Every Breath You Take, Every Move You Make, I'll Be Watching You

Materials Prepared By: Liz Roussel, Richard Caldwell, Jr. and Jennifer Smith Thomas

This presentation will take a look at how companies are using technology to track their employees' work activities. We will discuss what technologies employers are using to collect data about their employees, what information they can collect with that technology, how they can use the data to their benefit, what risks and limitations they might encounter if they choose to collect or use the data, consider the potential for unintended consequences, and end with some takeaways.

What technologies are employers using to collect data about their employees?

Let's considering the different types of technology employers can use to track their employees and surveil their activities.

It wasn't too long ago that employees could work for companies for years without their employer knowing much at all about their health, personal habits, work habits, or activities outside of work unless their supervisors or co-workers personally observed it or they chose to share it. Many employers also did not use technology for operational purposes. They used sign-in sheets to record attendance and keys to open and lock entryways.

Today, of course, is a different story.

Employers are routinely using technology to improve efficiency, security, accuracy, to measure productivity, and even to direct people's work. This includes GPS technology, time-keeping software, and security access devices. Employees often also elect to use technology in connection with wellness programs, such as Fitbits and Apple Watches. Of course, many jobs require employees to use computers, and to access them at the office and remotely, and require the use of smart phones. In some industries and professions, sophisticated computer technology is incorporated into clothing and personal protective equipment. In some workplaces, employees even have the option to have a microchip installed under the surface of their skin.

In 2019, Gartner, Inc., a research and consulting company, published survey results indicating that nontraditional monitoring techniques (like tracking employees' movements around the workplace and their biometric data) rose from 30% of the 239 large corporations it surveyed in 2015 to 50% in 2018. It anticipated the number to increase to 80% by 2020.

What information do employers have the ability to collect?

All of this technology enables employers to capture different kinds of data. With GPS technology, employers can locate their employees, determine the rate of speed they are traveling, and see the routes they are taking to get from point A to point B. Employers that no longer rely on sign-in sheets and punch clocks to record time worked may be using fingerprints to determine when employees arrive at and leave from work or be using other computer software applications. To ensure building security, employers may be using facial recognition software or hand geometry scanners.

More and more frequently, employees are investing in Fitbits and Apple Watches to record biometric data like their heart rate, number of steps taken in a day, temperature, and sleep patterns. Of course, this same sort of biometric data often is stored on employee's smart phones and those devices also can serve as location trackers.

With company-issued computers and laptops, employers can determine when the computers are on and off, when the employee is connected to its server through a Virtual Private Network, and how much time the employee spends browsing internet sites.

Some company-issued clothing designed to improve safety can also capture biometric data. For instance, companies can purchase hats fitted with EEG monitoring devices that can detect fatigue. "Smart fabrics" can monitor heart rate, temperature, and location.

In some workplaces, employers have also offered employees the option to have microchips inserted into their hands that they could use to swipe into work, sign on to their desktops and pay for food. The companies that offer these technologies point out that they provide benefits like contactless entry to workplaces and contactless payment methods.

Potentially, companies can obtain personal information about employees without their knowledge. There are numerous ways to engage in data mining of publicly-available information that employees post on social media. For example, one author has written about "Project Comet," a program that mines data from employees' social media accounts and analyzes that information for employers.[1] The program uses text mining and data scraping to search through an individuals' social media feeds. The program then aggregates and sorts the information for easier interpretation. Healthcare

[1] Eisenstadt, Lenora, *Data Analytics and the Erosion of the Work/NonWork Divide*, 56 Am. Bus. L.J. 445, 471-75 (2019).

companies have used this information in two ways. First, it is used to build better teams.[2] Project Comet's algorithm is fed data on an existing, successful team, including variables on the team members' hobbies, consumer preferences, interests, habits, and beliefs. The idea is that those factors, in combination, create positive working relationships. Project Comet then searches for those variables in all employees and attempts to combine employees into teams to replicate the original successful one. The program is also used in the health insurance context. Essentially, it will mine social media data to determine employee risk factors and then the company will use that information for assistance in setting insurance rates.

How can employers use the data for their benefit?

As employers continue to modernize their businesses to incorporate the most current technology available, they are learning that the data they collect can benefit them.

Let's take **wage and hour claims and compliance** as an example. Wage and hour claims continue to be among the most popular claims filed by plaintiffs against employers. They are popular because of the potential to bring them on behalf of groups of people collectively and because of the availability of statutory penalties and attorneys' fees. The Department of Labor also has continued to step up its wage and hour compliance investigative efforts. In 2019, the DOL reported collecting $322 million in wages owed to workers. Often wage and hours claims involve allegations that employers did not pay employees for time they worked.

Employers can use data, such as the data reflecting when employees' computers are on and off or when they are connected to the company's server via the VPN to verify the accuracy of time records, to investigate demands for non-payment of time allegedly worked, and sometimes to defend against claims when they are made.

Data that can be collected from smart phones and GPS devices in company vehicles also can be used to determine when employees arrive at and leave job sites. Employers may also be able to use that technology to confirm that employees are taking meal and rest breaks if they are required or to confirm that employees are not using more than the allowable amount of time for breaks.

Some employers also are using collectible data to evaluate **performance and productivity** and to award **incentive compensation**.

For outside sales jobs, employers can review data from GPS devices in vehicles to determine whether employees are making sales visits, the amount of time they are

[2] *Id.* at 473.

spending at customer sites, whether they are covering their territory, and the time they are devoting to making sales calls. They can incentivize employees to work longer hours, cover more territory, and make more sales visits by structuring compensation systems that rewards the behavior they want to see.

Some published studies have correlated the amount of time employees spend on their cell phones with their productivity. Employers with access to information about the amount of time employees spend on their cell phones during work hours can rely on that data to support disciplinary action or in evaluating employee performance and determining eligibility for merit raises.

Some employers have sophisticated means of analyzing employee computer usage—such as measuring keystrokes and knowing when employees access various software applications or create or save file materials. That information also can be used to evaluate performance and productivity. This has become and may continue to be increasingly important in environments where employees work from home, but do not have jobs where their level of activity and commitment outside of the office can readily be determined by other means, such as recording billable hours or generating reports or other outputs.

Technology and collectible data also can play an important role in **safety compliance**. In some industries—like trucking and transportation—companies have been relying on this type of information for years to ensure that employees are driving at safe speeds and not driving for more hours than the law allows. But using GPS and similar technology in company vehicles to achieve the same objectives in businesses that do not primarily provide interstate transportation services has become increasingly common.

Technology also can be used to ensure compliance with **other policies**. Recently, many companies have used software applications to ensure compliance with newly issued **COVID-19 safety policies**. You are familiar with them. Companies have issued policies requiring employees to stay home from work if they have a temperature or feel symptomatic for the virus. Employees can use apps to screen for symptoms and make determinations as to whether to go to the office or stay home.

Some of the same devices employees use to monitor their health and wellness are offering these sorts of products. For instance, Fitbit developed a "Ready for Work Solution" that monitors temperature and symptoms and allows employees to use a Daily Check-in feature to give them guidance on whether they should go to work and/or allows employers to receive reporting and analytics to determine whether to allow and employee to come to work.

A number of employer-sponsored health benefit plans offer incentives to employees who take proactive measures to live healthier lifestyles. For instance, UnitedHealthcare offers a program called UnitedHealthcare Motion that gives participating workers up to $1,000/year if they hit certain goals (e.g., 10,000 per day with 3,000 within 30 minutes). Blue365 – is a program that offers Blue Cross members with a discount if they purchase a FitBit. Aetna has a similar program with Apple Watches. Employees can choose to share the results of their efforts with their employees. According to an annual survey from the Kaiser Family Foundation, 14% of employers who offered health insurance in 2017 collected data from their employees' wearable devices. In 2018, that number was around 20%. One tech consulting firm has predicted that annual sales of wearable devices for company wellness programs will hit 18 million in 2023.[3]

Significantly, if employees choose to share this data with their employers or authorize FitBit, Apple, etc. to collect it, it can lose its HIPAA-protected status. This means employers can learn information about their employees' health—such as information about the number of steps they are walking each day, their resting and active heart rate, their sleep patterns, and more. If the information is not HIPAA protected, employers may be able to use it in ways they otherwise wouldn't. This is because the Health Insurance Portability and Accountability Act, prohibits doctors, hospital and insurance companies from disclosing personal health information, but may not protect from disclosure that same information once the employee has authorized it to be shared with employers or companies like Apple and Fitbit.

For instance, last year, the Washington Post ran an article about a plastic fabrication company in Texas that invited employees to participate in the company's wellness program and to share the data collected about their health and fitness with their employer.[4] One employee returned to work after suffering a heart attack and having triple bypass surgery. Through an app on his phone, his boss was monitoring his steps and would encourage him throughout the workday and workweek by sending him messages like "Man! I noticed your steps have picked up. You used to be under 2,000, now you're over 6,000. Two times you worked out this week. Good!" When interviewed about this workplace environment, the employee—who was 51 years old—

[3] https://www.advisory.com/daily-briefing/2019/02/20/employee-wearables (citing ABI research)

[4] https://www.washingtonpost.com/business/economy/with-fitness-trackers-in-the-workplace-bosses-can-monitor-your-every-step--and-possibly-more/2019/02/15/75ee0848-2a45-11e9-b011-d8500644dc98_story.html.

said he didn't find the real-time health monitoring intrusive and appreciate it, finding it motivating.

The employer also maintained and published rankings and every quarter the employees at the top of the rankings received a small check from the employer's health insurer.

Interestingly, most of the employees at this Texas facility who elected to participate in the program were older. Fewer millennials chose to participate. But one of those who did and who was interviewed about the programs said he wasn't concerned about what data was collected or where it went. He viewed privacy as something that may need to be sacrificed in exchange for the benefit of using technology.

What are the risks and limitations associated with using the data?

From an employment standpoint, the paramount concern, of course, is that employers will rely on the data they collect to make employment-related decisions. Organizations that advocate for consumer privacy[5] are concerned that employers will rely on what they know about employees' activities outside of work and their health to decide who to retain, promote, demote, or layoff. And certainly employers who choose to collect and use the sort of data we've been discussing open themselves up to the risk that workers who suffer adverse employment actions will claim that the data factored into the decision-making process. Employers can always defend against those types of claims by demonstrating that they did not rely on the data in question.

But what if they did rely on the data? Is that necessarily improper or impermissible?

It depends.

In some cases, employers clearly are within their rights to use available data to make employment-related decision. For instance, if an employer can determine through GPS technology that an employee is consistently speeding while on the job or is lying about the time he or she arrives at and leave the job site, it can take disciplinary action Likewise, if an employer can determine that an employee isn't actually working from home because it can see that they haven't turned on their computer or connected to the VPN, it can take disciplinary action.

But employers can get in trouble if they use information they haven't disclosed that they will be collecting. For instance, some states have laws prohibiting employers from

[5] Electronic Frontier Foundation

placing a GPS device in an employee-owned vehicle without consent. For instance, in Illinois, it is a misdemeanor. And one New York court held that an employer violated the law by placing a GPS device in an employee's personal vehicle to confirm its suspicion that the employee was stealing time by lying about his time worked.[6]

In some instances, it may be a statutory violation just to collect information without consent, regardless of whether the employer uses it. I suspect that many of you are familiar with the Illinois' Biometric Information Privacy Act (BIPA). This statute was enacted in 2008, but it didn't become well known until 2015 when five class action lawsuits were filed, including suits against a Facebook and Shutterfly.

Among other things, BIPA requires that employers obtain informed consent before collecting biometric data. It allows only limited disclosure of the information collected and has specific protection obligations and guidelines relating to retention and destruction of the information that is collected. It specifically prohibits companies from profiting from the biometric data collected and creates a private right of action. It allows for the recovery of statutory penalties in the amount of $1000 for negligent violations and $5000 for intentional violations. In 2019, the Illinois Supreme Court held that actual harm is not required to establish standing to sue under the law.

In one of the suits against Facebook, users of the social media platform brought a class action under BIPA accusing Facebook of collecting their biometric face information without consent or notice to use in its Tag Suggestions took, which uses facial recognition software to identify users' faces in images that are uploaded to Facebook. The only harm plaintiffs alleged was the statutory violation. Initially, the parties proposed to settle the case for $550 million, but the court refused to approve the settlement, finding the amount and the proposed remedial actions Facebook was required to take inadequate. A few months ago, the court approved a settlement in the amount of $650 million.[7]

The same sort of claim was made against Shutterfly. In that case, two consumers sued Shutterfly claiming that it violated BIPA by using its proprietary facial recognition technology to locate every face that appears in every photo uploaded to its service and then extracting face geometry from everyone, regardless of whether they are users of its services. That case hasn't reached its conclusion and in May 2020, the court ordered it to arbitration.[8]

---

[6] *Cunningham v. New York State Dept. of Labor* (NY Ct. App. 2013).
[7] *Patel v. Facebook, Inc.,* No. 3:15-cv-03747 (N.D. Cal.)
[8] *Miracle-Pond et al v. Shutterfly, Inc.,* No. 1:2019cv04722 - Document 68 (N.D. Ill. 2020)

As you might imagine, BIPA has created a new frontier for biometric data class action lawsuits. But most states do not have similar statutes. Some states—including Texas, Washington, California, New York, and Arkansas—have passed laws protecting biometric data or have expanded existing laws to include biometric identifiers.[9] But the statutes in those states don't clearly provide a private right of action or they limit

[9] **Texas**: Tex. Bus. & Com. Code §503.001 (a "person may not capture a biometric identifier" without a prior consent, may not sell biometric date without consent or unless allowed by law, must use reasonable care in storing it, and "shall destroy the biometric identifier within a reasonable time." The statute imposes civil penalty of "$25,000 for each violation," but there is no private right of action.

Washington: Wash. Rev. Code Ann. §19.375.020, prohibits any company or individual from entering biometric data "in a database for a commercial purpose, without first providing notice, obtaining consent, or providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose." Washington's law does not provide for a private right of action but authorizes enforcement by the attorney general.

California: The California Consumer Privacy Act (CCPA), which will go into effect in 2020, regulates biometric data by including it in the definition of personal information. The CCPA defines biometric data broadly to include "physiological, biological or behavioral characteristics, including … DNA[,] that can be used … to establish individual identity," including "imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information."

New York: New York amended its existing data-breach notification laws with its 2019 Stop Hacks and Improve Electronic Data Security (SHIELD) Act, which went into effect in early 2020. The SHIELD Act broadens the definition of private information to include biometric information. It defines biometric information to include fingerprints, voiceprints, retina or iris images, or other unique physical characteristics. Interestingly, it also includes other forms of unique digital representation of biometric data used for authentication purposes. Earlier, New York had also passed a limited biometric legislation, N.Y. Lab. Law §201-a, which applies specifically in the employment context. It prohibits fingerprinting "as a condition of securing employment or of continuing employment." It does not expressly provide for a private right of action.

Arkansas: Arkansas amended its breach-response laws, Arkansas Code §4-110-103(7), by revising the definition of covered personal information to now also include biometric data. It defined biometric data to include an individual's "Fingerprints; Faceprint; A retinal or iris scan; Hand geometry; Voiceprint analysis; Deoxyribonucleic acid (DNA); or Any other unique biological characteristics."

enforcement to the state attorney general. Nonetheless, employers who collect biometric data should ensure they are familiar with the laws in the states where they operate and know whether they need consent from their employees to collect it.

Employers also need to be mindful of traditional tort claims, like invasion of privacy. For instance, several years ago an employer in California fired its employee after she disabled the GPS technology in her company-issued smart phone.[10] The employee sued her employer asserting traditionally tort claims, including invasion of privacy. Ultimately, the case settled so we don't know whether the employee would have prevailed in the case.

Additional Issues Under the Electronic Communications Privacy Act and the Stored Communications Act

> "(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. 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") 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.

[10] *Arias v. Intermex Wire Transfer*, 15-cv-01101 (E.D. CA, 2015)

The Stored Communications Act (SCA) 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."

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.

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. 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. 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."

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. 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. However, it found a valid claim under the SCA where the co-employee opened any emails found to be unopened by Plaintiff.

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:

"…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.'" [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, 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.”

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, the otherwise privileged communication between Dr. Scott and PW would not have been made in confidence because of the BI policy.”

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."

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. 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.

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 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.")."

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.

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

Might there be unintended consequences associated with collecting or using the data?

Many laws provide guidance in about the sort of data that can be collected and used, but what about the law of unintended consequences? This old adage teaches caution when delving into things that are complex or unknown and it would seem to be relevant to the topic at hand.

Take the Hard Rock hotel project in New Orleans as an example. The City of New Orleans installed GPS equipment in vehicles operated by inspectors working for the Department of Safety and Permits. Presumably, the City installed the technology to track the whereabouts of its assets and also to track the activities of its employees while they were working. However, news outlets investigating the hotel collapse have reported that information on the logs completed by certain investigators disagrees with their vehicle GPS information. Specifically, they have questioned whether inspections actually occurred on certain dates because the logs says they did, but the GPS information from the inspectors' vehicles indicates they did not visit the hotel site that

day.[11] This would be an example of an unintended consequence because the City chose to employ the technology and collect the data for one purpose for its benefit, but it ultimately could be used for another, to its disadvantage.

What should employers do if they want to collect and use this sort of data?

- Be intentional – about the type of data you intend to collect and how you plan to use it
- Obtain consent – particularly if you are collecting biometric information, notify your employees and obtain written consent; offer employees the option to opt-out of providing the information
- Be transparent – tell employees what data you are going to collect and how you are going to use it
    - Attitudes toward privacy are changing—but employees want transparency (see Gartner survey)
- Know the law – confirm that there aren't any state or federal laws prohibiting the collection of use of the data or requiring special permission to use it
- Make a compliance plan - if you conduct business in state that has laws protecting the use and disclosure of certain types of information, understand your retention and destruction obligations and the limitations on your ability to use and disclose the information.

[11] https://www.fox8live.com/2020/02/18/zurik-city-inspectors-approved-work-hard-rock-hotel-site-gps-shows-they-were-not-there/