**The Customer List**

**Teaching Note**

**Overview**

James Bean began as a part time sales associate at Tax Solutions Software Center (TSSC). After roughly a year James was offered his current position as Head of Sales and Marketing. He reported to the two partners who owned the business, neither of which were part of the daily operations, but oversaw the larger picture. In his current role, Bean supervised an onsite sales staff of 4-6 people and two remote sales teams of 10 sales representatives. Bean also was in charge of payroll, daily supervision, marketing, client retention, and general sales. James was surprised, but not alarmed when Rand Smith, his top salesman, did not report for work. However, James was surprised when he checked the company’s Facebook page. He found a post from Smith to his former and next employer containing a list of TSSC’s major customers with proprietary account information. Bean was furious and asked himself what he should do next, and what he should have done differently to avoid this situation?

This critical incident is most appropriate for classes in sales management, ethics, and communications.

**Research Methods**

This critical incident is based on field research. All of the events are true, but names, dates, and location information have been changed to protect company confidentiality and employee rights.

**Learning Objectives**

After analyzing this incident students should be able to:

1. Identify potential conflicts between workplace privacy and proprietary information.
2. Evaluate ethical and unethical uses of company information and technology.
3. Recommend steps firms can use to protect company information and technology.
4. Discuss the concept of workplace privacy.

**Questions**

1. Why is there conflict over who owns a sales person's customer list?

2. Did the salesman do anything unethical in releasing the information? Explain.

3. Did the salesman do anything illegal in releasing the information? Specify what, if anything, you consider illegal.

4. What can the company do to keep this sort of thing from happening in the future?

5. Did the company make the right decision in reference to Smith’s Workplace Privacy?

**Questions and Answers**

1. Why is there conflict over who owns a sales person's customer list?

Conflict over the ownership of customer lists is common in organizations. Sales representatives often arrive at a new job with names of friends and contacts made from previous jobs. Companies typically provide new employees with a list of existing customers and potential contacts when they start a new job. Once on the job, sales people are also expected to generate new contacts and customers. When the sales person leaves, there is often disagreement about what portion of the list belongs to the sales representative and what belongs to the employer.

One way companies attempt to get around this conflict is to require employees to sign a non-compete agreement. The logic behind the agreement is that having the contacts will not hurt the current employer if the sales person goes to work for a firm in a non-competing industry. According to Humphries (2012), every employee who signs their employee handbook also signs a non-compete agreement contained within the employee handbook. In this incident, Smith is going to work for a direct competitor. He would be in violation of the company’s non-compete agreement.

2. Did the salesman do anything unethical in releasing the information? Explain

Information ethics is a serious issue in the workplace today. Many forms of technology make it easier for the transfer of information from business to business and employee to employee (University of Pittsburgh, 2009). Ethical issues arise and are often interpreted differently by different points of view, especially employer vs. employee. In this case, most people would argue that Smith’s actions are unethical. By transmitting confidential data to a competitor in the tax software business, Smith essentially stole the customer list and will likely use it to lure customers from his former employer.

This incident also raises a bit of hypocrisy common in organizations. TSSC did not consider it unethical when hiring Smith from his former employer, a direct competitor. TSSC was probably willing to allow him to bring customer lists, experience, training, etc. with him when he came to work for them. It could be argued his experience and contacts at his previous employer enabled him to be the high performer he was at TSSC. It is unknown, but doubtful, that TSSC would have refused to hire Smith had his previous employer had a non-compete clause in their employee handbook.

When he left to go to a competitor, however, TSSC cried foul. TSSC likely argued Smith was violating the policies of employer information confidentiality and non-compete in the employee handbook. However, one important difference is that Smith emailed the customer list and other proprietary information to a competing firm. He did not just take his experience and whatever information he could recall. He also informed the new employer that he expected to be paid for the information in the form of a higher salary.

3. Did the salesman do anything illegal in releasing the information? Specify what, if anything, you consider illegal.

Depending on the state, conditions of the information transfer, and employee contract, legality is always open for interpretation (University of Pittsburgh, 2009). The issue of customer list ownership discussed in an earlier question is part of that interpretation. Employees typically argue the information they took with them is what they brought to the job. Employers are often unable to prove otherwise so courts may rule the employee simply took what was already theirs.

Clearly, the salesman violated the non-compete portion of the employee handbook. Handbooks are often considered part of the employee’s contract with the employer (Humphries, 2012), hence, Smith violated his employment contract with TSSC. However, courts have sometimes been reluctant to enforce non-compete agreements. Typically employers are required to show damages in order for the court to determine a settlement amount. Proving damages is often difficult to do. Likewise, damages are often relatively small, and employers do not attempt to enforce the agreement as damages won are offset by legal expenses incurred in taking the case to court.

Students, and employees, may also argue Bean violated Smith’s right to workplace privacy. Again, TSSC had a policy guaranteeing employees the right to maintain friendships and have contact with people in competing organizations. The one stipulation was that the contact be made during the employee’s private time. Students may well consider Bean’s reading of Smith’s post as unethical because it was intended to be a private post. However, the post does not fall under workplace privacy for Smith (Privacy Rights Clearinghouse, 2012) because it was posted on a public page of Facebook.

If an employee suspects that an act is questionable, it is often more appropriate to not engage in the act than to engage in it and see what happens in court. As stated in the epilogue, TSSC took Smith to court. His defense was workplace privacy. The court did not agree with his position and awarded TSSC damages.

4. What can the company do to keep this sort of thing from happening in the future?

Employers have the legal right to monitor employees and discipline them accordingly. Email, phone, and verbal monitoring laws and how the monitoring takes place are different state to state, but are not illegal (Hamilton, 2012). The company can easily access employee internet usage, emails, phone calls, and listen to verbal conversations to keep future employees from doing the same thing. As the employer engages in this activity, it is best not to infringe on workplace rights and employee rights. An employer must find an equal and moral stance to employee rights and workplace privacy and act within legal boundaries (Hamel, 2012). TSSC can legally monitor their employees through phone, email, and verbal communications while at work. This monitoring can be conducted by supervisors or off site by electronic monitoring systems. There are also companies that do such monitoring.

It also can be argued that employers have the right to know whatever information is available as a way of protecting their property rights in the business. Thus, employers have the right to monitor any social networks for information about their employees. A quick internet search will show several instances of people being terminated or suspended for emails and blogs organizations found inappropriate (c.f., Ford, 2010; Holland, 2010; Clark & Roberts, 2010). Employees have the right to quit a job if they do not agree with the employment practices of the organization.

5. Did the company make the right decision in reference to Smith’s Workplace Privacy?

According to Hamilton (2012), Workplace Privacy is a different issue than employee confidentiality of trade secrets. An employee’s workplace privacy is an issue when an employee takes care of personal matters at work that are private and not involved with the place of business (Hamel, 2012). In the workplace, monitoring can take place when it concerns information about workplace issues or confidential information (Myatt, 2009). In this situation, TSSC did not violate Smith’s workplace privacy because the information communicated was about the business’ confidential information. TSSC is further covered because, the managerial staff decided not to take action against Smith when he had personal communications with his previous employer that did not include information the company considered proprietary.

**Epilogue**

Rand Smith was fired the day the message was placed on Facebook to his previous employer. Mr. Smith is now employed by Perfect Tax Company, once again. He signed one large client that he had generated while at Tax Solutions Software Center. The owner of Tax Solutions Software Center later took Smith to Small Claims Court and won a $4,000 law suit for his misuse of company property.

**References**

Clark, L. and Roberts, S. (2010). Employer’s use of social networking sites: A socially irresponsible practice. *Journal of Business Ethics*. *95*(4), 507-525.

Ford, C. (2010). Facebook: Professor suspended for posts. http://www.higheredumorning.com/professor-suspended-for-facebook-posts. Retrieved 3/4/2010.

Hamel, Gregory. (2012). Definition of Workplace Privacy. <http://smallbusiness.chron.com/definition-workplace-privacy-15419.html>. Retrieved 10/10/2012.

Hamilton, Regina. (2012). Employee Confidentiality Laws. <http://www.ehow.com/list_6782921_employment-confidentiality-laws.html>. Retrieved 10/10/2102.

Holland, J. (2010). Facebook (take 2): Student punished for blunder. [http://higheredmorning.com/school-punishes-student-for-facebook-blunder. Retrieved 3/4/2010](http://higheredmorning.com/school-punishes-student-for-facebook-blunder.%20Retrieved%203/4/2010).

Humphries, Kenneth. 01 September 2012. “Anonymous Company” Owner Interview. Personal Interview Conducted by David Green (With written Release of Information).

Myatt, M. (2009). Employer’s rights vs. employee’s privacy. <http://ezinearticles.com/?expert=Mike_Myatt>. Retrieved 3/4/2010.

Privacy Rights Clearinghouse. (2012). Workplace Privacy and Employee Monitoring. <http://www.privacyrights.org/fs/fs7-work.htm#computermonitoring>. Retrieved 10/10/2012.

The University of Pittsburgh. (2009). Information Ethics. <http://www.2.sis.pitt.edu/~ethics/>. Retrieved 01/15/2009.