Chapter 6
Perceptions of Students on Location-Based Privacy and Security with Mobile Computing Technology

John C. Molluzzo
Pace University, USA

James P. Lawler
Pace University, USA

Pascale Vandepeutte
University of Mons-Hainaut, Belgium

ABSTRACT

Mobile computing is a maturing technology with benefits for consumers. The purpose of this chapter is to furnish research on the perceptions of non-information systems students in both America and Europe on the impact of mobile computing devices on privacy and security. The chapter expands upon earlier research on only the perceptions of information systems students in America on mobile computing privacy and security. This research indicates a higher level of knowledge of the features of mobile computing, but lower levels of knowledge of inherent issues of mobile computing and consumer privacy and of precaution with mobile computing devices. Findings imply an inadequacy in general curriculum, and especially in data mining curriculum, but also an opportunity to improve the curricula. This research will benefit educators attempting to improve their pedagogy with syllabi summarized in the chapter that integrates contemporary issues of privacy and security with mobile computing technology.

INTRODUCTION

The authors of the chapter describe the benefits of mobile computing devices for both American and European consumers in the context of location-based services. They discuss the benefits of location-based services as constrained by the challenge of concerns of privacy and security with the devices. The data mining of information on consumers by business firms and by governments, as consumers interact

DOI: 10.4018/978-1-60566-906-9.ch006

and transact with location-based services on organizational and governmental applications on the devices, is a concern cited by the authors in this chapter, consistent with the theme of the Handbook.

The focus of the chapter is on the findings of the authors on perceptions of privacy and security of location-based services. The findings are from a survey of European and American students who were proxy for consumers of mobile computing. From the findings, the authors furnish a foundation for integrating location-based privacy and security into data mining and general curricula of schools for undergraduate and graduate students who are the current and future consumers of mobile computing, so that privacy and security might be perceived as critical facets of pervasive computing in society, a perception that might not be evident in the curricula pedagogy of schools.

The objectives of the chapter are to discuss the benefits and concerns of location-based services with mobile computing devices, the perceptions of privacy and security of the devices by proxy students, and the proposed solutions and trends with mobile computing devices and services that might be integrated into curricula of schools. The research in this chapter is important to the field, because curricula of schools might not be current with organizational and governmental practices of data mining that impact, if not intrude on, privacy and security of mobile computing technology. The research helps educators by informing them of the perceptions of non-information systems students who might not be as knowledgeable of privacy and security threats as information systems students.

The Appendix following the chapter will be especially helpful to instructors considering syllabi of privacy regulation and security of mobile computing technology.

BACKGROUND

Mobile computing applications on mobile computing devices (MCDs), such as cellular phones, laptops, personal digital assistants (PDAs), tablets, and other devices, are advancing in beneficial features for consumers. Browsing information and news, game playing, instant messaging, personal and professional e-mailing, and photo and text messaging are frequent features on the devices (M: Metrics Inc., 2006). These devices have advanced from basic cellular phones and PDAs to light computing devices interfaced to the Internet with information-rich and location-based or enabled services. Innovations in mobile computing have advanced from cellular payment systems to high speed networks in Europe, which is considered further along in the development of the devices than in America (Lundquist, March, 2007). Mobile computing with location-enabled services is considered by pundits as *the* killer application (Lundquist, April, 2007) and *the* technical trend of 2007 integral to consumers (Castells et al., 2007). Miniature mobile computing is contributing to a new period of pervasive computing (Denne, 2007).

Data mining involves searching and finding hidden patterns in large databases of mostly public data to generate profiles based on personal data and behavior patterns of citizens and consumers (Tavani, 2004). Data mining analysis methods evaluate the potential of current customer profiles in order to facilitate future customer prospecting and sales. Much of the data that is mined today is either public or semi-public – our supermarket purchases, surfing habits, salary, location, and other such information. The main ethical issues in data mining are that consumers are not generally aware their data is being gathered, do not know the uses to which the data will be made, or have not consented to the use of such data.

Presently, in the United States, there are limited legal restrictions on the use of personal data for data mining. Other than the protection of healthcare data under the 1996 Health Insurance Portability and Accountability Act (HIPPA), financial data under the 1999 Gram-Leach-Bliley Act, or the protection of children while on-line under the Children's Online Privacy Protection