

Ethics in the Technology Driven Enterprise

Bobbie Green, James A. Nelson

Abstract—Innovations in technology have created new ethical challenges. Essential use of electronic communication in the workplace has escalated at an astronomical rate over the past decade. As such, legal and ethical dilemmas confronted by both the employer and the employee concerning managerial control and ownership of e-information have increased dramatically in the USA. From the employer's perspective, ownership and control of all information created for the workplace is an undeniable source of economic advantage and must be monitored zealously. From the perspective of the employee, individual rights, such as privacy, freedom of speech, and freedom from unreasonable search and seizure, continue to be stalwart legal guarantees that employers are not legally or ethically entitled to abridge in the workplace. These issues have been the source of great debate and the catalyst for legal reform. The fine line between ethical and legal has been complicated by emerging technologies. This manuscript will identify and discuss a number of specific legal and ethical issues raised by the dynamic electronic workplace and conclude with suggestions that employers should follow to respect the delicate balance between employees' legal rights to privacy and the employer's right to protect its knowledge systems and infrastructure.

Keywords—Information, ethics, legal, privacy

I. INTRODUCTION

THE digital revolution has led to new habits as employees and consumers, in an effort to control their destinies, determine where, when, and how they consume content and communicate with the world. In this fiscally uncertain, yet globally connected world, one thing is clear. Technology has been irrevocably changed the workplace.

Gordon Moore, one of the founders of Intel, defined "Moore's Law," which predicted the doubling of computing power every 18 months. This premise has proven to be true, thus, technology will continue to get smaller, faster, and more powerful. Yet, legal reform and ethical standards are slow to develop and often take years to implement. This further complicates matters. While technology is changing rapidly, legal reform and evolving ethical standards do not reflect technical innovation. Furthermore, the advantages afforded by technology also come with a hefty price tag for employers, namely the need to protect data, to manage productivity, and to avoid attacks from disgruntled employees, unscrupulous hackers, and cyber terrorists. As the technology has become more powerful, the ethical challenges have become more complex. This complexity stems from a proliferation of data; critical for decision-making, but risky due to the inherent exposure of the data to those who can potentially misuse it. Increasingly, the creation, storage, manipulation, and management of data introduces vulnerability. Add mobility to

this proliferation, and the result is a maze of networks and servers that can be accessed from any place and at any time. The risk of exposure to hackers, identity thieves, and cyber terrorists has become almost insurmountable. When valuable information falls into the wrong hands, the results can be catastrophic. This begs the question: How can data be leveraged to maximize shareholder investment yet at the same time protect against security breaches? Not only is there a real concern about unauthorized data access, most enterprises have an obligation to their stakeholders to protect their assets, which includes maximizing shareholder investment and securing technical resources. In addition, the convenience of technology in the workplace has introduced the potential for abuse of technical resources. Inappropriate use of workplace resources and violation of company policies can lead to a loss of productivity, employee termination, and expensive litigation. Employers must be diligent about establishing policies to protect their resources, and at the same time, employees' rights must be protected. The Fourth Amendment, which protects citizens from illegal search and seizure, now has unanticipated implications for work products such as email, web portals, and computer hard drives.

II. HISTORY

Most of the technologies that are commonly used today have evolved over the years. For example, the Internet, which is the ultimate network of networks, was established in the late 1960s through a Department of Defense research project. The Internet was initially designed so that military mainframe computers could share information and still be "platform independent." In the past 40 years, the Internet has evolved from simple host file resolved host names to Internet Protocol (IP) addresses into a hierarchy of domains and a conglomeration of worldwide Domain Name Servers (DNS) that resolve host names electronically via sophisticated software and servers. Since 1994, when the first graphical Internet browser was introduced, the "commercial" Internet has revolutionized the way business is conducted and simultaneously introduced opportunities for crippling viruses and web-based attacks. It is projected that the number of Internet users worldwide will be close to 2 billion in 2010. Intranets and extranets allow companies to conduct business electronically while simultaneously managing supply chains and purchasing goods and services via electronic data interchange (EDI). The same interconnectedness that has allowed electronic data interchange, e-commerce transactions, intranets and extranets has also exposed network vulnerabilities and costs billions of dollars in administrative and security overhead. Companies spend billions of dollars to protect customer data and prevent embarrassing and potentially bankrupting security breaches. Consumers and businesses also take advantage of the flexibility afforded by wireless connectivity. The first U.S. patent for a cell phone

Bobbie Green is with New Mexico State University, Las Cruces, NM 88003 US (e-mail: bobbie@nmsu.edu).

James A. Nelson is with New Mexico State University, Las Cruces, NM 88003 USA. (e-mail: jnelson@nmsu.edu).

was issued in 1908. Originally used for ship-to-shore communication during World War II, commercial use of cell phone technology began in 1946, [3] However, only since 1995 has wireless communication evolved into the low-cost, voice, data, and video capable hand-held personal digital assistants (PDAs) that are so common today. Wireless technologies have created unprecedented convenience, allowing any-place, any-time communication and access to information. The use of mobile devices has surpassed that of traditional computers. Market research indicates that an estimated 210 million people worldwide will own PDAs and "smart" cell phones by 2011. According to the Bureau of Labor and Statistics, wireless telecommunications carriers are among the top 25 fastest growing industries. Jobs with wireless telecommunications carriers, at approximately 195,900 jobs in 2002, will increase to 294,800 jobs by 2012.

III. CHALLENGES

Today's mobile workforce accesses an Internet that has morphed into an all encompassing global network connected by routers and wired or wireless technologies. This proliferation of wireless technologies has created a global work environment filled with telecommuters and mobile workers. This flexibility brings about a new set of ethical dilemmas. E-commerce, social networks, blogs, and a myriad of electronic water fountains have introduced new challenges for employers. Social networking websites such as FaceBook, MySpace, Twitter, LinkedIn, and YouTube have changed interactions with colleagues. Some would even suggest that online communication has replaced traditional conversation. Electronic banking and email have replaced visits to the brick-and-mortar banks and post offices. The same companies that were trying to migrate from "sneaker-net" to Ethernet in the mid-1980s are globally managing and protecting terabytes of information using the Internet, data warehouses, and wireless technologies today. These companies are also attempting to manage a global workforce, increase productivity, decrease costs, and protect assets all under the radar of ethics and jurisprudence. The convenience of doing business electronically has opened a Pandora's Box plagued with security breaches, viruses, worms, and a potential misuse of company resources. As a result, company policies have become virtually unenforceable and need to be rewritten to address the legal and ethical issues inherent with the Information Age. E-commerce websites that provide flexibility and convenience generate billions of dollars in revenue for commercial businesses, to the tune of an estimated \$133.6 billion in 2008, according to the U.S. Census Bureau. Some experts predict that business-to-consumer (B2C) transactions have the potential to exceed \$1 trillion and make up 25% of all sales in the United States by 2012. Behind the electronic shopping carts and transparent credit-card transaction validation, there is a back-end database. This database is filled with customer information that if breached can lead to electronic terrorism and virtual disaster. Powerful online transaction processing systems (OLTPs), i.e., databases are used for storing and retrieving information from e-commerce, banking, retail, government, military, and academic environments. Leveraging this gold mine of existing data from

an OLTP database to an Online Analytical Processing (OLAP) database has created a proliferation of data warehousing systems that have been implemented in most of today's successful companies. These sophisticated data warehouses are used for forecasting, trend analysis, and decision-making. Regardless of the enterprise, more than likely there are one or more databases for storing and retrieving information, thus turning these electronic gold mines into potential financially crippling security minefields. Technical innovations, which have been the mainstay of most successful businesses, have unleashed security snares that can lead to downtime, lost productivity, and public relations nightmares. According to the Computer Crime Research Center, "Cybercriminals are not only leveraging new technologies to propagate cybercrime but are also reinventing forms of social engineering to cleverly ensnare consumers and businesses." [8]. New methods are quietly being socially re-engineered to attack email service providers, banks, e-commerce websites, and voice-over-IP (VoIP) sites. Some of these attacks are so subtle that they often go unnoticed until the damage has been done. According to a recent article in USA Today, on a typical day, 40% of the 800 million computers are connected to the Internet. The damage that can be inflicted by an act of electronic terrorism can be transparent, cleverly disguised, and undetected until it's too late. Web bots are engaged in distributing spam, and stealing sensitive data targeting banking and shopping websites. These web bots are designed to extort, creating denial-of-service attacks, and spreading fresh infections", according to Rick Wesson, CEO of Support Intelligence [1]. Creative uses of these software and servers have created new challenges. Phishing scams and botnets are built by creating a network of infected PCs that receive orders from a server that is designated as the command-and-control server at the top of the hierarchy. A new technique, called fast flux, electronically changes the DNS record, thus changing the source IP address and ultimately migrating the phishing or spam host site, making it difficult to trace. This constant "flux" means the source cannot be located, making it extremely difficult to prevent such scams [5]. It is estimated that cybercrime became a \$105 billion market in 2008 and is climbing as cybercrimes become more complex [2]. A recent study by Ponemon Group [4] estimated that the loss of customer data can cost in excess of \$14 million per incident with direct costs such as attorneys' fees and the cost of notifying affected customers, plus indirect expenses such as lost productivity and opportunity costs.

IV. SECURITY PRACTICES

Even the most security-conscious organizations have found it challenging to prevent cyber crimes. Protection of an organization's assets and work products is a daunting task. Typical security practices such as firewalls, password protection, and anti-virus software do not eliminate security threats. A recent article [7] suggested keystroke loggers and insecure protocols, such as the commonly used hypertext transfer protocol (http), can be used to detect passwords. There are new tools on the horizon that promise added security. Among the most promising are biometrics: authentication based on physiological or behavioral characteristics such as

face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice recognition. Biometric-based solutions can increase data privacy and minimize the risks of security breaches. Enterprise wide network security infrastructures, government IDs, secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies. The executive branch of the United States government is using biometric screening to protect the nation against "known and suspected terrorists" (KSTs). A framework has been established to ensure that federal agencies are consistent with the methods and procedures in the collection, storage, use, analysis, and sharing of biometric data in a lawful and appropriate manner, while respecting their information privacy and other legal rights under U.S. law.

V. LEGAL ISSUES

Every day millions of Americans go to work and use a computer. These employees work at private and public workplaces. Some employees share work stations and share computers. Some are required to seek security clearance as a condition of their work. Some employees telecommute. The diversity of workplace arrangements between employees and employer is limited only by the business owner's propensity to creativity. The traditional 8 to 5, 40-hour work week is no longer the standard. Regardless of the working circumstances, employers must protect and control all work-related products, information, and innovations because these are a source of economic advantage. From the employers' perspective, any information created related to work must be protected. To achieve this goal, information must be scrutinized and monitored using the best and most efficient available technology. From the perspective of the employee, even in a workplace setting, the worker is entitled to individual rights such as privacy, freedom of speech, and freedom from unreasonable search and seizure. As the use of technology has accelerated, the e-information quandary with respect to ownership and control has escalated. The fine line between appropriate legal and ethical behavior has led to great debate and been the catalyst for proposed workplace reforms. The workplace in general has always been fraught with legal issues, raised by employers, employees, and independent contractors. The electronic workplace adds a new dimension to this debate. From the employer's point of view, most, if not all, e-information generated either in the workplace or as a result of work-related activity belongs to the business and should be monitored and protected. But at what cost can an employer monitor its workers? Do employees have privacy rights in the workplace? When is it legally permissible for an employer to "electronically snoop" on an employee? Does an employee have any expectation of privacy related to computer use? What about when the computer is shared? Is the workplace considered a public or private venue and does this matter legally? These are just a few of the many relevant legal dilemmas. From legal perspective, constitutional issues, federal and state statutes, numerous court decisions, and company policies legally impact this area. The following section sets out a brief overview of the legal tapestry in this area. It is worth noting that all of the legal inquiries turn on an

employee's expectation of privacy. In other words, if an employee acknowledges that he or she had no expectation of privacy, absent a Fourth Amendment violation, chances are there are no actionable legal issues raised when an employer monitors or checks employees' e-information. It is important for companies to have well-defined policies. Such policies should explicitly state that all company-owned computing assets and work products are subject to inspection at any time. These policies can reduce exposure to litigation and demonstrate the intent of an organization to be forthcoming, fair-minded, and objective. Organizations should prominently display warning banners on all computers to inform users that the organization reserves the right to inspect computer systems and network traffic [6]. It should also be explicit that any laptop or personal computer or device that connects to a corporate network is subject to the same restrictions and regulations as corporate property. A legal inquiry should begin with the U.S. Constitution. Technically speaking, there is no one specific provision in the Constitution that pertains to an employers' right to monitor workplace information or an employees' right to be free from this type of activity. The Constitution is a majestically vague document and sets out individual liberties in the first 10 amendments known as the Bill of Rights. Does an employee have a legal right to request that prior to searching through one's computer, the searching authority (employer) should have a warrant. The most relevant Constitutional right raised is found in the Fourth Amendment. However, constitutional protections extend only against actions by the government; in other words state action is required prior to one claiming constitutional violations. The vast majority of Americans work in the private sector, so the U.S. Constitution has no legal impact.

VI. CONCLUSION

Organizations should maintain an accurate inventory of computing systems, including hardware and software. Also, it is important to maintain communication with internal organizations, including management, human resources, and security departments to track reoccurring issues, complaints, and reported problems. Recent court decisions have defined computer misuse and employee harassment as contributors to a hostile work environment. The Internet and free, web-based email services such as Gmail, Hotmail, and Yahoo make it difficult for employers to provide a safe and secure environment for employees, providing anonymity for senders and creating an administrative burden for those who must identify email-based harassment in the workplace. Email used for inappropriate purposes can put an employer at risk. Network logs and proxy server logs can track the sender of inappropriate emails, but the overhead is expensive. The tradeoff is that litigation could prove to be even more expensive.

REFERENCES

- [1] B. Acohidio and J. Swartz, "Botnet Scams are Exploding," USA Today, http://www.usatoday.com/tech/news/computersecurity/2008-03-16-computer-botnets_N.htm, March 2008.
- [2] L. DMonte, "Virtual Nightmares Ride High," Computer Crime Research Center, <http://www.crime-research.org/articles/e-commerce08/>, January 2008.

- [3] T. Farley, "Mobile Telephone History," http://www.xtimeline.com/timeline/History-of-Mobile-Phones--Cell-Phones-_.March 2005.
- [4] M. Hall, "Price of Security Breaches," Computerworld, http://www.computerworld.com/securitytopics/security/story/0,10801,106180,00.html_.November 2005.
- [5] G. Knight, "Cybercrime is in a State of Flux," Computer Crime Research Center, http://www.crime-research.org/articles/cybercrime0308_.March 2008.
- [6] B. Nelson, A. Phillips, and C. Steuart, "Guide to Computer Forensics and Investigations," Course Technology, 2010.
- [7] J. Steward, "10 ways hackers breach security," Global Knowledge, http://images.globalknowledge.com/wwwimages/whitepaperpdf/WP_Steward_Hackers.pdf_.2007.
- [8] Trend Micro Inc., "Cybercriminals Reinvent Methods of Malicious Attacks," Computer Crime Research Center http://www.crime-research.org/analytics/3451/_.July 2008.