STATE BAR LITIGATION SECTION REPORT

THE ADVOCATE

COMMERCIAL LAW DEVELOPMENTS AND DOCTRINE

VOLUME 56

FALL

2011

PRIVACY RIGHTS OF EMPLOYEES IN AN ELECTRONIC WORLD

BY MICHAEL KELSHEIMER & TRAVIS CRABTREE

I. History of Privacy in the Workplace

Privacy has come a long way since the U.S. Supreme Court outlined its penumbrae in *Griswold v. Connecticut*. Citizens have been wrapped in a cloak of protection from government intrusion into their private lives. While this cloak follows public sector employees into the workplace, private sector employees must disrobe at the door to the office, and, in some cases, before entering the parking lot of their employer. What sparse protections private sector employees receive arise from common law privacy protections accepted by the Texas Supreme Court. But these protections, too, are essentially surrendered in the workplace where the desire to remain employed causes employees to relinquish what few privacy protections they have. Only where employers permit an expectation of privacy to exist, do employees have any chance of preventing an employer from examining their private property at work.

Three privacy causes of action exist in Texas for a private citizen. They include claims for unreasonable intrusions upon the seclusion or private affairs of another; unreasonable publicity given to an aspect of a person's private life in which the public has no legitimate concern; and unwarranted appropriation of one's name or likeness.[1] These protections, however, have been eroded over time. Communication of even embarrassing, intimate facts is permitted if the publication is of legitimate public concern.[2]

If an employee dislikes a proposed change to the relationship, such as adding a drug testing policy, that employee can mark their dissent by quitting.

Fortunately, or unfortunately, depending on your perspective, employee attempts to drag these common law rights through their employer's door have been universally rejected by Texas courts. With the exception of term contract employees whose rights are governed by written agreement, "at-will" employment remains a unilateral contract modifiable on a going forward basis by either party.[3] If an employee dislikes a proposed change to the relationship, such as adding a drug testing policy, that employee can mark their dissent by quitting.[4] Courts have instead deferred to the U.S. and Texas legislatures to protect employees. The legislatures, in turn, have taken only few notable steps. In 1986, the U.S. legislature passed tandem the Electronic Communications Privacy Act ("ECPA") and Stored Communications Act ("SCA") discussed in much detail below. In 1988, the U.S. legislature passed the Employee Polygraph Protection Act of 1988 which prevents employers from using polygraph examinations except in certain limited circumstances.[5] Subsequently, in 1996, Congress again acted by passing the Health Insurance Portability and Accountability Act which provides protections from dissemination of employee health information.[6] Finally, in 2003, the Texas legislature passed a law prohibiting employers from transmitting an employee's social security number by mail.[7]

While acting with these few constraints, employers are generally free to infringe upon the claimed privacy of their employee; however, employers must be vigilant to avoid inadvertently creating an expectation of privacy among their employees. In *K-Mart Corp. Store No. 7441 v. Trotti*, an employee's work locker was opened by her employer in a search for stolen merchandise which the employee did not have.[8] Employer representatives rifled through the employee's purse and other property.[9] A jury awarded damages to the employee for an invasion of privacy claim and K-Mart appealed.[10] On appeal, the Houston Court held there was sufficient evidence to support a jury finding that K-Mart created an expectation of privacy in the locker because the employee was permitted to provide her own lock, to which K-Mart did not have a key.[11]

Since the *Trotti* decision, employers have commonly included provisions in their employee handbooks indicating that all locations within the workplace are subject to search, required employees to consent to searches of all property at the time of employment, and maintained separate access to any private space designated to an employee such as a locked drawer or locker. Following these simple requisites, employers are generally free of the concerns presented by *Trotti*.

Technology presents the new wrinkle in employee privacy considerations in the workplace. Office phones, cell phones, email and, more recently, social media may blur the distinctions so easily discerned with employee physical property.

II. Office Phones

An employer who wants to monitor calls on an office phone is subject to the privacy right considerations discussed above for physical property, but layered over them is the protection of the federal ECPA and Chapter 123 of the TEX. CIV. PRAC. & REM CODE ("Chapter 123").

The ECPA is a modified version of the former Omnibus Crime Control and Safe Streets Act of 1968, which applied only to telephone communications. It extends the prohibition against intercepting communications to other forms of electronic communication including emails and voicemail.[12] While the ECPA sounds formidable, two exceptions limit its effectiveness on employers. Acting as a backstop, Chapter 123 then removes one of the two ECPA exceptions in Texas.

Both laws permit interception with consent. The ECPA consent exception permits interception of communications where "one of the parties to the communication has given prior consent."[13] Under the ECPA, consent may be implied, but courts have been reluctant to do so, suggesting implied consent may not be casually inferred.[14] Determining implied consent is case specific, but generally requires language or acts that tend to show a party knows of and assents to encroachment upon call privacy.[15] Following the ECPA, simply knowing that your employer is capable of monitoring employees is also insufficient.[16] Under Chapter 123, intercepting communication is a violation if made "without the consent of a party to the communication . . ."[17] Unfortunately, there are few cases interpreting Chapter 123 and while implied consent may someday be upheld, Texas courts follow their federal brethren in holding that knowledge someone might be intercepting your communication is insufficient.[18]

The "business use" exception under the ECPA excludes from coverage "any telephone . . . instrument, equipment, or facility furnished to the subscriber or user . . . in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business."[19, 20] Divided into two elements, the exception requires that: (1) the telephone company provide the telephone or device which intercepted the communication for use in the ordinary course of business, and (2) that the device was used in the ordinary course of business.[21]

With respect to the first element, courts agree about interception of live calls, but there does appear to be a divergence regarding the use of a recorder to tape calls.[22] For the second element, the key question is the business nature of the call. Courts seem to agree that a purely personal call is not within the ordinary course of business regardless of an employer's attempted justification.[23] To avoid liability under the ECPA, employers may listen to the beginning of a call to determine its purpose and must terminate the surveillance if the call is personal.[24]

Because the business use exception is not available in Texas due to the greater limitation imposed by Chapter 123, employers here must obtain written consents from their staff with reference to each of these laws.

III. Cell Phones

Available for almost forty years, cell phones really came into their own in the 1990s. Since then, they have become a must-have business tool with the added benefit of internet connections and texting capability. While voicemails, call histories, and text messages are each different, the different mediums do not affect the analysis regarding privacy. Ownership of the device is the key. Cell phones are sometimes provided and paid for by the employer, but in other instances employers reimburse employees a portion of their cell phone bill, or the employee receives no reimbursement but only occasionally uses their private phone for work. These different levels of interconnectivity between work and private use do potentially affect the employee's privacy rights in the information stored.

The ECPA does not play a significant role in protecting privacy with respect to cell phones. This is because it applies only to contemporaneous interception of communication and it is virtually impossible for an employer to intercept a live cell phone call.[25] Rather, its sister statute the SCA, which governs access of stored communications, occupies the field.[26]

The SCA protects against direct access of protected communication. Specifically, it prevents an employer from intentionally accessing a facility or cell phone through which electronic communication service is provided, without consent.[27, 28] Where employers might then think of accessing the information directly from the cell service provider, they will again run into a wall – even for phones they provide to employees for their use.[29]

Worse still, the SCA does not incorporate the business use exception granted by the ECPA. Employers are left with only the option to obtain consent from the employee to gain access to stored communications.[30, 31] Employers may, however, obtain "customer records" regarding a phone it provides to the extent providing the information is "incident to the rendition of the services by the provider."[32] Customer records may include transactional records, account logs,

usage, email addresses, visited internet sites, addresses, and phone numbers called, but it is unclear how much of this information an employer can obtain from the service provider without consent.[33] Courts have not explained what more than a billing statement the subscriber, or employer, is entitled to without consent of the employee. Conversely, for accounts which are maintained by the employee and reimbursed by the employer, no information is available without consent under the SCA because the employer does not even stand in the place of subscriber.

Court interpretation of Chapter 123's language and meaning is woefully behind the SCA and inadequate in consideration of today's cell phone usage. By definition, Chapter 123 applies only to the "aural acquisition" of content, presumably rendering it ineffective against review of text messages and raising the question whether it applies to voicemails which were not originally intercepted aurally, or "live."[34] Other questions arise about Chapter 123's application to "content" of communication.[35] Will this term be interpreted in the same manner it is under the SCA or will it include what the SCA defines as "customer records" relating to information about the content? If it is broadly construed, Chapter 123 will strip away even the limited information an employer may obtain regarding "customer records" under the SCA. Until these issues are resolved, the only safe maneuver for employers is to obtain clear consent with respect to both the federal and state laws.

Because the SCA prevents employers from obtaining almost all information regarding employee cell phone use, the only area in which common law privacy expectation may come into play relates to video and photographs taken by the employee that reside on a cell phone. If the image or video was received by the employee, the SCA applies and prevents access, but the SCA does not have jurisdiction over video and images which an employee has made.[36] Regardless of whether the employee has sent the images to another person, they originated on that employee's phone.

The recently decided U.S. Supreme Court case of *City of Ontario v. Quon* provides insight on this point.[37] In *Quon*, the city police department issued alphanumeric text pagers to members of its SWAT team for police business only.[38] Team members were required to sign a written policy making it clear that the city reserved the right to monitor and log text messages sent on the pagers.[39] When Quon and other team members started incurring large overages against their allotted messages, their supervisor threatened to audit the messages to determine if the pagers were being used for personal purposes.[40] The supervisor then offered not to audit the accounts if Quon and others would pay any overages.[41] After months of continued overages, Quon's supervisor decided to audit accounts to determine if the department should purchase more messaging time.[42] Quon's messages for two months were pulled and reviewed.[43] The messages revealed that the vast majority of his communications were personal, sexually explicit, and directed toward another department officer with whom he was having a relationship.[44] The records were turned over to internal affairs and Quon was investigated for possible disciplinary action.[45]

Quon filed suit against the wireless provider for violations of the SCA and against the department for violating his Fourth Amendment rights as a public sector employee.[46] When the matter reached the Supreme Court, it reasoned that Quon had an expectation of privacy in the messages despite the explicit department directive because his supervisor had created an expectation of privacy by altering the policy to allow Quon to pay for overages.[47] While the case does not have direct application in the private sector, it does reiterate the message of *Trotti*. Creating an expectation of privacy can lead the employer down a precarious path. In both cases, the creation was unintentional. K-Mart ran out of company issued locks and allowed Trotti to purchase her own lock for which the company did not maintain access.[48] The City of Ontario committed to a position distinct from its written requirement by allowing Quon to pay for overages.

An employee would not likely have an expectation of privacy in a company phone. For that reason, the employer should be permitted to examine pictures and video taken by the employee without hesitation. That said, it is easy to compromise the employer's right without even realizing the consequence. Employers should institute written policies regarding ownership of all company property and the right to examine every nook and cranny of the company's facilities at any time. Additionally, employers should institute a consent to be searched and for the company to have access to all records on company cell phones under Titles I and II of the ECPA and Chapter 123 of the TEX. CIV. PRAC. & REM. CODE.

IV. Email

The development of email has eased corporate communications but also presented a bevy of privacy issues as it relates to employees. Most companies have policies in place making it clear that emails received and sent on the company account are subject to review, belong to the company and there is therefore no expectation of privacy. The more difficult issue arises from personal web-based email systems accessed by

employees on company accounts and other non-work related behaviors.

A. The ECPA and SCA

As noted above, ECPA[49] and SCA[50] are equally important sister statutes. Generally speaking, the ECPA, often called the Wiretap Act, applies to electronic communications[51] in transit and the SCA applies to communications stored on servers.

While most of the cases deal with stored communications, the ECPA still creeps into the workplace when dealing with emails. For example, the Seventh Circuit was forced to examine whether auto-forwarding emails in the workplace violated the Wiretap Act. In *U.S. v. Szymuszkiewicz*,[52] an IRS revenue officer secretly adjusted his boss's Outlook program to forward all emails.

The subordinate was convicted of a federal crime and appealed to the Seventh Circuit. On appeal, the court denied the subordinate's argument that the interception had to be "contemporaneous" with the "transmission" under the Wiretap Act. In other words, under the traditional phone tap, the interception is made while the call is being conducted and the voice transmission is in route. Once the email hits the Outlook account, it is technically completed and only then did the program forward it to the defendant's account.

Upholding the conviction, the court determined the interception of the message was "contemporaneous by any standard." Getting into the technological details, the court claimed the evidence showed the Outlook rules operated on the server and to auto-forward, a copy needed to be immediately made at the server at the time of delivery and then forwarded to the defendant.

A plaintiff under the Wiretap Act can recover a minimum award of $10,000 or $100 per day of violation—whichever is greater, or, actual damages, plus punitive damages, attorneys' fees and costs.[53] To avoid any confusion, employers should include the right to review and monitor emails and all electronic communications at any time in any form in their standard computer use policies. After all, auto-forward is a standard operating procedure to use when a departed employee leaves so the company can address customer concerns emailed to that employee. Obtaining consent at the time of hire is much easier than asking if the leaving employee minds as he walks out the door.

The SCA meanwhile, makes it illegal for anyone to "intentionally access[] without authorization a facility through which an electronic communication service is provided or . . . intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorize access to a wire or electronic communication while it is in electronic storage in such system."[54] In plain English, it is illegal to access someone's Hotmail account without their authorization and read their emails because those emails are stored on Hotmail's servers and not the company's. The main litigated issues are, therefore, whether a communication is covered by the SCA and consent.

The SCA covers "electronic communication services" which is defined as "...any service which provides to users thereof the ability to send or receive wire or electronic communications."[55]

When employees access web-based email accounts, for example, a company's server or computer may store passwords and certain communications. When employees leave for a competitor, companies are tempted to not only search the work-issued emails stored on the servers, but also check what duplicitous communications may be gathered through the departed employees' personal accounts. That is where the SCA and other laws come in to play.

One court has specifically ruled that personal emails that are stored on a company laptop are not protected by the SCA. In *Thompson v. Ross*,[56] a Pennsylvania district court was forced to determine whether messages from AOL and Yahoo accounts already saved on a laptop computer were in "electronic storage" as defined by the SCA. In the *Thompson* case, the plaintiff's ex-girlfriend kept the plaintiff's laptop after a break-up.[57] The ex-girlfriend let two of her co-workers see the email messages stored on the existing computer.

Under the SCA, electronic storage is defined as "any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[58] The messages on the laptop were not stored by AOL or Yahoo, but were saved to the laptop. The court rejected the notion that saving the messages to the laptop constituted "backup storage" because the court determined the statute was not supposed to be interpreted that broadly.

While not absolutely failsafe given the lack of mature developed law, the general rule of thumb is that if someone's personal email is, for whatever reason, saved to the company's server or saved to a company laptop, the company can generally review and use it assuming there is a broad computer use policy. Accessing additional emails on their personal account because you happen to have access to the password

or through other means without the employee's knowing consent, however, raises serious concerns under the SCA.

B. The Computer Fraud and Abuse Act

In addition to the ECPA, employers need to consider the Computer Fraud and Abuse Act (the "CFAA").[59] The CFAA makes it illegal to access a data base without proper authority or to exceed one's authority.[60] The primary focus of the law is on hackers, but it is becoming the add-on violation of choice for trade secret and noncompetition fights between companies and former employees.

The most common application comes when an employee leaves to go to a competitor and downloads trade secrets from her former employee's database. A perfect example comes from *Andritz, Inc. v. Southern Maintenance Contractor, LLC.*[61] Defendants Pettit and Harper left plaintiff Andritz, Inc., after they allegedly accessed proprietary information from their company-issued laptops and gave it to their new employer.

Although the plaintiff company may have been able to show improper access to the database, the court dismissed the claim because the plaintiff failed to show the type of "loss" or "damage" required by the statute.[62] The plaintiff claimed it lost the prerequisite amount because defendants accessed information to poach customers which caused a loss. The CFAA, however, requires there be an impairment of the computer system or data accessed. Because the plaintiff "still had access to the data just as it had before [d]efendants' actions," there was no violation of the CFAA.

In the case of *ShareLee v. PMSI, Inc.*,[63] the outcome was the same although the roles were reversed. In *ShareLee*, the former employee started the litigation with a pregnancy discrimination allegation. The company, counterclaimed under the CFAA claiming the former employee used the company resources to access Facebook and check her personal email. The company claimed they lost the necessary amount because of the loss of productivity.

The court dismissed the claim because there was no damage to the company's computer system. Moreover, the employee only accessed her own data on Facebook and the web-based email account and not the data of the company.

When the employee accessing the data violates a fiduciary duty by doing so, the result may be different. In *U.S. v. Nosal*,[64] a former employer sued the former employee claiming the latter accessed proprietary information and destroyed important data prior to his departure.

Trying to dismiss the claim, the defendant argued the complaint failed to establish that access to the work computer was without authorization because defendant's access, while employed, was never restricted. Creatively, the plaintiff claimed the defendant's access violated the fiduciary duty the employee owed the employer. That claim was enough at the pleading stage to show the defendant exceeded his authorization to access the company computer. Because the employee destroyed the actual data, the company also pleaded the necessary loss.

V. Social Media

As if web-based email was not enough to muddy the waters, social media only complicates matters further. While it is clear companies have the right to restrict the use of social media at the worksite, the law is still wrestling with the rights of both employees and employers when it comes to social media activities of employees on their own time.

While it is clear companies have the right to restrict the use of social media at the worksite, the law is still wrestling with the rights of both employees and employers when it comes to social media activities of employees on their own time.

A. Taking Action for Employee's Social Media Conduct

A manager of a Houston's restaurant discovered his employees created a closed MySpace forum complaining about the restaurant.[65] The manager allegedly coerced the hostess to give him the password to her account. After reviewing the site, he fired two of the employees who created the group. The two employees sued the restaurant.

The jury's verdict that the restaurant violated the SCA was upheld by the federal district judge in New Jersey. The court also upheld the jury's verdict that Houston's acted maliciously authorizing exemplary damages.

The MySpace group, called "Spec-Tator" was maintained by one of the employees during non-work hours. It was a closed group meaning an invitation from the two plaintiffs and a password was needed before any of the messages could be seen. The group was labeled as private and described as a forum where employees could vent on "crap/drama/and gossip" related to their workplace. Management was not invited. The plaintiffs claimed

no one accessed the site during work hours or on work computers.

There was disputed evidence as to whether one of the group members who worked as a hostess voluntarily provided management with her password to allow management to access the site or whether she was coerced into doing so. Nevertheless, two managers accessed the site using someone else's password several times and terminated the employees who managed the chat group.

On a motion for new trial, the federal district court found there was sufficient evidence the company "knowingly, intentionally, or purposefully," accessed an otherwise private chat room without authorization in violation of the SCA. Had management simply been provided the password to view the chat room without putting any pressure on the hostess, the outcome may have been different because there would have likely been the necessary consent.

Interestingly, the jury determined the company did not violate the employees' common law right to privacy and that part of the ruling was therefore not part of the district court's opinion.

B. The National Labor Relations Board

Not only do employers need to be concerned about lawsuits from employees, the National Labor Relations Board has recently taken action against employees who crack down on employees engaged in social media. On October 27, 2010, the NLRB issued a complaint against American Medical Response of Connecticut, Inc.[66] The company fired the employee when it discovered negative comments on Facebook. Under the National Labor Relations Act, employees may discuss the terms and conditions of their employment with co-workers and others as a protected activity—even if it is on Facebook.

The NLRB claimed the company had an overly restrictive policy about employee blogging and Internet posting infringing on their rights to discuss working conditions with each other. Probably even more problematic, the company denied union representation to the employee during an investigatory interview shortly before the employee posted the negative comments on Facebook.

The NLRB settled with the company in February 2011.[67] As part of the settlement, the company agreed to broaden its policies to allow employees to discuss their working conditions with each other. The company also promised that employee requests for union representation would not be denied and that no adverse actions would be taken against employees who make such a request. The settlement between the employee and the company was separate from the NLRB's settlement and was confidential.

While this development caused many employers to re-examine their social media policies, a subsequent NLRB decision may decrease the concern. The NLRB more recently held that a newspaper had the right to fire a newspaper reporter over his "tweets" on the micro-blogging site Twitter.[68] The *Arizona Daily Star* reporter had already been warned more than once about the content of his tweets that identified him as a reporter and linked to the newspaper's website.

One of the first questioned tweets criticized one of the newspaper's headlines. The paper's human resource department encouraged the reporter to address his concerns internally rather than on Twitter. Subsequently, the reporter's managing editor told the reporter he should not make comments damaging to the newspaper's reputation via social media.

According to the NLRB decision, the paper encouraged the reporters to use Twitter, but had no written policy about it. The reporter stopped tweeting about the paper, but still found himself in trouble. The reporter tweeted various comments about Tucson's homicide rates. Some of his tweets included:

- August 27 - "You stay homicidal, Tucson. See Star Net for the bloody deets."
- August 30 - "What?!?!? No overnight homicide? WTF? You're slacking Tucson."
- September 10 - "Suggestion for new Tucson-area theme song: Droening [sic] pool's 'let the bodies hit the floor'."
- September 10 - "I'd root for daily death if it always happened in close proximity to Gus Balon's."
- September 10 - "Hope everyone's having a good Homicide Friday, as one Tucson police officer called it."
- September 19 - "My discovery of the Red Zone channel is like an adolescent boy's discovery of h...let's just hope I don't end up going blind."

The reporter also retweeted a local television news station post, noting a misspelled word. The television station's tweet said: "Drug smuggler tries to peddle his way into the U.S." The newspaper reporter retweeted the post and added: "Um, I believe that's PEDAL. Stupid TV people."

When the television station complained to the newspaper, the managing editor told the reporter to stop tweeting until a senior management meeting. Rather than stopping, the reporter changed his screen name and removed some of his

supervisors as followers. The reporter also protected his tweets so only people with his approval could view them. The reporter was fired later that month.

The NLRB wrote: "In this case, even if the employer implemented an unlawful rule, the charging party was terminated for posting inappropriate and unprofessional tweets, after having been warned not to do so. The charging party's conduct was not protected and concerted: it did not relate to the terms and conditions of his employment or seek to involve other employees in issues related to employment."[69]

Conclusion

If there is a common thread among the legal issues presented by the introduction of mobile phones, email, and social media into employee privacy, it is the universal need for employers to set expectations and obtain written acknowledgement of those expectations from employees. Consent, and vigilant avoidance of exceptions to the policies created, will carry an employer through the largest portion of the minefield. A basic understanding of some of the applicable laws and statutes will also help when issues not addressed in the policies inevitably arise. Venturing, then, into social media employers must be wary of using an employee's public complaints about the conditions of his or her work as a basis for discipline or termination. As communication tools evolve and blur the line between company and private communications, companies will struggle to maintain the proper balance. The employers are not the only ones. The law is struggling to keep pace as well.

Travis Crabtree is a Member of the law firm of Looper Reed & McGraw, P.C. in Houston who focuses on Internet law and commercial litigation. He authors the blog www.emedialaw.com where he discusses the latest on these and many other similar issues.

Michael Kelsheimer is a Shareholder of the firm of Looper Reed & McGraw, P.C. in Dallas, practicing employment law. Michael maintains the website www.texasemployerhandbook.com and authors a monthly guide called the The Employer Handbook. ★

1 *Billings v. Atkinson*, 489 S.W.2d 858, 860 (Tex. 1973).

2 *Indus. Found. of the S. v. Tex. Indus. Accident Bd.*, 540 S.W. 668, 680 (Tex. 1976), cert denied 430 U.S. 934 (1977).

3 *Jennings v. Minco Technology Labs, Inc.*, 765 S.W.2d 497, 499 (Tex. App.—Austin, 1989); *cf., Farrington v. Sysco Food Serv's, Inc.*, 865 S.W.2d 247 (Tex. App.—Houston [1st Dist.] 1993).

4 *Id.*

5 29 U.S.C. § 2002 (2010).

6 45 CFR § Part 160; 45 CFR Part 164, Subpart A & E.

7 TEX. BUS. & COMM. CODE § 501.001 (2010).

8 *K-Mart Corp. Store No. 7441 v. Trotti*, 677 S.W.2d 632, 634 (Tex. App.—Houston [1st Dist] 1984).

9 *Id.*

10 *Id.*

11 *Id.* at 637-638.

12 18 U.S.C. § 2509, *et seq.* (2010).

13 18 U.S.C. § 2511(2)(d) (2010).

14 *U.S. v. Amen*, 831 F.2d 373, 378 (2nd Cir. 1987); *Williams v. Poulos*, 11 F.3d 271, 281 (1st Cir. 1993)(quoting *Griggs-Ryan v. Smith*, 904 F.2d 112, 116-17 (1st Cir. 1990).

15 *Griggs-Ryan*, 904 F.2d at 117.

16 *Deal v. Spears*, 980 F.2d 1153, 1157 (8th Cir. 1992).

17 TEX. CIV. PRAC. & REM. CODE § 123.001(2) (2010).

18 *Collins v. Collins*, 904 S.W.2d 792 (Tex.App.—Houston [1st Dist.[1995).

19 18 U.S.C. § 2510(5)(a) (2010).

20 There is a dearth of case law interpreting the business use exception under the ECPA. Many of the cited cases were decided before the statutes were recast, but remain applicable due to the use of the same language.

21 *Deal*, 980 F.2d at 1157.

22 *Id.* at 1157-58 (determining that recorder was instrument rather than phone and since the recorder was not provided by the phone company, exception not applicable); *cf., Epps v. St. Mary's Hosp. of Athens, Inc.*, 802 F.2d 412, 415-16 (11th Cir. 1986)(holding interception device was dispatch device to recorder).

23 *Watkins*, 704 F.2d at 582-83; *Briggs v. American Air Filter Co., Inc.*, 630 F.2d 414, 420 (5th Cir. 1980).

24 *Id.* at 583-584.

25 *See United States v. Steiger*, 318 F.3d 1039, 1048-49 (11th Cir. 2003); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002); *Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 36 F.3d 457 (5th Cir. 1994); *see also Wesley Coll. v. Pitts*, 974 F. Supp. 375 (D.Del. 1997), *summarily aff'd*, 172 F.3d 861 (3d Cir. 1998).

26 *See* 18 U.S.C. §§ 2701–2711 (2010); Note, the SCA has been given various names by commentators including: (1) the "Electronic Communications Privacy Act" or "ECPA" because it was first enacted as part of that statute; (2) the "Stored Wired and Electronic Communications and Transactional Records Access" statute or "SWECTRA" because that is the formal title given to Chapter 121 in Title 18; (3) Stored Communication Act, by the United States Supreme Court in *City of Ontario v. Quon*, and (4) "Title II" because it was enacted as the second title of ECPA. The SCA is technically part of the ECPA and not a stand-alone act. For ease of reference, this article will refer to Title I of the ECPA, sometimes referred to as the "Wiretap Act" as the ECPA and Title II as the SCA.

27 18 U.S.C. § 2701(a)(1) (2010).

28 Cell phone and text messaging services are each an "electronic communication service" within the meaning of the SCA. 18 U.S.C. § 2711(1) (2010)(incorporating definitions from Title I at 18 USC § 2510(12) and (15)); *see also Crispin v. Christian Audigier, Inc.*, 717 F.Supp.2d 965, 979 (C.D. Cal. 2010) citing *Jayne v. Sprint PCS*, No. CIV S-07-2522 LKK GGH P, 2009 WL 426117, *6 (E.D.Cal. Feb. 20,

2009)(cell service); *In re Applications of U.S. for Orders Pursuant to Title 18, U.S.Code § 2703(d)*, 509 F.Supp.2d 76, 79 (D. Mass. 2007) (cell service); *Quon v. Archstone Wireless*, 529 F.3d 892, 900-03 (9th Cir. 2008), *reversed on other grounds by City of Ontario v. Quon*, 560 U.S. ----, ---- - ----, 130 S.Ct. 2619, 2629-31, 177 L.Ed.2d 216 (2010)(text service).

[29] 18 U.S.C. § 2702(a)(1) (2010).

[30] 18 U.S.C. § 2701(c)(1)(content and user information) and 2702(b)(3)(as to content of voicemails or texts).

[31] There is small chance an employer may claim rightful access to content of communications for company issued cell phones under 18 U.S.C. § 2702(b)(1) if the employer can successfully argue that it is the "addressee" or an "agent" for the recipient. This point does not appear to have been raised in a case and was glossed over in *Quon v. Archstone Wireless*, 529 F.3d at 900.

[32] 18 U.S.C. § 2702(c)(3) (2010).

[33] "Customer records" include "record[s] . . . pertaining to a subscriber" include transactional records, such as account logs that record account usage; cell-site data for cellular telephone calls; and email addresses of other individuals with whom the account holder has corresponded. *See* H.R. Rep. No. 103-827, at 10, 17, 31 (1994), reprinted in 1994 U.S.C.C.A.N. 3489, 3490, 3497, 3511; *see also Hill v. MCI WorldCom Commc'ns, Inc.*, 120 F. Supp. 2d 1194, 1195-96 (S.D. Iowa 2000) (names, addresses, and phone numbers of persons called"); *United States v. Allen*, 53 M.J. 402, 409 (C.A.A.F. 2000) (log providing date, time, user, and detailed internet addresses); *In re Application of United States*, 509 F. Supp. at 80 (historical cell-site information).

[34] TEX. CIV. PRAC. & REM. CODE § 123.001(2) (2010).

[35] *Id.*

[36] 18 U.S.C. § 2711(1) (2010) (incorporating the definition of "electronic communication" from 18 U.S.C. § 2510 (12)).

[37] 560 U.S. ----, ---- - ----, 130 S.Ct. 2619, 2629-31, 177 L.Ed.2d 216 (2010).

[38] *Id.* at 2625.

[39] *Id.*

[40] *Id.* at 2626.

[41] *Id.*

[42] *Id.*

[43] *Id.*

[44] *Id.*

[45] *Id.*

[46] *Id.*

[47] *Id.* at 2630-33; note that certiorari was denied regarding the lower court's decision against the cell service provider under the SCA.

[48] *Trotti*, 677 S.W.2d at 634-35.

[49] 18 U.S.C. § 2510.

[50] 18 U.S.C. §§ 2701-12.

[51] 'Electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12) .

[52] __ F.3d __, 2010 WL3503506 (7th Cir. Sept. 9, 2010).

[53] 18 U.S.C. § 2520(b).

[54] 18 U.S.C. § 2701.

[55] 18 U.S.C. § 2510(15).

[56] 2010 WL 3896533 (W.D. Pa. Sept. 30, 2010).

[57] Interestingly, family law cases raise an equal amount of issues concerning what can and cannot be done with data on laptops and password-protected Internet email or social networking accounts.

[58] 18 U.S.C. § 2510(17)(B).

[59] 18 U.S.C. § 1030.

[60] 18 U.S.C. § 1030(a)(1).

[61] 2009 WL 48187 (M.D. Ga. Jan. 7, 2008).

[62] Damage is defined as "impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). "Loss" is "any reasonable cost to any victim, including the cost of responding to an offense, conducting damage assessment, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Id.* at § 1030(e)(11). Through 18 U.S.C. § 1030(a)(4) liability is premised on there being at least $5,000 in losses in any one-year period.

[63] 2011 WL1742028 (M.D.Fla. May 6, 2011).

[64] __ F.3d __, 2011 WL1585600 (9th Cir. 2011).

[65] *Pietrylo v. Hillstone Restaurant Group d/b/a Houston's*, D.N.J., No. 06-5754, unpublished, Sept. 25, 2009.

[66] NLRB Case No. 34-RC-002401. For details, see the February 11, 2011 NLRB Press Release available at www.nrlb.gov/news-media/news-releases/archive-news (last visited June 14, 2011).

[67] *Id.*

[68] *Lee Enterprises, Inc., d/b/a Arizona Daily Star*, NLRB Dir. of Advice, No. 28-CA-23267 (April 21, 2011 [released May 10, 2011]).

[69] *Id.*