"So what can I do (or not do)?" Employer control of employee activity and communications.

> "(The law) is like a single-bed blanket on a double bed and three folks in the bed and a cold night. There ain't ever enough blanket to cover the case, no matter how much pulling and hauling, and somebody is always going to nigh catch pneumonia."

Robert Penn Warren, *All the King's Men.*

Some of the most difficult choices an employer may be called upon to make concern the amount and degree of surveillance of actions of its employees.[1] In today's climate, the requirement of secure data storage and communications for businesses has never been more pressing. To combat this trend, employers may utilize enhanced security procedures to attempt to monitor employee-generated data and communications. The catch (and there always seems to be a catch) is that legitimate efforts to enhance data and communications security can sometimes lead to lawsuits by employees and others on the grounds of invasion of privacy and other claims.

The "business purpose exception" to the prohibition of the Electronic Communications Privacy Act ("ECPA")[2] of monitoring electronic communications specifically provides that employer may monitor employee communications if the employer has a "legitimate business purpose" for doing so. The employee may also obtain the employees' consent to monitoring, often by requiring acknowledgement by the employee when signing into the business network. Perhaps unsurprisingly, however, these provisions do not always protect the employer from litigation.[3]

The Stored Communications Act (SCA)[4] may also pose difficulties for employers. The SCA was enacted in response to Congressional recognition that neither Constitutional nor then-current statutory provisions adequately protected against "…potential intrusions on individual privacy arising from illicit access to stored communications in remote computing operations and large data banks that stored e-mails." [5]

These two complementary statutes are often discussed together in cases. The intersection of the ECPA and SCA has been described as a "…complex, often convoluted area of the law…" compounded by the fact that the ECPA was written prior to the advent of the internet and World Wide Web.[6]

---

1 This section focuses on issues surrounding employer control of employee communications, particularly by e-mail. Other aspects of control over employee behavior, or attempts to do so, are beyond the scope of this part.

2 18 U.S.C. sec. 2510 *et seq.*

3 For example, some state statutes require consent by *all* parties to the monitoring of a communication in order to avoid liability. *See, e.g.*, Cal. Penal Code sec. 632(a).

4 18 U.S.C. sec. 2701, *et seq*.

5 *Garcia v. City of Laredo, Texas*, 702 F.3d 788, 791 (5th Cir. 2012).

6 *Konop v. Hawaiian Airlines, Inc*., 302 F.3d 868,874 (9th Cir. 2002).

There are distinctions between these two statutory provisions, however, as illustrated by *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F.Supp.2d 548 (S.D.N.Y 2008). There, a former employer sued an ex-employee and the employee's new business, alleging that the employee had improperly appropriated customer lists and like data to aid in the start of the new company. At issue were a number of the employee's e-mails which the employer had obtained from outside electronic communications providers through various means, including a "lucky guess" that the password for those outside accounts was the same as for the employer's internal network.[7] The former employee sought to preclude the use or disclosure of those e-mails.

The Court held that the employer's act of accessing data maintained by the outside providers did not violate the EPCA, pointing out that this Act applied to persons who "intercept" electronic communications. Because the employer did not access and print the e-mails until well after they were sent and received (indeed, this occurred at some point after the former employee had left the company), the Court found that there could not be any interception as required by the EPCA.

A different result obtained with respect to claims under the SCA. The Court specifically pointed out that none of the items in question had been obtained from the employer's system, but had been found in the course of intrusions into employee's other networks, without the employee's knowledge.[8] The Court found that the employer accessed the servers in question without the knowledge or permission of the former employee, and obtained the e-mails in question while they were in storage on one or the other of the employee's systems. The court held that, "Either of those actions, if done without authorization, would be a violation of the SCA."[9]

In *Fraser v. Nationwide Mut. Ins. Co*., 352 F.3d 107 (3d Cir. 2003), Plaintiff Fraser had been an independent agent for Nationwide. After publicly criticizing Nationwide on a number of issues, he was terminated. While the agency contract specified that the relationship was terminable at will, the parties disagreed over the cause for termination: whether because of Plaintiff's activities with respect to state insurance authorities and public advocacy of positions antithetical to Nationwide's, or because of disloyalty, including approaches to Nationwide's competitors.

In response to Plaintiff's claims, and before his termination, Nationwide undertook a search of Plaintiff's e-mails which were contained on Nationwide's server, and apparently found documents confirming Plaintiff's "disloyalty." His termination followed.

The 3d Circuit found that Plaintiff could not demonstrate an EPCA violation, (1) because an "interception" violation under the Act can only occur contemporaneously with transmission of the message, and (2) because they were in permanent storage, not addressed by EPCA provisions.

---

7 The employer also contended that employee had provided at least some access information to other employees, who provided same to the employer.

8 587 F. Supp. 2d at 557-8.

9 *Id.* At 556.

Nor could Plaintiff make out a violation of the SCA, because the e-mails were stored on Nationwide's own system.

Possible exposure under EPCA and SCA is not necessarily confined to official acts by management on behalf of the company. For example, in *Lazette v. Kulmatycki*, 949 F.Supp.2d 748 (N.D. Ohio 2013), Plaintiff was a former Verizon employee who had been given a Blackberry to use in connection with her job duties. When she left Verizon, she turned in the Blackberry, mistakenly thinking that she had erased all personal e-mails, phone records, etc. (she was allowed to utilize the device for personal communications). A co-employee accessed these communications after Plaintiff turned in the device, which included personal communications received by the Blackberry after the surrender of the device, and subsequently shared some of these with other Verizon employees. The opinion states that these actions were within the course and scope of the co-employee's duties.

The Court found no actionable violations as to already-opened e-mails, as the Blackberry was not a "facility" under the SCA and no "interception" was made since the emails were already sent to employee's computer and opened.[10] However, it found a valid claim under the SCA where the co-employee opened any emails found to be unopened by Plaintiff. [11]

It is of course essential that an employer promulgate reasonable, readily understandable policies regarding monitoring of employee communications. The presence (or absence) of such a policy can be crucial in this type of litigation.

It has been stated that courts have "routinely" found that employees have no reasonable expectation of privacy in their workplace computers, at least where they are informed that they will be monitored. *Williams v. Rosenblatt Securities, Inc*, 136 F. Supp. 3d 593, 607 (S.D.N.Y. 2015). Citing *Pure Power Boot Camp, supra*, the *Williams* Court stated: "The plaintiff had no reasonable expectation of privacy in his work emails that are subject to the employer's review and RSI was authorized to access and obtain those emails." *Id*.

In *Shefts v. Petrakis*, 758 F.Supp.2d 620 (C.D. Ill. 2010), a company president sued other corporate officers, alleging that the installation of spyware on his desktop, laptop and Blackberry violated the ECPA, SCA and other statutes, entitling him to summary judgment. The Court rejected this contention, finding that:

---

[10] *But see, Hately v. Watts*, 913 F.3d 770 (4th Cir. 2019), holding that while previously opened e-mails might not be the subject of violations of the SCA subsection dealing with "temporary storage" of electronic communications, they did fall within the ambit of the subsection addressing protections for communications in "backup" storage.

[11] *Huff v. Spaw*, 794 F.3d 543 (7th Cir. 2015) presents an interesting "twist" on these fact patterns. There, an employee received a call inadvertently or "pocket" dialed from her supervisor's cell phone. Realizing that she was overhearing conversations relating to sensitive personnel matters, the employee recorded an extensive discussion, which was later disclosed to management. The supervisor sued, alleging violations of the ECPA, among other claims. The 7th Circuit affirmed entry of summary judgment on the supervisor's claims, holding that the supervisor failed to exhibit an "objective expectation of privacy," analogizing the supervisor's inadvertent dialing to forgetting to pull the drapes on a home window facing a public street. Thus, *Huff* appears to be an obverse application of the principles discussed in this section. However, claims of the supervisor's spouse were held not to be barred, which illustrates some of the limitations of defenses based on statutory provisions.

> "…the Employee Manual makes clear that Plaintiff's electronic communications on Company equipment are subject to archiving at all times. The Manual states, in relevant part, 'Employees must be aware that the electronic mail messages sent and received on Company equipment are not private and are subject to viewing, downloading... and archiving by Company officials at all times.' The Manual also defines 'electronic mail messages' as including 'personal/private/instant messaging systems.'" [12] [internal record citations and footnotes omitted].

Thus, the Court found that Plaintiff had consented to the logging of his communications as a matter of law.

Other cases have also considered the extent to which liability can attach because of an employer's review of employee communications using the employer's facilities. In a case arising under state law,[13] the Court in *Falmouth Firefighters Union v. Town of Falmouth*, 2011 WL 7788014 (Mass. Barnstable Cty., Feb. 2, 2011), a firefighter sued the City after personal e-mails, sent through a City-administered account, were reviewed in connection with an investigation. The Court held that no expectation of privacy existed, where the Defendant City's own account was used for the communications.

The results are rather more mixed in cases involving an employee's e-communications with his or her lawyer. Two state court cases illustrate this point.

In *Scott v. Beth Israel Medical Center*,17 Misc.3d 934, 847 N.Y.S. 2d 436, 441-43 (N.Y. S. Ct. 2007), Plaintiff contended that Defendant had improperly accessed a series of e-mails between Plaintiff and his attorney (PW), during the period of time Plaintiff was employed with Defendant Beth Israel (BI). Rejecting this contention, the Court pointed out that all of the e-mails in question were sent over Defendant's server. Importantly, Defendant's written policy specifically provided that:

> "Employees have no personal privacy right in any material created, received, saved or sent using Medical Center communication or computer systems. The Medical Center reserves the right to access and disclose such material at any time without prior notice." [14]

17 Misc. 2d at 936-7.

The fact that the e-mails in question were between Plaintiff and his attorney did not bolster Plaintiff's arguments. The Court pointed out:

> "… the effect of an employer e-mail policy, such as that of BI, is to have the employer looking over your shoulder each time you send an e-mail. In other words,

---

12 758 F. Supp. 2d at 651.

13 MGL c. 214, sec. 1B, "Right of Privacy."

14 17 Misc. 2d at 936-7.

the otherwise privileged communication between Dr. Scott and PW would not have been made in confidence because of the BI policy."[15]

However, in *Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650, 201 N.J. 300 (2010), Plaintiff, while employed with the Defendant company, sent e-mails to her attorney using the company's laptop, although the communications utilized a personal, password-protected account. When Plaintiff resigned, her laptop was returned to Defendant, which subsequently was able to retrieve those e-mails.

Later, Plaintiff filed an employment discrimination complaint against Defendant and, after it appeared that Defendant had obtained and copied the e-mails in question, demanded their return. Defendant objected, arguing that Plaintiff had no reasonable expectation of privacy with respect to e-mails sent or received on company computers. Defendant's Electronic Communications Policy [Policy], specifically provided that:

> "…Loving Care may review, access, and disclose "all matters on the company's media systems and services at any time."

It also states that e-mails, Internet communications and computer files are the company's business records and "are not to be considered private or personal" to employees. It goes on to state that "occasional personal use is permitted."

The New Jersey Supreme Court held that the Policy was not sufficient to overcome Plaintiff's reasonable expectation of privacy:

> "…we find that Stengart had a reasonable expectation of privacy in the e-mails she exchanged with her attorney on Loving Care's laptop.
>
> Stengart plainly took steps to protect the privacy of those e-mails and shield them from her employer. She used a personal, password-protected e-mail account instead of her company e-mail address and did not save the account's password on her computer. In other words, she had a subjective expectation of privacy in messages to and from her lawyer discussing the subject of a future lawsuit.
>
> In light of the language of the Policy and the attorney-client nature of the communications, her expectation of privacy was also objectively reasonable. As noted earlier, the Policy does not address the use of personal, web-based e-mail accounts accessed through company equipment. It does not address personal accounts at all. Nor does it warn employees that the contents of e-mails sent via personal accounts can be forensically retrieved and read by the company. Indeed, in acknowledging that occasional personal use of e-mail is permitted, the Policy created doubt about whether those e-mails are company or private property."[16]

---

15 17 Misc.3d at 938.

16 990 A.2d at 663.

The Court flatly disagreed with the holding in *Scott v. Beth Israel, supra*, and other cases which found such communications using employer facilities were not protected.[17] A key distinction seized on by the Court is that Ms. Stengart utilized a password-protected account that, while accessed on the company-owned laptop, was separate and password-protected. The Court pointed out that this indicated Plaintiff's *subjective* expectation of privacy. The Court went on to hold, however, that this expectation was *objectively* reasonable, because (1) the policy did not address personal accounts at all, (2) it failed to warn employees that e-mails sent on personal accounts could be retrieved and read, and (3) it created doubt about whether such e-mails were personal or company property.

Leaving no doubt as to where it stood on the issue of employee communications privacy, the Court went on to flatly hold that even a perfectly clear policy, unmistakably declaring that all e-mails, even to or from employees' personal counsel, were company property, would be void and unenforceable as against public policy.[18]

Stengart did not elaborate on criteria for the reasonableness of a subjective privacy expectation, focusing rather on the perceived ambiguities in the company policy. While no policy can be perfect, that discussed in *Beth Israel, supra*, would seem to compare at least somewhat favorably to the one discussed in *Stengart.*

The specific language used in the employer's policy on workplace communications can be the key to the result in a particular case. In *Bingham v. Baycare Health System*, 2016 WL 3917513 (M.D. Fla. 2016), the employee had maintained correspondence with his lawyers on a personal computer, but had downloaded certain items to his work computer for ease of reference. In weighing the extent to which the privilege applied, the Court pointed out:

> "…courts consider the specificity of the policy and the extent to which the policy diminishes an employee's reasonable expectation of privacy in communications transmitted over the employer's systems. However, because the overarching consideration in determining whether a communication is privileged is whether the individual had an objectively reasonable expectation that his or her communications were confidential, privilege determinations of this nature are extremely fact-specific and often depend on the particular policy language, if any, adopted by the employer."

The Court went on to state:

> "In determining this issue, courts have considered the following four factors: (1) whether the corporation maintains a policy banning personal or other objectionable use; (2) whether the company monitors the use of the employee's computer or e-mail; (3) whether third parties have a right of access to the computer or e-mails; and (4) whether the corporation notifies the employee, or whether the employee

---

17 Interestingly, both *Stengart* and *Scott* cite *In re Global Crossing Ltd*., 322 B.R. 247 (S.D.N.Y. 2005) as authority. This bankruptcy case held that the use of a company's e-mail system by an employee communicating with the employee's personal counsel does not, without more, waive the privilege.

18 990 A.2d at 665.

> was aware, of the use and monitoring policies. See Asia Global, 322 B.R. at 257. The four-factor test provides persuasive guidance in evaluating whether an individual's expectation of confidentiality is reasonable in light of the existence of other factors that tend to cast doubt on the reasonableness of that expectation, namely the scope of an employer's policy. See id. at 258 ("[T]he question of privilege comes down to whether the intent to communicate in confidence was objectively reasonable.")."[19]

The company policy in *Bingham* provided specifically that the system was for the use of legitimate company business, and that while employees could make very limited personal use of company computers, no personal business could be transacted. The policy specified that all communications on the system was company property and not the private property of any employee. Disregarding the employee's contention that, although he was generally aware of the possibility of monitoring, he thought it was only occasional and for certain purposes, the Court held that the Defendant company had legitimately accessed the e-mails in question between Plaintiff and counsel.

The disparity among the results discussed above may well lead to confusion, not to say despair, on the part of those attempting to construct reasonable, comprehensive and understandable policies governing communications by employees pertaining to their job duties, or otherwise while utilizing employer-provided equipment or facilities. Drafters can be torn between sometimes competing goals of comprehensiveness and ease of understanding. Frustratingly (at least to defense counsel), policies which appear at least similar may be upheld in one case, yet denounced in another.[20]

The cases discussed above illustrate that employers must exercise careful consideration to protect the company and its data, yet avoid overstepping in formulating policies designed to safeguard the company's intellectual property. Notwithstanding the decisions in *Scott v. Beth Israel* and *Bingham,* both *supra*, an employer's monitoring of communications between employee and counsel obviously carry the highest degree of risk.

Likewise, accessing an employee's communications outside the employer's system, as discussed in *Pure Power Boot Camp, supra*, is hazardous in the extreme. There, not only did the company lose the argument, but the intrusion into Plaintiff's personal networks exposed defense counsel to sanctions. This also occurred in *Stengart, supra*, even though the court found that accessing Plaintiff's communications was done simply in the course of zealous representation.

Bright-line criteria are difficult to define in many contexts, and especially so in the area of monitoring employee communications. That said, the cases examined above indicate that thoughtful, comprehensive and precise provisions in company policies, based on clearly-expressed needs of the company, stand a good chance of surviving court tests. Policies which are ambiguous

---

19 Note that both *Bingham* and *Stengart* discussed the "objectively reasonable" test in evaluating an employee's expectations or intent of privacy, although arriving at divergent conclusions.

20 *E.g., compare Scott, supra, with Stengart, supra.*

enough to give rise to an employee's "reasonable expectation of privacy," as described by the *Stengart* court, may not prove as robust.