Unit 5 Research Project

Eddie S. Jackson

Kaplan University

IT590 Legal and Ethical Issues in IT

Professor Linnea Hall, JD, MSBA

01/27/2015

TABLE OF CONTENTS

ABSTRACT....3
INTRODUCTION....4
PART I....4
Code of Ethics....5
Compare and Contrast....5
Differences....6
Adequacy....7
Unified....8
PART II....9
Workplace Privacy....10
Key Loggers....12
Email Scanning....12
Video Surveillance....12
Recommendations....13
Websense....13
Carrier Service....14
CONCLUSION....14
REFERENCES....16

Abstract

The study of ethics provides a window into human behavior. When ethics intersects with technology, understanding behavior and ethics become critical to maintaining the integrity of the technology. The primary issue with technology is its intrusive nature. On one hand, technology represents the progress of society; on the other hand, technology possesses the potential to impede upon a person's civil liberties, i.e. personal privacy and confidentiality. To gain an appreciation for ethics in information technology, a two part project has been designed on professional ethics. In part one, two codes of ethics are to be assessed, and a dialog created which discusses similarities and differences between the codes. In part two of the project, the ethical issues of a company using key loggers, reading employee email, tracking cellphone usage, and installing video surveillance are to be discussed. The research is meant to emphasize the value of professional ethics, as well as reinforce real-world ethical principles.

Keywords: Technology, ethics, information technology, ACM, IEEE

Unit 5 Research Project

The study of ethics is essential to distinguishing between what is *right* and what is *wrong*. The applied concepts of ethics promote a good reputation, maintain high quality in products and services, and facilitate the compliance of laws (BLR, 2011). A pragmatic approach to implementing ethics is through having a *code of ethics*. A code of ethics is a document that establishes specific guidelines that a professional should follow; this document may contain a mission statement, company values, organization standards, and other principles which are relevant to maintaining ethical conduct (Ethics Resource Center, 2009). Fundamentally, a code of ethics creates a framework for minimal acceptable behavior. Thus, it is no wonder why numerous professions—such as lawyers, paralegals, physicians, and nurses—have a professional code of ethics (Quinn, 2013). Considering ethics in information technology, although there is no official code of ethics, most organizations and technical societies do have a set of well-defined rules. These rules can be labeled as a code of ethics, code of conduct, or simply as polices. No matter what the label may be, the intention is clear; professionals are obligated to act ethically. To better understand ethics in information technology, two topics have been selected in a two part research project. In part one, two codes of ethics from technical societies are to be compared and contrasted. The code of conducts are to be assessed for differences, examined for their adequacy, and finally, clauses are to be drawn together to formulate a unified code of ethics. In part two of the research, the ethical concerns of key logging, monitoring e-mails, tracking cellphone use, and installing video surveillance are to be discussed. Afterwards, an appropriate plan for managing security is to be recommended. Each part of the research is meant to study ethical concepts, and how they relate to technology and working professionals.

Part I – Code of Ethics

Ethics in information technology are critical to the integrity of all technology-based systems. People that design, manage, and maintain technology have a responsibility to society. That responsibility includes making sure technology is safe, secure, meets industry standards, and does not violate any laws (Quinn, 2013). Because technology is vital to the everyday lives of many people, societies have been formed which advance technology, and encourage professional behavior. Two of these societies are ACM and IEEE. ACM, or Association for Computing Machinery, founded in 1947, is an educational and scientific community. ACM furthers computing by maintaining knowledge bases, writing and posting articles, hosting conferences, and providing student and professional resources (Association for Computing Machinery, 2015). IEEE, or Institute of Electrical and Electronics Engineers, founded in 1963, is a professional society dedicated to electronics, electrical engineering, and computing (Institute of Electrical and Electronics Engineers, 2015). IEEE has numerous technology publications, hosts conferences and job fairs, and has a reputation for advancing technology on a global scale. What is interesting about these societies, is that each society possesses a document that highlights a code of ethics. While there are similarities, the structure and wording in the documents vary greatly. Thus, these differences warrant further examination.

Compare and Contrast

Upon the initial assessment of the ACM and IEEE codes of ethics, it is evident that both codes expect their members to adhere to a greater level of professional standards. ACM states the objective of its code is to enhance professional responsibility (Association for Computing Machinery, 1992). IEEE declares its members are obligated to commit to professional conduct (Institute of Electrical and Electronics Engineers, 2014). Both codes

highlight what it means to be *honest*. ACM presents honesty as a building block for trust; this is honesty as it relates to claims about a system, research, or one's own credentials. IEEE conveys the importance of being honest when asserting claims and providing estimates that are based upon available research and statistical data. Both codes also touch on privacy and confidentiality. For instance, ACM describes a digital era where the potential of violating privacy has become greatly increased. Consequently, the members of the ACM community are compelled to act ethically, and make a conscious effort to protect the privacy and integrity of data. Although brief, the IEEE code of ethics also promotes the concept of privacy, by stating its members are to be respectful of privacy, personal information, and personal data. When it comes to treating people fairly, and acting in a non-discriminant manner, both codes include clauses that reinforce social equality. Each code of ethics covers the common equal opportunity factors, such as race, sex, religion, nationality, and disability. Though, IEEE extends the inequalities principles, by adding "gender, sexual or affectional orientation, gender identity, gender expression, appearance, matriculation, political affiliation, marital status, and veteran status" (Institute of Electrical and Electronics Engineers, 2014, para. 3). One final topic outlined in both codes is *intellectual property*—that is, property which warrants legal protection using copyrights, patents, and trademarks (Oberholzer-Gee & Strumpf, 2010). ACM addresses intellectual property by proclaiming it is the computer professional's responsibility to properly cite the work of others, as well as to never take credit for someone else's intellectual property. IEEE approaches intellectual property slightly differently, and says its members are not to *misuse* or *infringe* upon the intellectual property that may belong to someone else.

Differences

While there are similar core principles that exist in the ACM and IEEE ethical codes of

conduct, the wording and structure of the codes vary greatly. For example, the ACM code of ethics contains twenty-four imperatives that dictate moral and ethical responsibility. In contrast, the IEEE code of ethics is much shorter, which lists five main rules. Also, though both codes of ethics are from technical societies, the ACM ethical standards are expressed in much greater detail, and provide extra principles and guidelines that computer professionals should follow. For example, the ACM code of ethics explains in detail what excellence should mean to a professional, whereas the IEEE does not mention excellence. The ACM code defines *harm*, and elaborates on how a professional should avoid harm, and what are considered acceptable actions in a work environment; IEEE does not cover harm. Conversely, the IEEE code of ethics does contain phrasing that does not appear in the ACM code. For instance, IEEE uses phrases such as *rejecting bribery* and *avoiding conflict of interest*; these phrases are not used in the ACM code. Additionally, IEEE addresses professional ethics as it pertains to economics—the code states IEEE members are obligated not to fix prices or negatively impact services, products, or consumer markets (Institute of Electrical and Electronics Engineers, 2014). Even though the IEEE and ACM codes do have similarities, the ACM code is more suitable for computer professionals. This has been determined based upon three distinct elements. One, ACM's targeted demographic is computer professionals. As such, many of the principles are center on computer use, ethical computer behavior, and computing professionals. Two, the rules and guidelines in the ACM code of ethics are in greater detail. Three, the ACM code has subsections which can be used by individuals filling specific roles. For instance, section three in the code pertains to those in a leadership role.

Adequacy

These *differences* between the codes of ethics raise an important question. Do these

codes adequately fulfil the needs of members and the general public? The answer to this question could be yes, or could be no, depending on the objective of each code ethics. In the ACM code of ethics, the membership demographic is mostly computer professionals. In the IEEE code of ethics, the specificity of membership is intentionally indiscriminate, which is meant to support numerous electronic and technology-based professions, not just computer professionals (as with ACM). Both codes are supposed to strengthen ethical behaviors, while at the same time maintain the privacy and integrity of data. Therefore, from a technical society point of view, each set of codes do indeed accomplish their primary objective—which is providing a list of rules and guidelines for their respective members to follow. Though, due to ACM being geared more towards computer professionals, and IEEE creating a code of conduct meant for a broader audience, the variances in the codes could be reduced, thus creating a more effective code of ethics. By decreasing the differences, and merging critically important clauses into one code, a unified code of ethics could be formed. Note, this is not to say these codes do not already possess a high level of ethical value, because they do. The ACM and IEEE ethical codes of conduct provide professionals with many of the principles and guidelines that encourage and support personal responsibility. Without these ethical standards, society would be negatively affected. However, as tremendous as the codes are, perhaps a combined code of ethics could be designed in a way that would support members and the general public even better. This segues into the next topic of unifying the codes.

Unified

If the needs of members and society are not being fully met—by any single code of ethics—a unified document could be created. This document would contain the *unification* of essential clauses, which upon compilation, would produce the best possible code of ethics.

Because the objective is to increase the ethical code's scope and range, there are a few important parts of each code of ethics that require further examination. First, due to the ACM code of ethics targeting computing professionals, much of the wording in the code is computer-centric. For example, in each section of the ACM code, the term *computing professional* is used (Association for Computing Machinery, 1992). It would be better, and increase the scope of the code, if *computing* was dropped, and only the word *professional* was used to describe a member. Remember, the aim is to design a more operational code of ethics, which will include all technology professionals. Next, in the IEEE code of ethics, the equal opportunity clause is perceived to be exceptional. IEEE extends the work equality clause to include gender, gender identity, appearance, and other equally important identifiers (Institute of Electrical and Electronics Engineers, 2014). Therefore, it is recommended that the equality clause be merged with the equality clause in the ACM code of ethics, which is not as comprehensive. Additionally, the IEEE code defines ethical economic principles, ones that compel members not to manipulate prices, services, or products that may negatively impact consumer markets. This clause should also be integrated into the ACM code of ethics. Note, it can be observed that the ACM code of ethics has been selected as the default code. The selection was made due to two reasons: (1) the ACM code already possesses many essential, highly detailed ethical principles; and, (2) the code of ethics only requires minor updates and modifications. A few important ACM clauses that highlight crucial ethical principles are sections: "(1.1) Contribute to society and human well-being; (2.7) Improve public understanding of computing and its consequences; and (2.8) Access computing and communication resources only when authorized to do so" (Association for Computing Machinery, 1992, para. 2). Consequently, it will be the ACM code of ethics that should be considered the universal code, once all changes and updates have been completed.

Part II – Workplace Privacy

When considering the modern workplace, it would be hard to imagine a company that had no forms of security in place. From the cameras in the parking lots, to the security officers that patrol the site, the businesses of today realize the importance of security. In an online world, employers are not only challenged to secure the physical assets of a business, but also its digital assets. This *digital* security requires the use of technology and information systems (Privacy Rights Clearinghouse, 2012). Whenever there are computers and technology involved, ethical concerns may arise. For example, is the security being implemented in an ethical way? Does the technology protect and secure data without violating a person's personal rights? Is the technology intrusive? These questions center on ethics, and are the subject of the case study used in this assessment. The study highlights three critical points, which warrant further examination. Point one, a CEO has determined there is a loss in productivity. Point two, the CEO believes this decrease in productivity is due to cell phone and Internet use. Point three, because of the loss in productivity, the company now uses key loggers, has access to all email, is looking into cellphone monitoring, and has installed cameras throughout the company for video surveillance. It will be aim of this research to address workplace privacy, and to provide a better approach to monitoring employees.

Workplace Privacy

In the presented case study, the CEO believes productivity is being negatively affected by technology, i.e. cellphones and the Internet. Consequently, there has been a security lockdown within the company. This raises an interesting question. Are employers required to provide their employees any level of privacy? In most cases, the answer is no, no they are not. According to the Privacy Rights Clearinghouse (1993), not only are employers allowed to install cameras to

monitor business sites, but employers also have the ability to scan emails, monitor telephone calls, and even track everything an employee does on a computer (Privacy Rights Clearinghouse, 1993). Hence, employees do not have privacy at work. Some of the lesser known, and perhaps unethical, security measures that employers can take, concern cellphones, personal email, and social media. For example, if the company provides a cellphone to an employee, the employer has every right to monitor its usage. There are even retail applications that an employer can use to read text messages, emails, contacts, and web surfing history (Komando, 2012). Likewise, if an employee is sending and receiving personal emails using the company's email system, the employer can scan and read these emails, without warning or notification. Furthermore, if employees think their social media websites such as Facebook and Myspace are private, the employee is wrong. Although, certain states do have laws that prohibit employers from disciplining employees based upon negative social media—for instance, New York, California, and Colorado—there are no laws that prevent companies from casually monitoring social networking sites (Privacy Rights Clearinghouse, 1993). Note, though some of these security actions may seem intrusive and illegal, in most instances, the employer's right to monitor employees is backed by legislation. As an example of employer rights, in the court cases *Smyth v. Pillsbury* and *Falmouth Firefighters Union v. Town of Falmouth*, the courts sided with a company's right to read email, even if that email was considered personal (Privacy Rights Clearinghouse, 1993). In another court case, *City of Ontario v. Quon*, a police officer's personal messages were [legally] searched on a government-issued device (Privacy Rights Clearinghouse, 1993). This means, if an employee is using property that belongs to an employer, whether it is a computer, telephone, cellphone, email, or any other form of electronic device, that property is subject to monitoring. In review of the research thus far, the use of key loggers, scanning email,

and video surveillance are well within the rights of the employer, however, there are ethical concerns with implementing these security measures.

Key Loggers. First, addressing the use of key loggers, it is understandable that the CEO wants to increase productivity. If employees are using work computers for their own personal entertainment—which is affecting the company's bottom-line—that is wrong. Key loggers would indeed record every key stroke at a workstation, thus allowing the employer to track an employee's every move (Grebennikov, 2007). However, the ethical issue of using key loggers is the loggers may record truly private information. For instance, what if the employee enters personal bank account numbers, passwords to personal sites, or private healthcare data? Although the company does have every right to monitor computers for general usage, the legal and ethical implications of using key loggers could quickly outweigh their practicality. Therefore, it is recommended that key loggers not be used.

Email Access. In respects to the company reading employee email, sifting through email is time consuming, intrusive, and does not actually resolve the productivity issue (Furber, 2012). Of course, the company has the right to read employee email. However, if and when confidential information is sent through the email system, what responsibility does the employer, or person viewing the information, have? Could the information in the email be used to hurt or harm the employee? These are ethical questions which could become a legal matter quite quickly. Thus, the direct viewing of email is not recommended.

Video Surveillance. Video surveillance can be an important part of maintaining security. Though, if used improperly, could easily be construed as unethical, or immoral. If the company places *visible* cameras in public areas, such as entryways, hallways, and office spaces, these zones would be considered appropriate for video surveillance (Privacy Rights

Clearinghouse, 1993). Conversely, if the company installs *hidden* cameras in bathrooms, break rooms, or office spaces, this would be considered unethical, and even possibly illegal. For instance, the *Electronic Monitoring in the Workplace: Common Law & Federal Statutory Protection* prohibits employers from installing hidden cameras in locker rooms and bathrooms (Privacy Rights Clearinghouse, 1993).

Recommendations

Monitoring employees at the workplace has ethical implications. Due to these implications, certain security measures should not be used. Key loggers and scanning email have been deemed inappropriate security methods for monitoring employees. Because video surveillance can be ethically implemented, it is suggested the company continues to use cameras, as long as they are visible and installed in non-private areas.

Websense. To monitor employee Internet and email usage—rather than using key loggers and manually reading email—it is recommended that *Websense* be installed. Websense is enterprise software which offers a plethora of security, monitoring, and reporting features (Websense, 2015). The Websense computer security software will be installed in the datacenter. From this centralized location, all computer workstation Internet activity can be monitored. The advantage of using Websense over key loggers, is that Websense does not violate personal privacy, meaning, it will not display the passwords, personal information, or other confidential data. However, the software will track *when* and *where* employees go online, how long certain webpages remain open, and how often the employee visits particular websites (Websense, 2015). This solution is far more robust than key loggers, and not only provides tracking capability, but also offers reporting and malware protection. Additionally, Websense can automatically scan emails for inappropriate keywords, non-professional content, and prevent emails from being sent

or received that meet specified criteria (Websense, 2015). Overall, the Websense enterprise software would best fit the needs of the company.

Phone Carrier Service. When it comes to monitoring the use of company-issued cellphones, the recommended approach is to work directly with telephone carrier service, and to place restrictions on cellphone usage (Sprint, 2014). For example, rather than having unlimited text, talk, and web access, the voice and data plans will be limited to 500 minutes. Because cellphone texting does not serve a business purpose, the texting feature will be disabled. Additionally, cellphone records will be randomly audited every month, to verify cellphones are being used for work-related tasks. Also, rather than reading the private contents of messages and viewing confidential information entered into websites on cellphones, only the email addresses and website location history will be tracked. This history will be provided to the company by the carrier service (Rose, n.d.). It is important to note, these security measures are not to be implemented in secrecy. Policies are to be created, and employees are to be educated and trained on the proper use of work cellphones, computer systems, and Internet access (Rose, n.d.). By implementing the recommended security solutions, the CEO's concern about productivity can be ethically and appropriately addressed.

Conclusion

Ethics are important. If a professional establishes a code of ethics, they will be more likely to act ethically, make the right decisions, and to protect the privacy and confidentiality of data. In the ACM code of ethics, the code is specifically geared towards computing professionals. In the IEEE code of ethics, a broader approach is taken to include electrical engineers, computer specialists, and technologists. Both of these codes provide core principles, that when followed, can bring integrity and professionalism to the field of information

technology. In the case study, where key loggers, reading email, and video surveillance are used to monitor employees, the application of professional ethics can be used to find more effective solutions. Rather than implementing key loggers to record key strokes, Websense would be more practical and ethical. In regards to monitoring cellphones, there is software to track phone usage, however, another option would be to just work with the phone carrier service. Ultimately, understanding how to apply ethical concepts to real-world problems is essential to a professional's career. Thus, if a professional wants to maintain a high level of integrity, establishing a code of ethics will encourage honesty, competence, and trustworthiness.

References

Association for Computing Machinery. (2015). ACM. Retrieved from http://www.acm.org/

Association for Computing Machinery. (1992). ACM code of ethics and professional conduct. Retrieved from http://www.acm.org/about/code-of-ethics

BLR. (2011, January 2). Why is ethical conduct important? Retrieved from http://hr.blr.com/HR-news/HR-Administration/Workplace-Ethics/Why-is-Ethical-Conduct-Important#

Ethics Resource Center. (2009, May 29). Why have a code of ethics? Retrieved from http://www.ethics.org/resource/why-have-code-conduct

Furber, Lesley. (2012, October 31). Workplace surveillance: Can your employer spy on you at work? Retrieved from http://www.crunch.co.uk/small-business-advice/2012/10/31/workplace-surveillance-can-your-employer-spy-on-you-at-work/

Grebennikov, Nikolay. (2007, March 29). Key loggers: How they work and how to detect them (part 1). Retrieved from https://securelist.com/analysis/36138/keyloggers-how-they-work-and-how-to-detect-them-part-1/

Institute of Electrical and Electronics Engineers. (2015). IEEE. Retrieved from http://www.ieee.org/

Institute of Electrical and Electronics Engineers. (2014). IEEE code of conduct. Retrieved from http://www.ieee.org/about/ieee_code_of_conduct.pdf

Komando, Kim. (2012, February 24). Can your employer monitor your smartphone? Retrieved from http://usatoday30.usatoday.com/tech/columnist/kimkomando/story/2012-02-24/work-monitor-smartphone/53221804/1

Oberholzer-Gee, F., & Strumpf, K. (2010, February). *File sharing and copyright*. National Bureau of Economic Research. Retrieved from http://www.nber.org/chapters/c11764.pdf

Privacy Rights Clearinghouse. (2012, October). Securing your computer to maintain privacy. Retrieved from https://www.privacyrights.org/securing-your-computer-maintain-your-privacy

Privacy Rights Clearinghouse. (1993, December). Workplace privacy and employee monitoring. Retrieved from https://www.privacyrights.org/workplace-privacy-and-employee-monitoring

Quinn, M.J. (2013). *Ethics for the Information Age*. Boston: Addison-Wesley.

Rose, Suzanne. (n.d.). How to monitor cell phone usage at the office. Retrieved from http://smallbusiness.chron.com/monitor-cell-phone-usage-office-46358.html

Sprint. (2014). Sprint Mobile Controls. Retrieved from https://mobilecontrols.sprint.com/welcome.htm

Websense. (2015). Websense products. Retrieved from http://www.websense.com/content/websense-products.aspx?intcmp=nav-mm-products