Names: Brandon Bowling, EJ DeGuzman,

Mirsad Bekric, Scott Morgan,

Zach Smith

Section: CIS 150-76 Case Study: 5.4, Group 5

Case Name: E-mail Privacy at Johnson and Dresser

Date: 11/28/2016

Part 1: Ethical Dilemma

Johnson and Dresser, a moderate-sized retail brokerage firm implemented a newly advanced email system. With this system, employees would be encouraged using this system as the primary means of communicating with other employees within the company. When introducing the system at company training sessions they expressed that their privacy in using the email communications would be protected. However, the company neglected in informing employees that their messages would be kept in archive and be used for future use whenever the need arises. Lisa Curry, an analyst in the company sent emails to Margaret Leonard criticizing the company as well as their boss. Unbeknown to Curry, her emails were being inspected by her boss for her evaluation, and upon learning of the content of her emails he berated her for not displaying qualities of an employee within the company and abuse of the system. Because of this, Curry received a slight salary increase and mixed performance review although her performance as an employee was stupendous. However, with this policy the company was able to crack down on an inside trade scandal. Jason Perry, the Information Systems director received complaints regarding the system and wonders whether he should reconstruct a better email policy for the company. Despite the number of complaints, electronic monitoring is legal under the Electronic Communications Privacy Act of 1986. What should Perry propose to the executive committee?

Part 2: Role of I.T.

The I.T components that would be included are the computers, the company's network servers, the technology used to perform surveillance, and the email system itself. The computers are owned by the company which allows employees to conduct emails and send them to other employees within the company. Another component is the company's network. With Internet access, the email system is able to send mail digitally through the Web. The technology that monitors the employee's' emails is another important component. While monitoring the emails of employees, they will be able to intervene in any possible criminal activity going on within the company. The email system is the biggest component of this case. This system was implemented in the company and was encouraged to employees as the primary source of communications within the company. Using this system, the employers of Johnson and Dresser save these messages to the archive and can be accessed if the need ever arises.

Part 3: Stakeholders

1. Jason Perry: He began working at Johnson and Dresser as a Senior Systems Analyst, but after two years of service, he was promoted to Information Systems Director. His responsibilities were to oversee, purchase, and install an e-mail system, which would soon be depended on by many employees at Johnson and Dresser. Jason Perry has the right to meet with the executive committee of Johnson and Dresser to propose a new privacy policy that protects the employees. He also has the right to protect the company from any future scandals that might be contained in emails, along with sticking with their high moral ideals.

- 2. Lisa Curry/Employees: Lisa Curry is a 10 year veteran at Johnson and Dresser and her responsibility is to maintain a close relationship with the utility industry. Lisa provides reports of this industry to many brokers and inputs her opinion on which stocks they should look out for. Lisa was called in for her annual review and the manager pulled up her email which contained some that were criticizing Johnson and Dresser for being sexist and not being sensitive to specific issues. Lisa was in full belief that her emails would be permanently deleted if she and the receiver deleted them. Johnson and Dresser never mentioned to their employees that they would keep an archive of the emails and possibly use them for future issues, if any were to ever occur. Lisa's received a mixed annual review along with a small salary increment, due to the emails she had sent. Lisa has the right to do her job of keeping up with her specified industry, while receiving appropriate privacy and being able to express her thoughts about the company.
- **3. Chief Operating Officer**: The Chief Operating Officer main responsibility is to oversee the operations of the company. The COO makes sure that both the employee and the customer are treated fair and makes sure business is running smoothly. The COO has the right to address any problems that may occur and assign jobs to employees. The COO wants each employee to be aware of their privacy rights at Johnson and Dresser, while achieving the high amount of productivity as possible.
- **4._Johnson and Dresser's Customers:** The customers of Johnson and Dresser have the right to obtain services from brokers who are up to date with the stock market. The customers also have a right to have a say or control where their money is going. If insider trading is occurring within the company, this could affect what the customer's money is actually being used for and where it is going. Reviewing emails during each employee's annual review helps ensure that the customer is being taken care of and the employees are doing their best to achieve customer satisfaction.

Part 4: Alternative Actions and Consequences

- 1. Leave privacy policy as it is (Do Nothing): Archiving emails from employees to possibly view them in the future has benefitted Johnson and Dresser before. The company had a scandal occur that would have turned out a lot worse, if the emails were not archived and viewed. Sticking with the current policy will allow the company to discover any suspicious or scandalous actions that may occur. Johnson and Dresser is a well-known and respected company, and they will want to keep it that way. Archiving their employees email will help them in several ways, but it will also have some negative effects, such as employees not relying on email anymore, which improves productivity. There could also be trust issues with employees and those above, because the employees may believe they are still be monitored in more ways than one.
- 2. Change privacy policy so the company doesn't archive or view emails: Ever since Lisa Curry had her annual review, and the monitoring of employee's email was uncovered, there was a lot of anger and confusion. Employees were enraged at this because the company took no effort into letting their employees know the emails were actually being collected.

Changing the policy so the company doesn't collect emails will give their employees some relief, by allowing them to send confidential emails to one another. The downside to this is that the company and know knowledge of suspicious emails being sent, so will be more prone to scandalous behavior upcoming.

- 3. Leave the policy unchanged, but inform the employees: The IT department at Johnson and Dresser led many employees, along with Lisa Curry, that their emails were completely confidential. The IT department, out of everyone, should know that emails are being collected and possibly viewed. The IT department and those who are able to access archived emails should let the employees know that they are indeed being collected. Being honest and straightforward about archiving and viewing emails with the employees of Johnson and Dresser, will allow everyone to benefit. The employees will understand that they are trying to protect the company from any future scandals that may happen, and deal with them properly. Employees that do have the intention of scandalous behavior will refrain from using email because they know they are being watched. Releasing this information will allow the company and employees to have a better, more trustworthy relationship, but it will also decrease some emails being sent, such as scandalous emails as mentioned before.
- 4. Develop new policy that has more restrictions on the data being collected: If the company doesn't collect their employee's emails, they are more prone to negative employee behavior. Keeping their current policy will anger some employees because they want their privacy to be protected. One way to keep both sides happy is for each to give a little. This means, the company loosening up on what they collect, while the employees giving up some privacy in order to receive some privacy.

Part 5: Deontological Perspective

From a deontological perspective developing a new email monitoring policy would be the morally right thing to do. When training employees on the e-mail system Johnson and Dresser frequently compared e-mail to regular postal mail leading employees to believe that their emails were private. They encouraged employees to use the new email system to communicate with each other instead of making phone calls or quick office visits, but never mentioned that the emails would be monitored or archived. Unlike regular mail, employees do not have a right to privacy when using company computers and email servers. Johnson and Dresser were well within their rights both legally and ethically when monitoring the emails. Monitoring the emails had even helped find brokers who were guilty of insider trading. Due to the nature of their business Johnson and Dresser have a duty to ensure that their employees are behaving ethically in their business dealings. While it is within their right to monitor the employee emails, in order for it to be morally right from a deontological perspective, the monitoring must be applied equally to all employees. In the new e-mail monitoring policy Perry should be sure that the monitoring applies to everyone using the email system. Johnson and Dresser also has duty

to treat their employees with respect by not archiving messages for longer than necessary, and to give employees correct information about their privacy rights in the workplace. It is wrong to compare email to regular postal mail. Perry's new e-mail monitoring policy should be paired with a new training session for employees stating that their e-mails may be monitored in some cases. The new monitoring policy should be very clear in what information will be collected, how long it will be stored, and what the information will be used for. This policy should be readily available to employees of Johnson and Dresser. Developing this new, more detailed policy and informing the employees about it is the morally right thing to do from a deontological perspective.

Part 6: Teleological Perspective

From a teleological perspective, creating a new policy that has more restrictions on the data being created and conducting new training to fully explain that policy would be the best course of action. Teleology focuses on consequences, minimizing harm and maximizing benefits. The monitoring and storage of emails has benefited the company in the past when the company had the scandal of insider trading within their company. The company has a strong reputation and needs to maintain that reputation to conduct business so dealing with the matter swiftly really helped to maintain their integrity. However, keeping the policy as is might end up doing more harm than good as employees become untrusting of the company and may even decide to look elsewhere for work, which would still ruin the company's reputation from an employment standpoint. If the current policy is kept, the government, shareholders, and clients will have faith in the company, but the employees and the general public will not. Removing the policy of email monitoring all together is just as bad because even though such an action will boost morale, promote efficiency, and establish trust between the corporation and its employees, the risks for doing so is great. Not only can insider trading within the company occur without any way of monitoring such behavior or finding out who's responsible, but other illicit activities could go on under the executives noses. Employees using company resources to run side businesses, legal or possibly illegal, could also occur with no easy way to find the culprit. If someone was using the company's servers to conduct lets say a black market trade site and the company got blamed for it, then their reputation would be ruined, possibly beyond repair. The best action that minimizes risks to both sides would be to create a clear and concise new policy that explains to employees what will be monitored, what will be collected, how long will the information be kept, and all the rules for using company resources. This policy might indeed decrease efficiency because some employees will choose not to use company communications if they can help it and go out of their way to avoid being monitored, but letting the policies be known from the start will make sure that surprises like what happened with Lisa Curry don't happen again and it also removes liability from the company if an employee violates these rules. This minimizes the risks on both sides and creates a good compromise between protecting the company and protecting the employees.

Part 7: My Recommendation

There are many ways that the company could have went about the email monitoring system. Some things that happened within the current system hindered some employees due to the fact that the manager of Curry was allowed to see her emails. Below will be a list of things that need to occur in order to keep this system in place.

- 1.) First, the company needs to give more in-depth training to their employees on the mailing system and what exactly it entails. At one point when they were originally presenting the system to the employees, they were stressing the idea that all of the emails that they would send would be completely confidential. Which is untrue. This is already creating a level of distrust within the company and its employees. The company needs to be open with their monitoring methods and explain to the employees why this system is necessary. Since they've already caught an insider trading scandal with the system, the company could use this as evidence to further explain exactly this needs to be put into place. Once the company provides reasons to the employees why this is necessary, the majority of them will most likely come around.
- 2.) Secondly, the email archive system should be restricted and reviewed by an outside company. Meaning that most people in upper management, such as the supervisor that gave Curry a poor review, don't have access to such information. This could help avoid more cases such as Curry's, where the boss hands out a meager raise and a bad review just because of some comments on the way they handle things. This is not a way to run an operation. Having your employees fear that if they scrutinize the manager in any form that there performance reviews could potentially take a drastic hit. The company should outsource to another company to keep tabs on the archive of emails. This secondary company will be unbiased when viewing the archive emails and be able to make decisions about 'flight risks' to the company. It will also help employees get reviews they deserve and not reviews where the manager is sour due to his management style being scrutinized. With this in place not only will the email archive system be more secure, but it will allow more robust monitoring of the archive. Paying the security analytics company that would keep track of the archive would be costly, but it is a cheap price to pay to retain quality workers and maintain some semblance of privacy.
- 3.) The email system should also have a filtering system. Meaning that all emails would be archived, but only certain ones would be flagged for review. This automated system would search for keywords within the emails that could be pertaining to the company. This allows the company to keep up their observations of employees while also refining through the drivel that may contain smaller gossip talks and such. This is key to make the email system much more efficient than previously. It also helps the data analytics company analyze this 'big data' very quickly and get to the people that would be causing problems easier. The filtering system will have an algorithm that is always learning new things to spot by implementing new terminology into the program. This will be key in helping maintain the company image while also keeping in place the limited privacy that the employees have at a company such as this.

4.)