her husband so the latter could make occasional calls, not to let him freely rummage through the phone's logs, messages, or picture folders to "obtain information from a[] protected computer."[13]

The Ninth Circuit reached the opposing conclusion in another criminal case, *Nosal*, and construed "unauthorized access" narrowly.[14] Nosal was charged with a § 1030(a)(4) violation after using information pilfered from his previous employer's database to start a competing business. The court held "that the phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions." In other words, an employee does not violate the CFAA by accessing information in violation of the employer's computer-use policy using his or her otherwise valid password. The court reasoned, in part, that applying the CFAA under these conditions would also criminalize the conduct of employees who used their work computers for innocent—albeit arguably unauthorized—activities, such as "playing games, shopping or watching sports highlights."

[11] *See, e.g.*, *United States v. Barrington*, 648 F.3d 1178, 1203 (11th Cir. 2011) (holding that district court's finding that "defendants produced unauthorized access devices when they retrieved the passwords and user names from the data on the keyloggers" was not "clear error").
[12] 597 F.3d 263 (5th Cir. 2010).
[13] 18 U.S.C. § 1030 (a)(2)(C).
[14] 676 F.3d at 863.

C. The CFAA's damage and loss requirement

The defendant's authority to access a computer is not the only important element of a CFAA claim. The CFAA authorizes a cause of action to victims "who suffer[] damage *or* loss."[15] A civil claim under the CFAA's § 1030(g) requires the plaintiff to "prove (1) damage or loss (2) by reason of (3) a violation of § 1030(a), and (4) conduct involving one of the factors set forth in § 1030(c)(4)(A)(i)."[16] The CFAA defines damage as "any impairment to the integrity or availability of data, a program, a system, or information."[17] The term "loss"

> means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.[18]

One shorthand way to think about the distinction is that "damage" focuses on harm to data and information, *e.g.*, deletion or corruption, and "loss" focuses on monetary harm.[19]

Claims under § 1030(a)(2)(C) and (a)(4) require the plaintiff to demonstrate a loss, but claims under § 1030(a)(5) require both damage *and* loss (assuming § 1030(c)(4)(A)(i)(I) applies). Counsel must, therefore, also assess plaintiff's loss, or both damage and loss, depending on the asserted CFAA claim. Realistically, however, civil claims can be expected to arise only under sub-section § 1030(c)(4)(A)(i)(I), which requires "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value." Other § 1030(c)(4)(A)(i) sub-sections deal with physical injury, health and safety, and government computers—plausible but improbable topics of civil litigation in relation to unauthorized computer access in a family law context.

One would hardly be blamed for assuming that the CFAA's "loss" definition is subject to one interpretation, given its relatively straightforward statutory definition. But here again, courts are split on whether to construe the definition broadly or narrowly. Courts in the Southern District of Texas have followed the Southern District of New York's narrow statutory construction of the term "loss." These courts have held that "[t]he term 'loss' encompasses only two types of harm: costs to investigate and respond to an offense," *i.e.*, damage to data or information, "and costs incurred because of a service interruption."[20] In *Alliantgroup*, the plaintiff alleged that its former employee accessed its computers to filch confidential sales and marketing information. But because Alliantgroup did not allege an interruption of services, or costs incurred to investigate and respond to same, the court granted defendant's motion for summary judgment. Under these conditions, pleadings that do not allege an interruption of service, or costs incurred to investigate or respond to same, risk being struck. In *Rajaee v. Design Tech Homes, Ltd.*, another Southern District of Texas case, Rajaee alleged that his employer remotely wiped his iPhone shortly after he resigned, ostensibly deleting all data residing on the iPhone.[21] The court dismissed Rajaee's CFAA claim because he "produced [no] evidence of any costs he incurred to investigate or respond to the deletion of his data, nor do the losses and damages for which he does produce evidence arise from an 'interruption of service.'"

[15] For additional details on this topic, *see* Pierre Grosdidier & Mike Stewart, *When Employees Leave with Electronic Files: The CFAA's Eclectic Damage and Loss Case Law Illustrated*, Bloomberg BNA Electronic Commerce & Law Report, June 2, 2014.

[16] *See, e.g.*, *Jarosch v. Am. Family Mut. Ins. Co.*, 837 F. Supp. 2d 980, 1020 (E.D. Wis. 2011).

[17] 18 U.S.C. § 1030(e)(8).

[18] *Id*. § 1030(e)(11).

[19] *Kluber Skahan & Assocs., Inc. v. Cordogen, Clark & Assocs., Inc.*, No. 08-cv-1529, 2009 WL 466812, at *7 (N.D. Ill. Feb. 25, 2009) (mem. op.).

[20] *Alliantgroup, L.P. v. Feingold*, 803 F. Supp. 2d 610, 630 (S.D. Tex. 2011) (Rosenthal, J.) (citing *Nexans Wires S.A. v. Sark-USA, Inc.*, 319 F. Supp. 2d 468, 474–76 (S.D.N.Y. 2004), aff'd, 166 F. App'x 559, 562–63 (2d. Cir. 2006)).

[21] No. H-13-2517, 2014 WL 5878477 (S.D. Tex. Nov. 11, 2014) (Werlein, J.) (mem. op.) (motion for new trial denied, Doc. 47, Jan. 27, 2015) (disclosure: the author was one of the defense attorneys).

Other courts, including courts in the Northern District of Texas, have adopted a much broader construction of the definition of "loss." In *Meats by Linz, Inc. v. Dear*, the plaintiff asserted a § 1030(a)(2)(C) claim against a rogue former employee who absconded with confidential information.[22] Meats alleged that Dear transacted business with Meat's clients on basis of the pilfered information resulting in business damage or loss to Meat "aggregating at least $5,000 in value." The court held these damage-and-loss allegations sufficient to support a CFAA claim and it denied Dear's motion to dismiss. Likewise, in *Heil Trailer Int'l, Co.v. Kula*, another trade secret theft case, the plaintiff alleged § 1030(a)(2)(C) and (a)(5) claims and lost trailer sales in excess of $5,000 per year.[23] The court again held these loss allegations sufficient to survive defendants' motion to dismiss.

It is hard to imagine how a spouse's rummaging through the other spouse's cell phone or personal computer, without more, can result in a $5,000 threshold-qualifying loss, even under the broad statutory construction adopted in the Northern District of Texas. A CFAA claim for such conduct will likely fail unless the indiscreet spouse deletes documents or information on the phone and the victim has to spend money to recover the data, or the rummaging results in loss to a business.

The above cases show that plaintiff's counsel must precisely ascertain the facts that potentially give rise to a CFAA cause of action, identify the applicable statutory claim or claims, and thoroughly check the case law in the court where the lawsuit is to be filed to see how judges have construed the statutory language as it relates to both authorization and loss. Only then will counsel appreciate the viability of a CFAA claim. This pre-suit research might be time-consuming and, therefore, costly, but certainly less so than the motion practice that will invariably follow a weak or indefensible CFAA claim.

D. CFAA claims: Illustrative family law cases

The following cases illustrate how courts have addressed CFAA claims in a family law context. There are no reported Texas cases exactly on point and these cases are drawn from other jurisdictions.

Global Policy Partners, LLC v. Yessin deals with a dispute between former spouses and business partners.[24] Unbeknown to his wife, Friess, Yessin knew her email account password and accessed her emails after the couple separated. Plaintiffs sued Yessin and asserted a CFAA claim, *inter alia*, based on three types of "loss." As a threshold matter, and citing Fourth Circuit case law, the court placed the burden on the CFAA plaintiffs to show that their losses were both reasonable and caused by the CFAA violation.

The court accepted some of plaintiffs' costs (totaling $2,283) to migrate to a new website as "CFAA-qualifying losses." It rejected other such costs on evidentiary and eligibility grounds. The court next rejected plaintiff Freiss's claim that she lost 50 hours of work (valued at $27,000) investigating or responding to the CFAA violation. Even though the court held that this loss qualified under the CFAA, the facts supporting the claim were too insufficiently proven or too vague to count the loss toward the $5,000 threshold. The court also rejected plaintiffs' claim that they lost millions of dollars in revenue when the ex-spouses' dispute spilled over to potential clients and a deal consequently fell through. The court found that the undisputed facts showed no connection between the CFAA violation and the loss of business. In addition, the lost revenue was not a CFAA loss because it was not "incurred because of interruption of service."[25] Because the plaintiffs' loss allegations did not reach the CFAA's $5,000 threshold, the court dismissed the CFAA claims pursuant to § 1030(c)(4)(A)(i).

[22] No. 3:10-CV-1511-D, 2011 WL 1515028 (N.D. Tex. Apr. 20, 2011) (Fitzwater, C.J.); *see also Meats by Linz, Inc. v. Dear*, Complaint at ¶ 30 (Pacer Doc. 1) (alleging § 18 U.S.C. § 1030(a)(2)(C) claim).
[23] No. 4:12-CV-385-Y, 2012 WL 12877645 (N.D. Tex. Aug. 21, 2012) (Means, J.) (Slip op.).
[24] 686 F. Supp. 2d 642 (E.D. Va. 2010) (mem. op.).
[25] *Id*. at 653 (*citing* 18 U.S.C. § 1030(e)(11)).

Another district court also rejected a CFAA claim in a divorce-related case for failure to state CFAA-qualifying losses. In *Morgan v. Preston*, the plaintiff alleged that his spouse surreptitiously installed monitoring software on his personal computer.[26] The parties filed for divorce and Morgan thereafter sued Preston alleging §§ 1030(a)(2)(c) and (a)(4) claims, *inter alia*. The court dismissed the CFAA claims because Morgan provided no "factual allegations in support of his claim that he lost at least $5,000" as a result of Preston's alleged conduct.

These two cases show that, in general, merely accessing a spouse's cell phone, email, or computer without his or her consent will not likely support a CFAA claim because the plaintiff will struggle to satisfy the statutory $5,000 loss threshold. Things might be different when a family business is involved in the unauthorized access. In that case, the breach might result in losses totaling more than $5,000 provided that they qualify as CFAA losses under forum case law. The burden is again on counsel to carefully review whether the facts and the applicable case law support such a claim. The same claim that might stand in Dallas based on *Meats*, for example, might fail in Houston based on *Alliantgroup*.

III. CLAIMS UNDER THE SCA

Congress enacted the SCA in 1986 to protect the privacy of electronic communication—such as emails, then a novel technology for general public use.[27] Electronic communications, not computers, are the focal point of the SCA.[28] In a family law context, these communications are typically one spouse's emails or phone text messages.

As one court noted, the statute "is famous for its lack of clarity."[29] Victims of SCA transgressions enjoy a statutory cause of action.[30] But as with the CFAA, courts have not interpreted the SCA's language uniformly as it applies to unauthorized access of email accounts. The issue of concern in this article is whether a SCA claim stands against a spouse who indiscreetly reads the other spouse's emails without authorization. The answer depends on *where* the emails are physically located, *i.e.*, whether they are located on a hand-held device, a server, or a home computer. It also depends on whether the emails have already been read by their intended recipient. A little background on the SCA is necessary to understand why these issues matter.

A. Elements of an SCA claim

The elements of civil claim under the SCA's § 2701(a)(1) are:

i. The defendant intentionally accessed a facility through which an electronic communications service was provided;

ii. such access was not authorized, or intentionally exceeded authorization;

iii. the defendant thereby obtained, altered, or prevented authorized access to an electronic communication while it was in electronic storage in such system; and

[26] No. 3:13-00403, 2013 WL 5963563 (M.D. Tenn., Nov. 7, 2013) (mem. op.).

[27] *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 (2004); *see also* H.R. Rep. No. 99-647, at 62 (1986) (noting that § 2701(a) "addresses the growing problem of unauthorized persons deliberately gaining access to, and sometimes tampering with, electronic or wire communications that are not intended to be available to the public.").

[28] The SCA defines "protected computer" in reference to the CFAA. 18 U.S.C. § 2510(20).

[29] *See, e.g.*, *Cruz Lopez v. Pena*, No. 2-12-CV-165-J, 2013 WL 2250127, at *3 (N.D. Tex. May 22, 2013) (mem. op.) (*Lopez II*).

[30] 18 U.S.C. § 2707(a).

iv. the defendant's unauthorized access caused actual harm to the plaintiff.[31]

The key statutory terms in this language are "facility," "electronic communications service," and "electronic storage." These terms constrain the SCA's ambit.

The SCA does not define the term "facility." It defines "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[32] The SCA defines "electronic storage" as "—

> (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
> (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[33]

Remedies for a SCA claim include declaratory relief, actual damages, and reasonable attorney's fees and litigation costs.[34] "[I]n no case shall a person entitled to recover receive less than the sum of $1,000." Moreover, "willful or intentional" SCA violations may result in punitive damages.

B. Email technology in 1986

The SCA's language as it applies to emails is best understood in terms of *circa* 1986 technology, the year Congress enacted the SCA.[35] Publicly available email services were then in their infancy. Subscribers connected to private networks via phone lines and read their emails on their computer screen. The SCA protected the privacy of these emails during their transmission from source to destination server, and until the subscriber read them.[36] The SCA also protected copies of emails captured in server backups during their transmission.[37] Less certain was the SCA's protection of opened but undeleted emails that remained on the destination server.[38]

C. Email technology today

Email users (or subscribers, as the case may be) nowadays access email servers with or without a front-end email "client" program such as Microsoft's Outlook or Mozilla's Thunderbird. Of course, more and more users now access their emails on their hand-held device. In this article, the term "client" is used exclusively in its software sense, *i.e.*, it refers to an email program (*e.g.*, Outlook, Thunderbird, or an email App on a hand-held device) that accesses a server-based email service (*e.g.*, Microsoft's Exchange, gmail). This client program usually resides on the users' personal device, such as a personal computer or a handheld device. The email servers typically belong to the users' employers or to webmail service providers such as Yahoo! or Google.

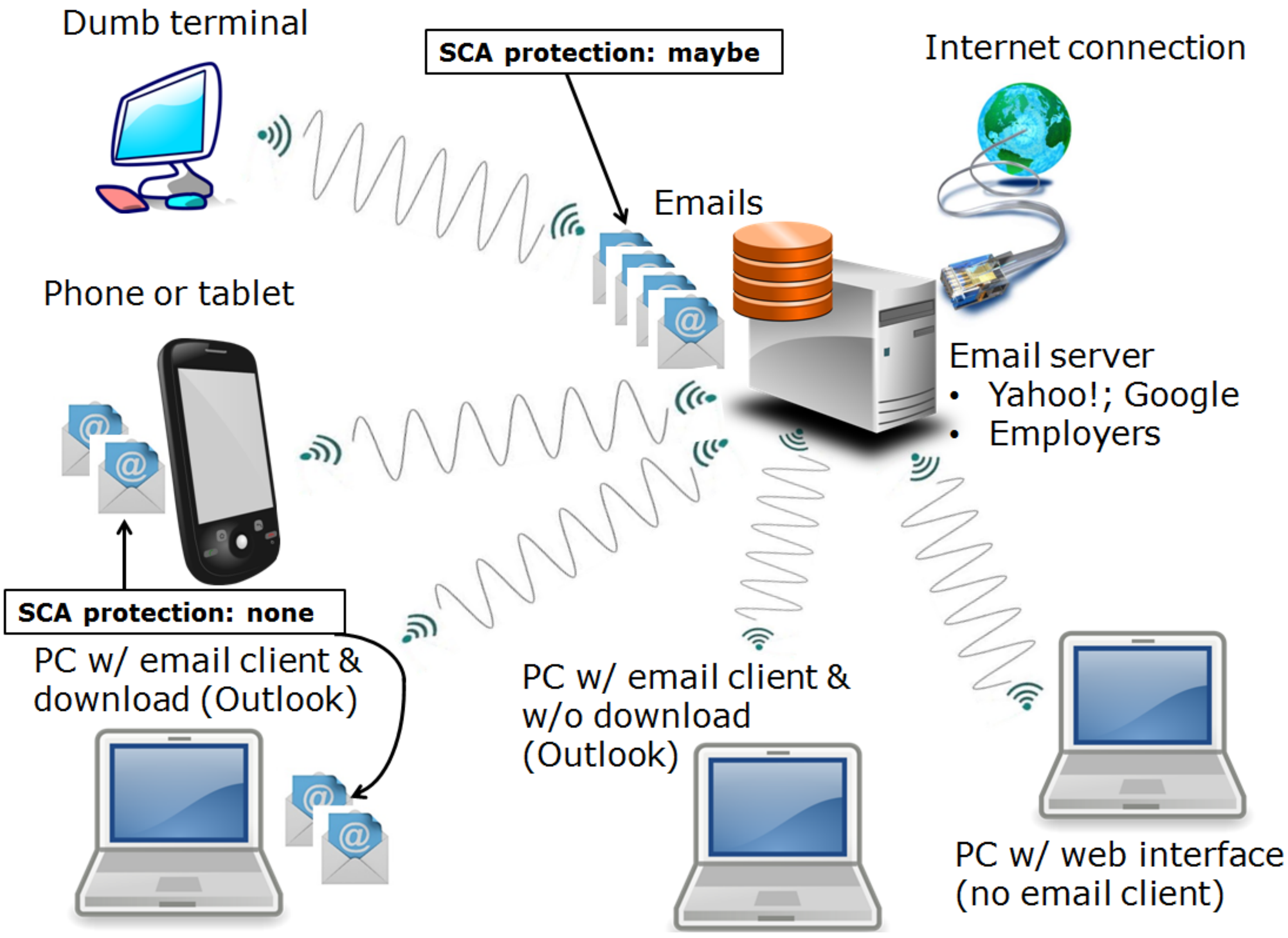
Webmail users often—but not always—access webmail servers without a client. They access their webmail accounts through web-browsers from any computer, handheld device, or "thin" client located anywhere in the world. In the absence of an email client, messages are not downloaded to the user's

[31] 18 U.S.C. §§ 2701(a), 2707; *Cornerstone Consultants, Inc. v. Prod. Input Solutions, L.L.C.*, 789 F. Supp. 2d 1029, 1047 (N.D. Iowa 2011).
[32] 18 U.S.C. §§ 2510(15), 2711(1).
[33] *Id*. § 2510(17), *see also* 18 U.S.C. § 2711 (incorporating the Electronic Communications Privacy Act's ("ECPA") definitions into the SCA).
[34] *Id*. § 2707(b), (c).
[35] *See* Kerr, *supra* note 27, at 1208–18.
[36] 18 U.S.C. § 2510(17)(A).
[37] *Id*. § 2510(17)(B).
[38] *See* Kerr, *supra* note 27, at 1216–18 and nn.53, 61.

personal device and remain on the server until expressly deleted.

Some webmail users, and many users of employer-provided email services, use a front-end email client to interface with the server email program. An email client offers much richer functionality than a webmail program—such as a better text editor. The client can be used in one of three main configurations. The user can choose to keep all emails on the server. In this case the user cannot access emails when working offline, but emails always remain safely stored on the server. This configuration is substantively not much different from using webmail with a browser, but the user enjoys a much better front-end to edit and manage emails. At the other extreme, a user can select a configuration that keeps all emails on the client and none on the server. In this case, incoming emails are immediately downloaded to the client on the user's personal device, or as soon as the user signs-on and synchronizes. This configuration's drawback is that the user will lose all emails if the personal device breaks or is stolen, unless the user previously backed-up the emails to separate media. Finally, a user can choose to keep copies of emails on both the client *and* the server. The user then gets the best of both worlds: offline availability of all emails, and *de facto* backup protection by the email server in case the user loses the personal device. These possible configurations are shown in Figure 1.

Figure 1. Email access and location options, and SCA protection



D. The SCA does not protect hand-held devices.[39]

The Fifth Circuit held in *Garcia v. City of Laredo, Tex.* that the SCA did "not apply to data stored in a personal cell phone."[40] Garcia, a former police dispatcher, argued that defendants accessed her cell phone without permission and fired her for the images and text messages that it contained. She appealed the district court's summary judgment decision for defendants as to her SCA claim. Affirming, the Fifth Circuit Court of Appeals held that cell phones "did not constitute facilit[ies] through which an electronic communication service is provided."[41] Cells phones "enable" these services, but do not "operate" them. The SCA only protects "facilities" operated by providers of "electronic communication services," such as Internet or email service providers.

The Court of Appeals also held that the text messages and pictures in Garcia's cell phone were not in electronic storage under the SCA. The SCA term "storage" encompassed only information stored by an "electronic communication service" provider "temporarily pending delivery or for purposes of backup protection." Text messages and pictures stored on a personal cell phone were, therefore, "outside the scope" of the SCA. Citing *Garcia*, the district court in *Rajaee* also dismissed Rajaee's SCA claim as to data held in his personal iPhone.[42] *Garcia* conclusively established that no SCA claim stands against a person who underhandedly peruses the emails, text messages, and pictures on his or her spouse's hand-held device.

District courts outside the Fifth Circuit have followed *Garcia*'s holding. In *Shefts v. Petrakis*, the plaintiff alleged a SCA claim after defendants accessed text messages on his BlackBerry.[43] Citing *Garcia*, the court held that a BlackBerry is "merely a device, . . . not a facility" as required by the SCA. Likewise, the text messages on the BlackBerry were not in "electronic storage" pursuant to § 2510(17). The text messages' transmission was complete by the time they reached the BlackBerry, and they could not be in "temporary, intermediate storage . . . incidental" to their transmission. The court granted defendants' motion for summary judgment as to plaintiff's SCA claim for the text messages.

E. The SCA does not protects home computers

In *Garcia*, the Fifth Circuit also held that the SCA does not protect information stored on a home computer hard drive, nor does it protect emails stored only on a personal computer.[44] The computer is not a SCA-qualifying facility, and the information is not "in electronic storage," as required by the statute. As in the case of hand-held devices, therefore, no SCA claim stands against a spouse who rummages through the other spouse's personal computer, including downloaded and locally-stored emails.

F. The SCA protects unopened server-resident emails.

There is no question that the SCA protects unopened emails stored on email servers before they are delivered to, and opened by, their recipients.[45] In *Cruz Lopez v. Pena*, for example, the court noted that

[39] For additional details on this topic, *see* Pierre Grosdidier, *Don't Look To SCA In BYOD-Termination Remote Wipe Cases*, Law360, Mar. 17, 2015.

[40] 702 F.3d 788, 790 (5th Cir. 2012), *cert. denied*, 133 S.Ct. 2859, 186 L.Ed.2d 911 (2013).

[41] *Id*. at 792 (citing *In re iPhone Application Litig.*, 844 F.Supp.2d 1040, 1057–58 (N.D. Cal. 2012) (internal quotations omitted); *see also Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263, 1271 (N.D. Cal. 2001) ("[The argument that] computers of users of electronic communication service, as opposed to providers of electronic communication service, are considered facilities through which such service is provided [is] destined to failure.").

[42] *Rajaee*, 2014 WL 5878477 at *2. The court also noted that Rajaee waived his SCA claim by failing to defend it in his response to defendant's motion for summary judgment. *Id*. at *2 n.12.

[43] No. 10-cv-1104, 2013 WL 489610, at *2 (C.D. Ill. Feb. 8, 2013) (*Shefts II*).

[44] *Garcia*, 702 F.3d at 793.

[45] *Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 36 F.3d 457, 461–63 (5th Cir. 1994).

"§ 2510(17) has been clearly established to protect unopened emails."[46] The SCA applies in this case because unopened emails are in "temporary, intermediate storage" pending delivery.[47]

The status of opened emails left on an email server remains unclear (let alone that of emails in "sent" or "deleted" folders, or of emails that have been opened but re-marked as "unread").[48] Once opened, server-resident emails are no longer protected by the SCA under 18 U.S.C. § 2510(17)(A) because they are "no longer stored incident to transmission."[49] The question is whether they are protected under the SCA's "backup protection" provision, 18 U.S.C. § 2510(17)(B). Courts struggle with the fact that the term "backup protection" is not defined in either the statute or the legislative history.

G. Some courts have held that the SCA protects opened emails left on a server after the subscriber downloaded the emails onto a personal device.

In *Theofel v. Farey-Jones*, the Ninth Circuit Court of Appeals addressed the claims of Internet service subscribers whose emails were allegedly accessed in violation of the SCA.[50] A third-party Internet service provider ("ISP") provided the subscribers' email service. The case facts offer no details regarding the subscribers' email software configuration. The court *assumed* that the subscribers downloaded copies of their emails into their personal devices.[51] Effectively, the court assumed that because the subscribers received their emails from an ISP (as opposed to, presumably, a webmail service provider), the subscribers necessarily all used an email client, downloaded their emails, and kept copies of same on the ISP's server. The case facts only support this last assumption (because the ISP had access to the emails).

The Ninth Circuit held that

> [a]n obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again—if, for example, the message is accidentally erased from the user's own computer. The ISP copy of the message functions as a "backup" for the user.[52]

The court held that the SCA protected the subscribers' opened emails because these emails were stored on the servers "for purposes of backup protection."

Fourteen subscribers appealed the trial court's decision. It is conceivable that at least one subscriber did not download received emails even if he or she used an email client. Would *Theofel*'s holding have been different had the court known the details of the subscribers' email configurations? *Dicta* in the opinion suggest that the answer might be "yes." The court noted that a "remote computing service might be the only place a user stores his messages; in that case, the messages are not stored for backup purposes."[53] This would be the case for any subscriber who did not download his or her emails to a client.

[46] No. 2-12-CV-165-J, 2013 WL 819373, at *4 (N.D. Tex. Mar. 5, 2013) (mem. op.) (hereinafter *Lopez I*).
[47] 18 U.S.C. § 2510(17)(A).
[48] In *United States v. Weaver*, a government subpoena "specified that the '[c]ontents of communications not in 'electronic storage' include the contents of previously opened or *sent* email.'" 636 F. Supp. 2d 769, 769–70 (C.D. Ill. 2009) (emphasis added); *see also Theofel*, 359 F.3d at 1070 ("[w]e see many instances where an ISP could hold messages not in electronic storage—for example, . . . messages a user has flagged for deletion from the server. . . . the messages are not in temporary, intermediate storage, nor are they kept for any backup purpose."). Note that Outlook allows an email message to remain flagged as unread even after the message has been read in the Reading Pane, which makes the case law's read-unread distinction effectively meaningless.
[49] *Lopez I*, 2013 WL 819373, at *4.
[50] 359 F.3d 1066, 1071–72 (9th Cir. 2004), *cert. denied*, 543 U.S. 813 (2004).
[51] *See Weaver*, 636 F. Supp. 2d at 772 (*Theofel* "relies on the assumption that users download emails from an ISP's server to their own computers.").
[52] *Theofel*, 359 F.3d at 1075.
[53] *Id*. at 1077.

Theofel is a case where the court assumed that the subscribers downloaded their emails, and held that email copies kept on servers were kept for "backup protection." These emails were in "electronic storage" and, therefore, protected by the SCA's § 2701(a). A number of courts have followed *Theofel*. In *Shefts v. Petrakis*, the court held that unauthorized access of server email copies fell under SCA's purview when plaintiff downloaded emails to Outlook.[54]

H. Other courts have held that the SCA does not protect opened emails kept solely on a server.

In *Weaver*, a criminal case, Microsoft objected to a government subpoena requesting previously opened emails less than 181 days old believed to be held in the defendant's Hotmail account.[55] The case turned on whether the emails were in "electronic storage," in which case the government needed a warrant. A subpoena would otherwise do. The court held that the emails were not in storage under § 2510(17)(A) because they had been opened. The emails were also not in storage under § 2510(17)(B) because the defendant used a web-based email account. The defendant only stored his emails on Microsoft's servers and not "for backup purposes." The government, therefore, only needed a trial subpoena to request the emails.[56] The *Weaver* court essentially adopted *Theofel*'s *dicta*, even as it held that *Theofel* was "largely inapplicable" to its case because the *Theofel* court assumed that the *Theofel* subscriber-appellants downloaded their emails.[57]

The *Weaver* court assumed that the subscriber did not download emails and held that emails kept only on a webmail server are not kept for "backup protection." These emails are not, therefore, in "electronic storage." Other courts have followed *Weaver*. *See, e.g.*, *Jennings v. Jennings*, below.[58]

I. Yet other courts have held that the SCA protects opened emails kept solely on a server.

In *Fischer v. Mount Olive Lutheran Church, Inc.*, the defendants accessed the plaintiff's Hotmail email account and the plaintiff alleged a claim under the SCA.[59] The plaintiff had opened the account from a public library computer and accessed it through his employer's computers. Nothing in the opinion suggests that the plaintiff downloaded his emails to a client. The opinion implies that the emails accessed by the defendants had been read by the plaintiff: "plaintiff arrived early at the church and read his email messages on his Hotmail account," *i.e.*, before defendants accessed the emails themselves.[60] The court cited the legislative history to hold "that Congress intended the [SCA] to cover the exact situation in this case."[61] The court denied defendants' motion to dismiss plaintiff's § 2701(a) claims. *Fischer* is a case where the courts held that the SCA's § 2701(a) protects emails that have not been downloaded to a client and have already been read.

In summary, courts seem to agree that the SCA's § 2701(a) protects server-resident emails if they are unopened or opened and downloaded.[62] Courts are split regarding emails that are opened and not downloaded. Some courts hold that the SCA's § 2701(a) does not protect these emails.[63] Others courts

[54] No. 10-cv-1104, 2011 WL 5930469, **2, 5–6 and n.7 (C.D. Ill. Nov. 29, 2011) (*Shefts I*).
[55] 636 F. Supp. 2d at 769–70; *see also* 18 U.S.C. § 2703 (specifying the conditions under which a government entity can compel the disclosure of electronic communications).
[56] *Id*. at 772–73.
[57] *Id*. at 772.
[58] 736 S.E.2d 242, 243 (S.C. 2012) (*Jennings II*).
[59] 207 F. Supp. 2d 914, 916–18 (W.D. Wis. 2002).
[60] *Id*. at 917.
[61] *Id*. at 925–26 (citing S. Rep. No. 99-541, at 36 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3590 (email subscriber would violate SCA's § 2701(a) by accessing other subscribers' emails)).
[62] *Steve Jackson Games*, 36 F.3d at 461–63; *Theofel*, 359 F.3d at 1075.
[63] *See, e.g.*, *Weaver*, 636 F. Supp. 2d at 772.

hold that § 2701(a) does.[64] The law is clearly not settled. It is no surprise that a district judge recently noted that "courts are in hot debate" over the meaning of the SCA's "backup provision."[65] Counsel's take-away from these cases is to pay close attention to applicable circuit law, if any, and also to whether the plaintiff actually downloaded emails to a client.

J. SCA claims: Illustrative family law cases

In *Morgan*, summarized above, the court dismissed plaintiff's SCA claim because his "personal computer [wa]s not covered by the SCA."[66] The court cited to *Garcia* and numerous other cases that have followed it or reached the same conclusion.

In *Jennings II*, a cheated spouse and her daughter-in-law accessed the husband's Yahoo! email account after successfully guessing the answers to the security questions.[67] Broome, the daughter-in-law, alleged that she only accessed emails that had already been read.[68] The court dismissed the plaintiff's SCA claim because it held that these opened emails, which had apparently not been downloaded or saved elsewhere, where not in electronic storage for backup protection under the SCA's § 2510(17)(B).

In *Bailey v. Bailey*, the plaintiff sued under the SCA after the defendant accessed the plaintiff's two Yahoo! email accounts, using key logger software to obtain the passwords.[69] The defendant alleged that the messages he read were already opened, and nothing in the case suggests that the plaintiff downloaded her email to a client. The court held that it agreed with *Theofel* and that the "plain language of the statutes seems to include emails received by the intended recipient where they remain stored by an electronic communication service."[70] The court did not acknowledge that *Theofel* involved downloaded emails and is distinguishable from *Bailey* on this basis.[71] The facts in *Bailey* show that the emails had been read, but not that they had been downloaded. The *Bailey* court denied defendant's motion for summary judgment regarding plaintiff's SCA claim.

IV. CLAIMS UNDER THE TEXAS HACA

A. Statutory provisions

The Texas HACA is a very simply worded statute that creates a civil cause of action for persons who are injured, or whose property is injured, by knowing or intentional violations of Texas Penal Code Chapter 33, Computer Crimes.[72] The injured party is entitled to actual damages and reasonable attorney's fees and costs.[73] Texas Penal Code Chapter 33, in turn, is a very broadly worded statute that criminalizes the mere knowing and unauthorized access to a computer:

> A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.[74]

"Access" means

[64] *See, e.g.*, *Fisher*, 207 F. Supp. 2d at 925–26.
[65] *Lopez I*, 2013 WL 819373, at *4.
[66] *Morgan*, 2013 WL 5963563, at *6.
[67] 736 S.E.2d at 243.
[68] *Jennings v. Jennings*, 697 S.E.2d 671, 673 (S.C. App. 2010) (*Jennings I*).
[69] No. 07-11672, 2008 WL 324156, at *1 (E.D. Mich. Feb. 6, 2008).
[70] *Id*. at *6.
[71] *Compare Weaver* with *Shefts I*, 2011 WL 5930469, *5 n.7 (recognizing this distinction).
[72] Tex. Civ. Prac. & Rem. Code Chap. 143.
[73] *Id*. § 143.002.
[74] Tex. Pen. Code § 33.02(a).

> to approach, instruct, communicate with, store data in, retrieve or intercept data from, alter data or computer software in, or otherwise make use of any resource of a computer, computer network, computer program, or computer system.[75]

The statute does not define the term "approach." Taking the term literally could criminalize merely standing next to a computer without consent. More likely and applying the *ejusdem generis* doctrine, the term probably means any attempt to log on a computer, and arguably also any "pinging" of a computer. No case law sheds light on this issue.

"Effective consent"

> includes consent by a person legally authorized to act for the owner. Consent is not effective if:
>
> (A) induced by deception, as defined by Section 31.01, or induced by coercion;
>
> (B) given by a person the actor knows is not legally authorized to act for the owner;
>
> (C) given by a person who by reason of youth, mental disease or defect, or intoxication is known by the actor to be unable to make reasonable property dispositions;
>
> (D) given solely to detect the commission of an offense; or
>
> (E) used for a purpose other than that for which the consent was given.[76]

Condition (E) is significant in that it implies a narrow construction of the term "consent." An employer's computer use agreement, for example, would normally restrict employees' access to that reasonably necessary to perform job functions, which implies that any downloading of information for personal use is without consent under § 33.01(12)(E). This language is consistent with *John*'s construction of "unauthorized access."

A computer is defined broadly to encompass essentially any digital device, including hand-held devices. "Computer" means

> an electronic, magnetic, optical, electrochemical, or other high-speed data processing device that performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, or communication facilities that are connected or related to the device.[77]

The statute also distinguishes mere access from access with ill intent, with higher criminal penalties:

> A person commits an offense if, with the intent to defraud or harm another or alter, damage, or delete property, the person knowingly accesses:
>
> (1) a computer, computer network, or computer system without the effective consent of the owner; or
>
> (2) a computer, computer network, or computer system:
>
> (A) that is owned by:
>
> (i) the government; or
>
> (ii) a business or other commercial entity engaged in a business activity;
>
> (B) in violation of:

[75] *Id*. § 33.01(1).
[76] *Id*. § 33.01(12).
[77] *Id*. § 33.01(4).

> (i) a clear and conspicuous prohibition by the owner of the computer, computer network, or computer system; or
>
> (ii) a contractual agreement to which the person has expressly agreed; and
>
> (C) with the intent to obtain or use a file, data, or proprietary information stored in the computer, network, or system to defraud or harm another or alter, damage, or delete property.[78]

For a civil litigant, the HACA is much broader and much simpler to wield than either the CFAA or the SCA. The statute does not impose a threshold loss amount, as does the CFAA, and it does not narrowly define access to email communications, as does the SCA. Its language is straightforward and easy to understand. Yet, for all its potential strength as a civil litigation tool, the HACA has remarkably little civil case law history.

What little civil case law exists shows that courts will construe "authorized access" narrowly, as did the court in *Institutional Sec. Corp. v. Hood*.[79] Institutional Securities Corporation ("ISC"), a securities broker/dealer, hired Hood as vice president to service ISC's clients, and also as a contractor to recruit additional ones. Hood enjoyed broad access to ISC's computerized client records *only in his capacity as vice president*, and "regularly downloaded" client information onto personal external hard drives.[80] Separately, Hood worked as an independent contractor and on a commissions basis to recruit new clients for ISC. ISC's other client-recruiting independent contractors did not have access to ISC's computer system.

ISC eventually terminated Hood, but Hood retained copies of ISC's downloaded computer files on personal media. ISC sued Hood within months of his termination after he tried to woo ISC clients to his new employer. ISC asserted a HACA claim based on Texas Penal Code § 33.02(a), *inter alia,* and applied for injunctive relief. ISC appealed the scope of the district court's order granting the temporary injunction.

The court held that "[t]he download of data from the computer system without ISC's consent could constitute a violation of section 33.02(a) of the Penal Code."[81] Hood's conduct "could constitute a violation" of the HACA because Hood "knowingly accessed ISC's computer system and downloaded its files to maintain a list of his customers for his business" as an independent contractor. In other words, Hood's unfettered access to ISC's computer system as vice president did not imply that he enjoyed ISC's consent to download ISC client information for his personal benefit. The Dallas Court of Appeals, therefore, narrowly construed the term "effective consent," consistent with the plain reading of the statutory language.

Hood's narrow construction of the term "effective consent" exposes the Texas Computer Crimes law to the same criticism that commentators have leveled against a broad construction of the term "unauthorized access" under the CFAA.[82] Under Texas's Computer Crimes law, a social media user who violates a dating website's terms of use by, *e.g.*, lying about her weight could be prosecuted for a Class B misdemeanor punishable by a fine not to exceed $2,000, up to 180 days in jail, or both.[83] A bored refinery or wastewater treatment plant operator working the graveyard shift who surfs sports news Internet sites to stay awake—but in violation of his employer's computer-use policy—could face 180 days to two years in

[78] *Id*. § 33.02(b-1). Underlined language denotes 2015 statutory amendments. *See also id*. § (b-2) for corresponding penalties.

[79] 390 S.W.3d 680, 684 (Tex. App.—Dallas 2012, no pet.).

[80] *Id*. at 682.

[81] *Id*. at 684.

[82] For a concise critique of the breadth of the CFAA term "unauthorized access," *see* Orin S. Kerr, Written Statement to the U.S. House of Representatives Subcommittee on Crime, Terrorism, Homeland Security and Investigations, Mar. 13, 2013, available at *http://www.volokh.com/wp-content/uploads/2013/03/KerrCFAATestimony2013.pdf.*

[83] Tex. Penal Code §§ 12.22, 33.02(a), (b).

jail, a $10,000 fine, or both, for committing a state jail felony.[84] But in neither case would such conduct support a cause of action unless it resulted in injury to the plaintiff, or to the plaintiff's property.[85]

B. HACA claims: Illustrative family law

In *Miller v. Talley Dunn Gallery, LLC*, Miller accessed his soon-to-be ex-wife Talley Dunn's cell phone and took screen shots of text messages between Dunn and another man and examined the phone's log.[86] Dunn and her eponymous art gallery eventually sued Miller alleging, *inter alia*, a HACA claim based on Texas Penal Code § 33.02(a) and for injunctive relief. As to the HACA claim, the court held that (1) a cell phone qualifies as a computer under the Texas Penal Code § 33.01(4); and (2) Miller accessed the phone within Chapter 33's meaning when he retrieved the phone's log and text messages. The court also rejected Miller's claim that he had effective consent to access the phone because it was community property. The phone belonged to Dunn; she used it "on a daily basis" and "it was the only way to reach her." She had the right to password-protect the phone, and Miller used her sleep to access the phone. The court held that Dunn had a greater right of access to the phone and it sustained the district court's injunctive relief order as to the information Miller obtained in violation of the HACA.

[84] Tex. Penal Code §§ 12.35, 33.02(a), (b)(2) (unauthorized access of "critical infrastructure facility" computer is state jail felony); 33.01(10-a)(B) ("'critical infrastructure facility' means . . . (B) a refinery; . . . (D) a . . . wastewater treatment plant").
[85] Tex. Civ. Prac. & Rem. Code § 143.001(a) (civil cause of action requires injury to person or property).
[86] No. 05-15-00444-CV, 2016 WL 836775, at **1, 11 (Tex. App.—Dallas Mar. 3, 2016, no pet.).