#PrivateNotPrivate

Employee Electronic Communications

By Tami Z. Hannon
and Kyle B. Melling

Until a replacement law is passed, attorneys are faced with advising clients in this convoluted legal landscape.

According to statistics, an estimated 215.3 billion e-mails are sent and received worldwide each day. Snapchat houses approximately six billion videos. Instagram users upload an estimated five million photographs every day. In 2012, Twitter reported 175 million tweets each day. The social media giant Facebook averages 510,000 comments posted, 293,000 statuses updated, and 136,000 photographs uploaded every 60 seconds.

With these numbers, it is easy to see how your business or your client's business will likely be affected by some form of electronic communication. It is also increasingly likely that you or your clients will be faced with potentially disciplining an employee over electronic communications. For example, a client was just told that an employee posted a harassing message to another employee on a social media site. The reported message is a clear violation of company policy and (gasp) was made on company time. Your client wants to pull the offending employee in and demand that he or she show your client the posting. Before hitting the "like" button, there are several issues to discuss with your client.

The law limits how you obtain electronic communications, which include e-mails, text messages, or social media postings. In 1986, Congress passed the Electronic Communications Storage Act, referred to as the Stored Communications Act or SCA, in response to growing concerns about the law's ability to protect the growing use of electronic communications.

It is a violation of the SCA for anyone intentionally to access "without authorization a facility through which an electronic communication service is provided and thereby" obtain, alter, or prevent "authorized access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C. §2701(a). With this type of description, it is no wonder that the SCA has been noted as "famous (if not infamous) for its lack of clarity." *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457, 462 (5th Cir. 1994). Violations of the SCA can result in civil penalties of $1,000 or ac-

■ Tami Z. Hannon is a partner at Mazanec Raskin & Ryder in Cleveland, Ohio. Ms. Hannon focuses her practice on defending governmental entities and their employees, as well as elected and appointed officials. She is a member of the DRI Employment and Labor Law, Governmental Liability, and Women in the Law Committees. Kyle B. Melling is an associate at Mazanec Raskin & Ryder in Cleveland, Ohio. Mr. Melling focuses his practice on civil rights and governmental liability, employment and labor law, and public sector law. He is a member of the Cleveland Metropolitan Bar Association and the Federal Bar Association.

tual damages, whichever is greater. 18 U.S.C. §2707(c). Courts vary in their interpretation of these statutory damages to be either a flat $1,000, $1,000 per login, or $1,000 per electronic communication accessed. (The Fourth and Eleventh Circuits require proof of actual damages for an award of compensatory damages, as do a split of district courts.) In addition, the statute provides for an award of costs and attorneys' fees. Regardless of which circuit claims are brought in, the damages for violations of the SCA can be substantial, and employers should make every effort to avoid it.

Consider the number of text messages or personal e-mails that may be stored on an employee's company cellphone. Consider the number of times an employee may return a company computer or cellphone without deleting all of the information stored on it. Given the vast number of communications and the remedies that the SCA provides, an attorney must be familiar with these rules. This article will offer the top tips for navigating the SCA and advising clients about employee electronic communications.

Have Policies Regarding Access to Electronic Accounts

An employer cannot create a policy opting out of the SCA. The employer can, however, provide itself with an additional measure of control and access over information stored on its computers and servers. A proper policy should advise employees that their communications would be monitored and that e-mails are not private and are subject to viewing, downloading, and archiving. Here a strongly worded policy is better than one that is not because some courts find that merely knowing that a company was capable of monitoring electronic communications was not enough. *Shefts v. Petrakis*, 758 F.Supp.2d 620 (C.D. Ill. 2010). This policy should extend to all devices connected to the employer's server.

Rules on Accessing Electronic Communications

Advise clients to keep these five rules in mind: (1) do not allow employees to use personal e-mail accounts to conduct business and vice versa; (2) do not request passwords for personal accounts; (3) do not use saved logins; (4) do not share passwords or allow employees to share passwords; and (5) deactivate employee passwords and access on separation.

Do Not Allow Employees to Use Personal E-mail Accounts to Conduct Business and Vice Versa

A real conflict arises when an employee either leaves or is terminated, and the employee previously used his or her personal e-mail address to conduct company business. Does the former employee have to delete all business e-mails upon his or her departure? Can the company access the former employee's e-mail account to obtain business records? What happens if the company contact sends the former employee a business e-mail after the employee has left?

The U.S. District Court for the Western District of Virginia was recently forced to decide this issue in the case of *Hoofnagle v. Smyth-Wyth Airport Commission*, 2016 WL 3014702 (Slip Copy) (W.D. Virginia 2016). In *Hoofnagle*, the plaintiff was a former airport operations manager for the airport. During his tenure as operations manager, the plaintiff set up a personal e-mail account, which he used to conduct both personal and airport business. The address was repeatedly published and held out to be the official e-mail address of the airport. When the plaintiff was terminated, the airport commission accessed the plaintiff's e-mail to recover the commission's business records. Despite allegations that the plaintiff had provided the airport secretary with the login information for the e-mail address, the U.S. District Court for the Western District of Virginia held that a genuine issue of fact existed pertaining to whether the airport was authorized under the SCA to access the e-mail.

As this case demonstrates, it is a best practice for companies not to allow or to encourage their employees to use their own private e-mail addresses, and instead to provide each employee with his or her own company e-mail address. A combination of this, and an effective digital use policy, as discussed above, will protect employers' ability to access employee's e-mails that contain business records after separation.

Do Not Request Passwords for Personal Accounts

Employers often want to request or to require employee login information for personal social media accounts as part of the application or background check process. Some employers may engage in ongoing monitoring of employee accounts, particularly when an employee may be out an extended leave. While there is value in reviewing the information that employees put out into cyberspace, employers must be cautious about how they obtain that information.

The SCA only prohibits accessing an "electronic communication" without authorization. If an employee provides the login information, you have authorization, right? Not likely. The SCA is the Fourth Amendment probable cause and warrant equivalent for private parties. Just as the courts will not uphold "forced consent" to a search, the courts will not uphold "forced consent" to obtain or to review an electronic communication. Even if an employee provided his or her login information, a court will likely determine that the "consent" was coerced if the employee was required to give the login information to be considered for employment or to maintain employment. You should also be cautious of any applicable state laws because 30 states currently have legislation prohibiting employers from requesting employee login information for personal accounts.

Do Not Use Saved Logins

Employers are increasingly providing their employees with personal cellphones and access to computers. Sometimes employees will save their usernames and passwords on these computers or forget to remove them from cellphones before returning them to a company. However, this oversight does not grant an employer consent to review an employee's e-mails, text messages, or other communications.

This issue was addressed by the U.S. District Court for the Northern District of Ohio in the case of *Lazette v. Kulmatycki*, 949 F. Supp. 2d 748 (N.D. Ohio 2013). In that case, Lazette was a former employee of Verizon Wireless. After Lazette left Verizon's employment, she returned her Verizon-issued cellphone, but she forgot to disconnect her personal Gmail account. Over the next 18 months, her former supervisor used the phone to read approximately 48,000 e-mails on Lazette's personal account. The district court denied Verizon's motion to dismiss, holding that Lazette did not give her former supervisor permission to access

her e-mails merely by returning the cellphone with her personal e-mail account still active. As the district court found, "negligence is… not the same as approval, much less authorization." *Id.* at 12.

A similar result was reached by the U.S. District Court for the Southern District of New York in *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548 (S.D.N.Y. 2008). There, the court found that the employee did not actually store any of his communications on the employer's computers, servers, or systems. Instead, the communications were all stored on and accessed from a third-party communication service provider system. As such, while the employees e-mail address and password were saved on the employer's computer, the employer's access to the employee's e-mail was a violation of the SCA.

You should also be cautious of any applicable state laws because 30 states currently have legislation prohibiting employers from requesting employee login information for personal accounts.

Do Not Share Passwords or Allow Employees to Share Passwords

Just as employees should ideally each have their own private e-mail accounts, they should also have their own private log-in information. This step is necessary for an employer to protect itself from accidentally providing to employees access to information that an employee is not authorized to access. When employers use common log-in information, or when they share passwords among employees, employers lose control over which data or information employees see. Many times, for simplicity's sake, employers will use common e-mail accounts, passwords, or both for their business accounts. When possible, this practice should be avoided so as never to have a situation in which an employee or an employer has the ability to access information that they may not have the authorization to access. This is especially true with things such as common login information for generic company e-mail systems. It is important to ensure that each individual employee has his or her own individual log-in, and that log-in can only access that employee's assigned account.

Deactivate Employee Passwords and Access on Separation

This tip—deactivating employee passwords—is not so much one that addresses employer compliance with the SCA, but it is an important tip for employers. If employers do not deactivate passwords or employee access upon separation, an employee can continue to use that information to log in remotely and potentially obtain confidential information. That said, employees should be aware that if they continue to use their employee access after separation, they may be in violation of the SCA and subject to liability as well. *See Tech Systems Inc. v. Pyles*, 630 Fed.Appx. 184 (4th Cir. 2015).

Rules Related to Obtaining Electronic Communications

Employers will want to observe three rules related to obtaining electronic communications: (1) do not request that anyone turn over personal postings or emails; (2) do not create fake accounts; and (3) take advantage of public information.

Do Not Request that Anyone Turn Over Personal Postings or E-mails

It may seem obvious given the above discussion that an employer could not force someone to provide a private e-mail, text message, or social media posting. What may be less obvious is that an employer should not even *request* that someone turn over a private e-mail, text message, or social media posting (reading over the employee's shoulder is equally frowned upon unless truly voluntary consent was given). Some courts find the request to be inherently coercive given the nature of the employment relationship. Other courts have found that directing a third party to access an account is no different from an employer accessing it directly. *Shefts v. Petrakis*, 2011 WL 5930469 (C.D. Ill. 2011). These rules hold true regardless of whether the electronic communication at issue is the employee's own message or one that the employee received from a third party.

Does this mean that employees have free reign to send, text, or post whatever they want without fear of employers obtaining it? No. An authorized individual can *voluntarily* provide an employer with a copy of the e-mail, text, or post. However, the facts and the circumstances surrounding the disclosure must show that the provision was truly voluntary. If an employee comes to his or her employer with message in hand at the very first report, then there are likely no issues. If, however, an employer receives a report similar to the one in the initial example in this article and an employee complains about a posting but does not provide it, then the employer must tread carefully.

The best choice is to advise such an employer to tell the reporting employee that the employer will investigate the matter and that the employer is not requesting a copy of the message and the employee does not have to provide a copy of the message, but if the employee wishes to do so voluntarily, it will assist in the investigation. No disciplinary action should be taken against any employee for failing or refusing to provide an employer with a copy of any private e-mail, text message, or social media posting.

Do Not Create Fake Accounts

When it comes to fake accounts, there are two separate issue here. The first issue would involve an employer that creates a fake online persona for itself to gain access to otherwise restricted sites. Even if an employee voluntarily allows an employer access to restricted messages under the fake persona, the courts will still likely find that the SCA was violated because the authorization was not knowingly and voluntarily given.

One of the best analogies for this example is to the common law of trespass, in the analysis adopted by the Ninth Circuit Court of Appeals. Permission to access a stored communication does not constitute a valid authorization if it would not defeat a trespass claim in similar circumstances. *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th

Cir. 2004). An employer cannot exploit a known mistake that relates to the essential nature of the employer's access of the site. *Id.* An employee can voluntarily choose to give ABC Company access to his or her restricted social media postings or information and in doing so defeat any potential SCA claim. However, an employee giving access to ABC Company masquerading as "Harry Scary" would not be considered a valid authorization under the SCA.

Authorization is also valid if an employee knowingly "friends" his or her supervisor, even if the supervisor only made the request to monitor the employee's social media page. The U.S. District Court for the District of New Jersey granted a summary judgment to an employer in a situation in which an employee provided unsolicited social media posts made by a coworker. *Ehling v. MonMouth-Ocean Hospital Service Corp.*, 961 F. Supp. 2d 659 (D.NJ 2013). In that case, Ehling knowingly and voluntarily "friended" a coworker who then had full access to all of Ehling's otherwise private Facebook posts. Unbeknownst to Ehling, the coworker regularly took screen shots of the Facebook page and e-mailed them to management. When Ehling made a controversial post about the shooting of a hate crime suspect, the hospital terminated her. Ehling filed suit, alleging that the hospital's access of her private Facebook postings violated the SCA. The district court disagreed, finding that the coworker was an authorized user who had authority under the SCA to provide the posts to the hospital voluntarily.

The second issue would arise when an employer creates an account as an authorized third party with the full knowledge and permission of the third party. On the surface, this approach would seem less concerning because the third party was given access to the original communication and has voluntarily granted access to the employer. However, the issue is not so clear cut and may actually run afoul of the SCA. The Ninth Circuit Court of Appeals addressed this issue in *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002). In that case, a pilot created a private online bulletin board where he could post complaints about management and the current union. He controlled access to the site by having a list of preapproved employees who were authorized to create an account. The terms and conditions for creating an account specifically stated that management was not permitted to access the site, and authorized users were prohibited from disseminating the contents of the site.

Word of the site got back to the management, which located two authorized users. One of those users had never been on the site, though he was on the list of approved people eligible to create an account. He gave management permission to use his name to create an account and access the site. Management created an account for him and reviewed the site. Konop filed suit under the SCA, among other laws. The district court granted a summary judgment to the employer. However, the Ninth Circuit Court of Appeals reversed the summary judgment, holding that the employer's access was improper, though not due to "forced consent" or trickery. Rather, the Ninth Circuit held that the employee was not an *actual user* of the site because he had never even been on the website. The SCA only permits "authorized *users*" of an electronic communication to grant others access to that communication. As the employee was not a user of Konop's electronic bulletin board, he could not give others permission to access that site. There was no discussion of the second employee, who provided his log in information to management and had previously accessed the site. This latter situation would likely be appropriate as the individual was an "actual user" under the SCA and appeared to have provided access to the employer voluntarily.

If an employer will participate in a social media site and request access to its employee's accounts, such access should only be requested under an account that clearly and correctly identifies the company or the name of the individual requesting access. If access is voluntarily granted to a restricted site or post, any information that an employer receives through that grant would not violate the SCA.

Take Advantage of Public Information

The SCA protects electronic communications that were intended to be private. It is not concerned with information that is made publicly available. If an employee has posted something on a website that is accessible to anyone (or anyone with an account, such as comments viewed on certain bulletin boards or comments to news articles), then an employer can properly review and rely on that information without running afoul of the SCA. This includes posts on internet blogs that are open to the public, posts to social media that are generally viewable without any type of authorization, and personal or other company webpages that do not require password access.

Software and technology are constantly evolving, and doing so at a pace far more rapid than the law.

Rules on Conducting Searches for Electronic Communications

When conducting searches for electronic communications, clients will want to adhere to four rules: (1) use caution when accessing restricted web-based accounts; (2) know your search; (3) there is an exception for company-based email; and (4) the SCA protections covers employees and independent contractors alike.

Use Caution When Accessing Restricted Web-based Accounts

Any electronic communication in "electronic storage" is protected by the SCA. This definition covers the obvious things, including web-based e-mail such as Gmail, Yahoo, and Hotmail, or company-provided e-mail. It also indisputably covers online social media sites. The more difficult question is to what extent other forms of web-based or cloud-based software are covered.

The U.S. District Court for the Northern District of Illinois was faced with that question when a salon filed suit against its former director for accessing the company's cloud-based management software. *Pascal Pour Elle v. Jin*, 75 F. Supp. 3d 782 (N.D. Ill. 2014). The court denied a motion to dismiss the complaint, finding that the cloud-based software had some vestiges of an electronic communication. Specifically, the software permitted direct e-mails and text messages to clients. While the district court was uncertain whether the complaint

would ultimately be successful, the court permitted the claim to proceed because sufficient facts were alleged that the cloud-based software was covered under the SCA.

Software and technology are constantly evolving, and doing so at a pace far more rapid than the law. Given this, it is not always clear how particular searches or access will be treated under the SCA. Generally, if a site has the capability of storing or sending private messages, then the site is likely covered by the SCA. If, however, the site does not have a private messaging capability, then the site is likely outside the coverage of the SCA.

Know Your Search

The SCA only covers electronic communications in "electronic storage." "Electronic storage" includes any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection." 18 U.S.C. §2510(17). What constitutes "electronic storage" is of much debate in the courts.

Unopened or unread messages stored on a web-based server are generally considered to be in "electronic storage"; the view is that they are in temporary, intermediate storage incidental to their transmission. Accessing this type of information without authorization is in direct violation of the SCA. In contrast, information saved directly on a computer's hard drive, a removable storage device, or a cellphone is generally not covered as "electronic storage" because it is not being stored by an "electronic communication service," but rather on the device itself. This type of information is outside the protections of the SCA. The hazy middle ground is the information somewhere in between. For example, what about an e-mail or text message that an employee read but did not delete?

The majority of courts agree that messages still saved in an employee's inbox or phone, where the employee can access them again, are covered by the SCA. Most of those courts treat this storage as an unofficial backup, which the SCA considers electronic storage. Other courts go into a more tedious and detailed analysis of how each server actually treats the message, whether the server continues to store a copy of the message after it is opened, or whether it is stored on an employee's personal computer. The minority of courts draw a strong line between read and unread messages, concluding that only those messages that are unread are covered by the SCA.

Items saved on an employee's assigned work computer can be reviewed without violating the SCA (though other laws may still apply). Items saved on a server elsewhere, or still saved on the internet, are likely covered by the SCA. If an employer wants to review an employee's computer or company phone, be cautious of the types of messages being reviewed (company or private) and how those searches are being conducted (hard drive only or web-based).

There Is an Exception for Company-based E-mail

The SCA addresses the accessing, obtaining, or reviewing of electronic communications that are sent through an electronic communication service. Typically, this term is limited to internet service providers, telecommunications services, and other entities that provide the actual service (compared to providing an item used simply to access that service, such as a laptop or cell phone). There is an exception to the SCA found in 18 U.S.C. §2701(c) that allows an "electronic communication service" to access electronic communications. This limited exception can apply to a company that provides its own e-mail server, stores the e-mails on the company computer system, and administers the system internally. *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107 (3rd Cir. 2003). It would also extend to permit a company to view text messages and cell phone-based communications when the employee composed or viewed them knowing that the cell phone communications were routed through a monitored company server. *Shefts v. Petrakis*, 758 F.Supp.2d 620 (C.D. Ill. 2010).

If this exception applies, a company can review the e-mails on the company server without running afoul of the SCA (though a proper policy should still be in place). Note, however, that this exception would be limited to company e-mails coming through the company server and would not include separate web-based e-mail or electronic communications. So, for example, a company that uses Gmail, Hotmail, Yahoo, or any other web-based e-mail provider for its e-mail would not fall under this exception.

The SCA Protections Cover Employees and Independent Contractor Alike

The discussion in this article has focused on employees and the employment relationship. However, the SCA's protections are not limited to employer-employee relationships. Rather, the protections apply to prohibit access by "any person" to private electronic communications of others. Given this, the same laws, limitations, and practices would apply regardless of whether an employer wants to review the electronic communications of its employees or an independent contractor.

Conclusion

The SCA is the quintessential example of a square peg in a round hole. It was originally crafted to cover electronic communications at a time when there were no e-mail or text messages and the internet was just beginning. The law has been amended several times since then to try to address varying issues faced by courts, but it largely remains a poor and confusing fit for today's technological world. Until a replacement law is passed, attorneys are faced with advising clients in this convoluted legal landscape.

For all of its twists and turns, the principal rules underlying the SCA can be summarized by stating that any private communication on the internet can only be accessed with knowing approval by either the sender or a proper recipient. Communications that are not private or are not stored by a communications provider are generally beyond the SCA's coverage. Likewise, posts to social media pages that are generally viewable and not protected by any kind of privacy restrictions, such as a requirement that a poster authorize viewing privilege or a requirement that a viewer log in, are ok for employers to access and review. Conversely, social media posts that are protected by privacy setting, or require authorization by the poster for a viewer to see are under the coverage of the SCA and should not be accessed by an employer without proper authorization. FD