Mobile Computing and Commerce Legal Implications

Gundars Kaupins
Boise State University, USA

INTRODUCTION

This article summarizes the present and potential legal constraints of **mobile computing and commerce** and provides company policy suggestions associated with wireless data collection, dissemination, and storage. The legal constraints focus on major American **laws** that directly and indirectly involve mobile computing and commerce.

Mobile computing is the ability to use **wireless devices** such as laptops and handheld computers in remote locations to communicate through the Internet or a private network. The technology involves a computer linked to centrally located information or application software through battery powered, portable, and wireless devices (Webopedia.com, 2007b).

Mobile commerce uses computer networks to interface with wireless devices such as laptops, handheld computers, or **cell phones** to help buy goods and services. It is also known as mobile e-commerce, m-commerce, or mcommerce (Webopedia.com, 2007b). Radio frequency identification (RFID) technologies are often a part of mobile commerce. The technologies use radio waves to provide services such as identifying product packaging, paying tolls, purchasing at vending machines, and covertly **monitoring** employee locations (Grami & Schell, 2007).

This article is significant because mobile computing and commerce are expanding at a terrific pace. Laws have been slow to catch up with the new technologies. However, some existing laws on mobile computing and commerce already have a large impact on how communication is disseminated, security and privacy are maintained, and companies develop mobile policies. This article helps corporate managers reduce potential litigation because these mobile laws are described and their implications on company policies disseminated.

BACKGROUND

Companies incorporating mobile computing and commerce must balance the freedom of communication with legal constraints associated with **privacy,** fairness, **copyrights,** and **discrimination**. Technological and legal changes in the last 40 years have lead to a plethora of wireless devices and laws.

Wireless Device History

First generation (1G) systems that began in the early 1980s provided analog voice-only communications while second generation (2G) systems introduced in the early 1990s provided digital voice and low speed data services. Third generation (3G) systems introduced in the early 2000s focused on packet data rather than just voice (Grami & Schell, 2007).

Greater standardization has contributed to greater wireless computing and communication especially in Japan and Europe. The United States is catching up (Ackerman, Kempf, & Miki, 2003).

An example of greater standardization is Wi-Fi, an underlying technology for laptops associated with local area networks (LANs) based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 specifications. It was developed to be used for wireless devices, such as laptops for LANs, but it is now increasingly used for more services, including the Internet, television, DVD players, and digital cameras (Webopedia.com, 2007a).

With faster data transmission speeds and battery power boosts, employees are making wireless devices natural extensions of themselves with increased use of LANs, more location-based services, and wireless gadgets (Hirsh, 2002). Accordingly, working wirelessly allows employees to work almost anytime and anywhere. Information becomes more readily available in which employees can see and talk to each other, send

data and pictures, use the Internet, and conduct business with customers. Wireless devices such as cell phones allow the technology to be tailored to employees' needs. Companies can monitor employee electronic communications and check employee locations; in other words, do location monitoring (Philmiee, 2004).

Mobile Law History

The emergence of wireless devices has resulted in technical disputes and complex legal questions that have a direct impact on the growth of mobile communications. The highly specialized field of cyberlaw is developing to provide a balance between mobile freedom and legal constraints (Cyberlaws.net, 2007).

American laws limiting employer and employee communications have grown over the last 40 years. The Telecommunications Act of 1996, Civil Rights Act of 1964, U. S. Patriot Act, Occupational Safety and Health Act, Americans with Disabilities Act, Digital Millennium Copyright Act, Electronic Communications Privacy Act, and various federal and state criminal and civil laws constrain employer behavior associated with mobile computing and commerce. Court systems further interpret the laws as privacy, discrimination, copyright, and other lawsuits multiply.

European Union directives regulating wireless device use got off to a late start. However, the Directive on Privacy and Electronic Communications from 2002 established legal standards for privacy protection in personal data processing for all electronic communication devices. Japan's Ministry of Posts and Telecommunications issued "Guidelines on the Protection of Personal Data in Telecommunications in Business" that established a clear standard requiring consent for the use of personal information (Ackerman, Kempf, & Miki, 2003).

Various authors agree that increased legal constraints on mobile computing and commerce will occur. Left unconstrained, major potential abuses of mobile computing and commerce include:

1. Copyright violations (Benedict.com, 2007).
2. Discriminatory practices involving hiring, firing, promotions, and selection to training programs based on age, race, gender, color, national origin, religion, pregnancy, and other protected categories (Kaupins & Minch, 2006).
3. Privacy violations associated with location monitoring, e-mail monitoring, Internet use monitoring, and sharing confidential customer data (Kaupins & Minch, 2006).
4. Subscription fraud (also known as identity theft) similar to what credit card issuers experience when someone pretends to be another subscriber (Grami & Schell, 2007).
5. Device theft that leads to unauthorized charges incurred by the thief on the customers account (Grami & Schell, 2007).
6. Safety violations stemming from hand held cell phone use while driving (Insurance Institute for Highway Safety, 2007).

MOBLINE COMPUTING AND COMMERCE LAWS

This section focuses on major American laws directly and indirectly involving mobile computing and commerce. Court cases are mentioned only if they have a major impact on the laws. Application of these laws to corporate mobile computing and commerce policies follows.

- Occupational Safety and Health Act (OSHA). Employees often work at home with mobile computing by telecommuting. Though OSHA does not apply to an employee's house or furnishings, employers who must keep work-related injury records must include those that occur in the home or other work-related places. Work-related accidents outside of the business have been shown to be related to Workers' Compensation laws (Swink, 2001).
- Americans with Disabilities Act (ADA). Though ADA does not mention mobile computing and commerce, some courts have suggested that mobile telecommuting is a reasonable accommodation for disabled employees (Swink, 2001). Furthermore, ADA protects individuals who have cancer, autoimmune deficiency syndrome (AIDS), various mental illnesses, alcohol and drug problems (under treatment only), and loss of major life functions such as hearing and seeing. If an employer finds out through monitoring an employee's mobile communications that an employee has one or more of these conditions, the