MONITORING EMPLOYEE COMMUNICATIONS THE DELICATE BALANCE BETWEEN AN EMPLOYER'S RIGHT TO REVIEW AND THE EMPLOYEE'S RIGHT TO PRIVACY

I. INTRODUCTION

In 1929, Secretary of State Henry Stimson famously made the proclamation that "gentlemen do not read other people's mail" in connection with his feelings against creating a national intelligence agency. Based upon the way we now exchange information and the blurred lines between work and personal emailing, that sentiment cannot survive the modern management landscape.

New technology has caused courts to grapple with balancing rights of employers seeking to monitor employee communications created on company equipment against the rights of employees. Employers fact critical dilemmas with respect to the usage and monitoring of company/government equipment because business machinery has the potential for personal use which can lead to decreased productivity and potential liability for employers. The court system is now faced with a changing workplace environment and has been forced to address several instances of finding a bright line test to determine the degree to which an employer can monitor employee communications.

A. What communications fall under the "electronic communication" category?

1. Computer server communications.

   a. Email

2. Internet-based social networking sites.

   Facebook

   Myspace

   Twitter

   Linked in

   a. 3rd party wireless/cellular phone platforms

   Text messaging

II. DISTINCTIONS BETWEEN PUBLIC AND PRIVATE SECTOR EMPLOYEES

A. Public Sector- Have expectation of privacy arising from Fourth Amendment of US Constitution and New Jersey Constitution.

1. Arises from the fact that management's action triggers "government action".

B. Private Sector- Protections are based upon the recognized tort; "Intrusion on seclusion" requiring showing that someone intentionally acted to intrude on someone's privacy rights.

III. RECENT COURT DECISIONS SHAPING ELECTRONIC COMMUNICATIONS MONITORING

Email Communications

STENGART V. LOVING CARE AGENCY, INC. 201 N.J. 300 (2010)

A. Facts: Plaintiff was an Executive Director of a large nursing facility which provided her with a company laptop with internet access through a company server. Stengart was not aware of the fact that the company had a program embedded in the machine that copied and documented her website usage and saved the contents of webpages from her browsing. The non-government employee plaintiff filed an action against her employer alleging violations of New Jersey's Law Against Discrimination. Relevant to her LAD Complaint, Stengart used her work computer to access her personal e-mail account, which was password-protected to exchange contact with her attorney related to the lawsuit. Loving Care retained a forensic expert to extract her personal communications and gained access to the employee's communications with her attorney by e-mail. Stengart filed an application seeking return of the e-mails and Loving Care opposed on grounds that their Company Policy outlined in the Employee Handbook permitted them to retain and review the emails.

B. Decision: The trial court found that the company's electronic communication policy was unambiguous and because of the company's asserted proprietary rights, Stengart waived the attorney-client privilege by sending personal e-mails on the laptop. The Appellate Division reversed and found that Loving Care's counsel had violated applicable Rules of Professional Conduct by reading and using the privileged documents. The Employer's motion for leave to appeal was granted and the New Jersey Supreme Court granted Certiorari. The New Jersey Supreme Court found that Loving Care's electronic communications

policy was in fact vague and further found that the plaintiff had a reasonable expectation of privacy.

The New Jersey Supreme Court's Decision was qualified by the court insofar as the Court addressed the notion that its decision should not be viewed as a complete bar on monitoring employee communications in New Jersey.

C. **Keys From Stengart-**

This expectation consists of both the employee's subjective expectation of privacy and an objectively reasonable expectation. State v. M.A. 402 N.J. Super. 353 (2008).

a. The subjective component consists of the employee's legitimate subjective expectation of privacy. The Stengart Court looked toward the ambiguity in the language of the Employee Manual regarding electronic communications, which explicitly advised the employee that some personal e-mail use was acceptable. This could very well give an employee a basis to form the legitimate belief that his or her personal communications were private.

b. The objective component necessary has been defined as "not only an individual's expectation but also society's willingness to recognize that expectation as reasonable" State v. Sloane (193 N.J. 423 (2008) citing California v. Ciraolo 476 U.S. 207 (1986).

D. **Attorney-Client Privilege.** Obviously, the fact that the communications made by the employee were protected by another distinct privilege influenced the Court's decision in this regard and makes certain that an employer cannot rightfully review and utilize information absorbed from electronic communications in such a situation.

Text Messages

The U.S. Supreme Court has been the first to tackle this issue, but keep in mind that the seminal case in this regard is a public employer, so there will obviously be some differences in this regard as it relates to private workers.

City of Ontario, California, et al. v. Quon 130 S. Ct. 2619 (2010)

Facts: The City of Ontario outfitted its police officers with cellular phones equipped with text message capability for work-related usage. A California police officer spent a significant amount of work time sending provocative emails to both his wife and his girlfriend that were obviously of a personal nature. Department policy did not specifically address text messages but the Department had a detailed policy regarding e-mail usage. The Department's policy for e-

mails gave the Department the right to monitor and log all network activity including e-mail and internet use and prohibited inappropriate obscene or suggestive language. The Department issued a memorandum advising its officers that the e-mail policy applied to the text messages sent by officers. In performing an internal audit of the text message use to determine whether the Department was properly using the system, it sought copies of the text messages from the cellular provider who turned over texts sent by Quan and upon review of the texts the Department disciplined Quan upon finding the inappropriate texts.

Decision: Interestingly, the Supreme Court did not address reasonableness of privacy and assumed that his subjective reasonableness was present. The Court found that the search had been motivated by legitimate work-related purpose, was not excessive in scope and not completely intrusive. The Department wanted to run a test to assess if their officers were overusing their text allotment and wanted to audit text records to see how much their officers were going over the limit and assessing the officers too much in the event that their officers were using the texts for work related purposes.

Social Networking Sites

Pietrylo v. Hillstone Restaurant Group 2009 WL 3128420 (D.N.J. Sept. 25 2009)

This opinion is unpublished but serves as a barometer for judicial review of social network sites.

Facts: Plaintiffs were Houston's Restaurant employees who started a group on My Space. The purpose of the group was by Plaintiffs' admission to "vent about any BS we deal with at work without any outside eyes spying in on us." The group was entirely private, and joined by invitation. The icon for the group, Houston's trademarked logo, would appear only on the My Space profiles of those who were invited into the group and accepted the invitation. Pietrylo invited other past and present employees of Houston's to join the group, including co-plaintiff Marino. Once a member was invited to join the group and accepted the invitation, the member could access the commentary whenever they wished to read postings or add new postings. Pietrylo also invited Karen St. Jean ("St. Jean"), a greeter at Houston's, to join the group, who accepted the invitation and made contributions. At some point, St. Jean inadvertently alerted management by accessing the page at the home of a Houston's manager whom she had a cordial relationship with. At some point another manager asked for the plaintiff's password to the group, which she provided same out of fear of reprisal. Although St. Jean testified that she was never explicitly threatened with any adverse employment action, she stated that she gave her password to members of the management solely because they were members of management and she thought she "would have gotten in some sort of trouble." Houston's management used the password provided by St. Jean to access the content from the page and printed the contents. Disciplinary

action was taken against the employee members of the group arising out of the statements and discussions made on the website.

Houston's did not have an en electronic communications policy applicable to their servers in the restaurant. The matter proceeded to trial and a jury found that Houston's conduct of demanding access the employees' private chats violated the Stored Communications act because the managers accessed the chat group without authorization and awarded the plaintiffs $13,000 in damages, inclusive of back pay.

For edification, the Stored Communications Act prevents an employer from accessing information form a third party access provider without prior, proper authorization. Pietrylo stands for the notion that an employee's password from a personal internet based account is private, in of itself.

Basically, an employer has to obtain proper authorization/consent to enter into an employee's protected account. Now, assuming management had a device that recorded activity in the hard drive that saved web page browsing, it is possible that the situation in Pietrylo could have been avoided. To do so, the employer should inform its employees that company equipment, and all activity on the equipment is the property of the company; therefore, all information contained on the computer can be retrieved from the computer hard drive and reviewed.

This type of policy, obviously, would have been difficult to express to employees in a restaurant setting, obviously, due to the fact that they typically are not privy to personal computer hardware found in an office setting, but in a more traditional office setting, a disclosure indicating that information contained on the computer would be company property, the expectation of privacy would be eliminated.

IV. OTHER CONSIDERATIONS

A. Gray Areas Regarding Equipment

1. **Ownership:** Courts accept a distinction between employees' use of company equipment and personal equipment.

a. Companies allowing "Smartphones" (Blackberry/Droid/Iphone) purchased by employee to be synched with workplace system must have an unambiguous policy regarding usage and privacy.

b. Company policy regarding the personal Smartphone must address handling of the information on the device itself.

2. **Content:**

a. Employee never has a reasonable expectation of privacy with respect to illegal activity.

b. Other laws may create an expectation of privacy, such as HIPPA for medical information, spousal communications, etc.

3. **Public Policy Grounds Lessen Expectation of Privacy:** Some industries require increased government oversight, which leads to a lesser expectation of privacy by employees. These "closely regulated fields" automatically lessen the expectation of privacy of employees and subject communications to higher scrutiny simply because the hardware is part of the closely regulated field.

a. Pharmaceutical industry
b. Financial Industry
c. Ports of entry- airports/sea ports
d. Government workers (OPRA Requests)
e. Energy/Natural Resources
f. Federal/State/Local Law Enforcement
g. Military Personnel

V. SYNTHESIS OF CASES

A. Although all of the cases involving employee use of email, text messaging and social networking sites have different nuances, the single most important component in determining management's right to review and utilize the information is notice to the employee that their activities on company equipment are subject to review. The lone exception of course occurs when an employer reviews web based social networking content by unlawfully obtaining passwords.

Here, letting the employee know that his or her activity on company equipment whether it be social or work related can be subject to review by management is of paramount importance.

VI. KEYS TO CRAFTING AN EFFECTIVE ELECTRONIC COMMUNICATIONS POLICY

A. Advise the employee that all computer and electronic resources are the company/government property.

B. State that all communications using company equipment lack privacy and can be reviewed at the company's discretion at any time.

C. Advise, with particularity, that the company can and will review all emails including personal, password-protected, web-based email accounts if they are accessed using he company's equipment.

D. Let employees know that all content of all emails are subject to review and are not private.

E. Create a policy that is distinct and unambiguous regarding usage of company equipment for personal communications. Employers should either allow personal usage (so long as the company/government maintains a right to review) or ban personal applications in their entirety.