ISSN: 1545-679X

Information Systems Education Journal

Volume 6, Number 32 http://isedj.org/6/32/ March 11, 2008

In this issue:

Integrating Issues of Location-based Privacy with Mobile Computing into International Information Systems Curricula

John C. Molluzzo
Pace University
New York, NY 10038 USA

James P. Lawler
Pace University
New York, NY 10038 USA

Abstract: Mobile computing continues to be an emerging technology with apparent benefits for citizens and consumers. As this technology expands in the marketplace and in society, concerns have developed about the control of personal information on mobile devices and about the perception of eventual frequent intrusion of privacy through location-based services. This paper describes exploratory research into the learning or non-learning of information systems students on the evolving impact and issues of mobile computing on privacy and security. Findings from a survey in a pilot stage of study of information systems students at Pace University indicate 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 a potential inadequacy in information systems curricula but also an opportunity to improve the curricula. This study will benefit information systems instructors attempting to improve their pedagogy with societal-sensitive syllabi that integrate contemporary issues of privacy and security with mobile computing.

Keywords: Information Systems curricula, location-based privacy, privacy, mobile computing, pervasive computing, Radio Frequency Identification devices, RFID

Recommended Citation: Molluzzo and Lawler (2008). Integrating Issues of Location-based Privacy with Mobile Computing into International Information Systems Curricula. *Information Systems Education Journal, 6* (32). http://isedj.org/6/32/. ISSN: 1545-679X. (Also appears in *The Proceedings of ISECON 2007:* §2512. ISSN: 1542-7382.)

This issue is on the Internet at **http://isedj.org/6/32/**

The **Information Systems Education Journal** (ISEDJ) is a peer-reviewed academic journal published by the Education Special Interest Group (EDSIG) of the Association of Information Technology Professionals (AITP, Chicago, Illinois). • ISSN: 1545-679X. • First issue: 8 Sep 2003. • Title: Information Systems Education Journal. Variants: IS Education Journal; ISEDJ. • Physical format: online. • Publishing frequency: irregular; as each article is approved, it is published immediately and constitutes a complete separate issue of the current volume. • Single issue price: free. • Subscription address: subscribe@isedj.org. • Subscription price: free. • Electronic access: http://isedj.org/ • Contact person: Don Colton (editor@isedj.org)

This paper was selected for inclusion in the journal as part of the ISECON 2007 best papers selection process. Papers in this category received preliminary reviews by three or more peer reviewers placing them in the top 30% of papers submitted.

EDSIG activities include the publication of ISEDJ, the organization and execution of the annual ISECON conference held each fall, the publication of the Journal of Information Systems Education (JISE), and the designation and honoring of an IS Educator of the Year. • The Foundation for Information Technology Education has been the key sponsor of ISECON over the years. • The Association for Information Technology Professionals (AITP) provides the corporate umbrella under which EDSIG operates.

Integrating Issues of Location-based Privacy with Mobile Computing into International Information Systems Curricula

John C. Molluzzo
jmolluzzo@pace.edu
Information Systems, Pace University
New York, NY 10038

James P. Lawler
jlawler@pace.edu
Information Systems, Pace University
New York, NY 10038

ABSTRACT

Mobile computing continues to be an emerging technology with apparent benefits for citizens and consumers. As this technology expands in the marketplace and in society, concerns have developed about the control of personal information on mobile devices and about the perception of eventual frequent intrusion of privacy through location-based services. This paper describes exploratory research into the learning or non-learning of information systems students on the evolving impact and issues of mobile computing on privacy and security. Findings from a survey in a pilot stage of study of information systems students at Pace University indicate 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 a potential inadequacy in information systems curricula but also an opportunity to improve the curricula. This study will benefit information systems instructors attempting to improve their pedagogy with societal-sensitive syllabi that integrate contemporary issues of privacy and security with mobile computing.

Keywords: Information Systems Curricula, location-based Privacy, mobile computing, pervasive computing, Radio Frequency Identification Devices, RFID

1. BACKGROUND

"*Data is moving into the wild*." – Richard Purcell, Corporate Privacy Group, 2006

Mobile computing applications on mobile computing devices (MCDs) such as cellular phones, consoles, flash drives, 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 (Shannon, M.M., 2007) of 2007. Miniature mobile computing is contributing to a new period of pervasive computing.

Location-based services on mobile computing devices continue to emerge in conven-

ient features for consumers in this period of pervasive computing. Features include automobile assistance and destination guides, 911 fire, hospital and police help, finders of friends, parents and teenagers, movie and restaurant locations, and traffic and weather reports. Further functions may include marketing of personalized products and services to customers from behavioral information already in data bases and from geographic information on the devices. The goal is marketing a perfect personalized pitch: specific service to a specific consumer who is likely to buy the service at a specific time (Holahan, p.94, 2007). Marketers may spend $19 billion on mobile marketing by 2011 (Holahan, p.97, 2007). Location is furnished 50 to 300 meters from the devices or from networks or systems linked to these devices that triangulate signals. Location-enabled services are furnishing popular and tangible utility (Minch, 2004).

Location-based services are facilitated by continuous developments in global positioning systems (GPS) and microchip radio frequency identification tags (RFID) or smart radio tags, that are integrated into mobile computing devices (Hamilton, 2007). Services are expanding onto the devices because of federal and state initiatives, such as in enhanced 911 (E911), driver licenses and passports (Songini, April 2, 2007). Industry initiatives in marketing products and services through GPS to customers, and in monitoring inventory of products and in shopping in stores through RFID, are further expanding location-enabled services (Arar, 2006). Industrial studies indicate mobile marketing to be accepted by customers if the marketing benefits them (Burt, 2007). Management of patient services, such as in hospitals, and marketing of personalized products and services to customers and consumers through RFID are likely to be features on MCDs by 2010. Improvements in the functionality of the keyboards and screens of MCDs, and in the longevity of the devices, are likely to increase the number of features on the devices for an increased number of consumers in our society.

The benefits of location-based services are coupled, however, by concerns about control of personal and private information on the mobile devices and by perception of frequent incidents on the devices of likely identity theft and intrusion on the privacy of consumers. Privacy activists, such as the Electronic Privacy Information Center and the European Commission, cite fundamental issues in the mismanagement and marketing of information on citizens and consumers. They cite issues in the monitoring of consumers by business and carrier firms and of citizens by governmental bodies from information retained from interactions or transactions (Eggen, 2006; Reding, 2007). RFID is not infrequently considered by consumers and pundits as synonymous with surveillance (Soat, p.44, 2006). Further issues include networks and systems behind the services that might be hacked by intruders, phishers, spammers and stalkers (Brandt, 2006) but not disclosed by firms when they learn of the hacking. Firms might lose mobile devices having information on customers because of internal loss or theft (Pratt, 2007). Firms might lose customers because of this (Romano and Fjermestad, 2007). Clearly the benefits of location-enabled services can be considered paltry when contrasted with issues on privacy and security (Stross, 2006).

The impact of the concerns on location-based services may eventually hinder the deployment of mobile computing in the marketplace and in society. Concerns of access of information or of location beyond the carrier, firm or government and beyond known collaborators in the absence of the knowledge of citizens and consumers are considerations in the design of location-enabled services. Consumers continue to have concerns about information interacted on the Internet (Sraeel, 2007). Consumers and citizens may not have confidence in the privacy and security of location services on their mobile computing devices or in regulation already considered by legislators to not include MCDs (Hines, 2007). The lack of confidence may impede pervasive computing as a trend (Tentori, Favela, Gonzalez and Rodriguez, p.1, 2005) if improved control of information and of privacy is not implemented in the field by information systems practitioners. Therefore, this paper introduces a framework for practitioners and instructors in information systems in integrating issues of location-related privacy with mobile computing, so that pervasive computing continues in society to be a bona fide trend.

2. INTRODUCTION

In this paper, privacy is defined as introduced in an earlier study of data mining and information ethics in information systems curricula (Lawler and Molluzzo, 2006): accessibility privacy, decisional privacy, and informational privacy (Tavani, 2004). Accessibility privacy is freedom from intrusion; decisional privacy is freedom from interference in personal choices; and informational privacy is freedom to limit access to and to control the flow of private information. Because the protection of the right to privacy is not explicit in the Constitution of the United States, legislation governs the federal government and the financial and health care industries in information and in rights to privacy, but generally not in other American industries. Consumers have to be dependent on privacy policies of other industries. Firms in these industries integrate the Code of Fair Information standards of the Organization for Economic Cooperation & Development in initiating informational privacy and security policies.

In Europe informational privacy is governed by European Directive 95/46/EC. Information has to be processed fairly and lawfully, collected for explicit and legitimate purposes and not further processed in a manner inconsistent with such purposes, not excessive in relation to the collected or processed purposes, current, and in a form that permits identity of consumers no longer than necessary. Though the Directive is more coherent, enforced and protective than legislation in America (Ackerman, Kempf and Miki, p.14, 2003), consumers in Europe as in America have to be conscious of and dependent inevitably on privacy and security practices in industries. Legislation in America and in the European Union governs information that is confidential, explicit and exchangeable between firms, but not information that is non-confidential, implicit and non-exchangeable, as in the data mining of derived information implicit in patterns of information in data bases of the firms if not governmental bodies (Lawler and Molluzzo, 2006). Such information may be private and sensitive to consumers and citizens. Location-based information and privacy in mobile computing and RFID with a telecommunications carrier or a wireless service provider extends this issue with the potential relinquishing of implicit, if not explicit, information in inherent systems (Ackerman, Kempf and Miki, p. 6, 2003).

Legislation controlling the use of location-based information has not been clearly defined and enforced in America, exacerbating issues of privacy. Federal legislation began with the Telecommunications Act of 1996 defining location-based information about a mobile consumer as *customer proprietary network information (CPNI) for completing calls for customers but not for marketing products and services to them*. Not clearly defined in this Act for the carrier or the provider was the form of opt-in or opt-out by customers for the products and services. Further confusing the issues were the 1998 Federal Communications Commission (FCC) CPNI decision on actual approval of opt-in by customers, the U.S. West (Qwest) challenge to the CPNI decision for flexible opt-out, the FCC clarification on CPNI not for opt-in, and the final 2002 FCC CPNI decision for notice and opt-out and for opt-in or opt-out (Ackerman, Kempf and Miki, p.10, 2003). The FCC Third Report and the Order and Third Further Notice of Proposed Rulemaking on CPNI, in reply to the Cellular Telephone and Internet Association to establish fair location-enabled information practices, continued the confusion as to opt-out or opt-in as *the* consent regulation (Ackerman, Kempf and Miki, p.7, 2003). Recently the FCC required marketers to have opt-out ("no" or "stop") for customers and mobile marketers to have express consent from customers in order to release information on them. However, enforcement of these regulations seems nebulous, as customers continue to be marketed services on the Internet, though they indicated opt-out on spam (Holahan, p.96, 2007).

Further legislation of location-based information and privacy includes the Wireless Communication and Public Safety Act (WCPSA) or E911 Act of 1999 for a future infrastructure with 911 as the natural emergency number. More legislation continues to be introduced in the Congress of the United States but with limited passage of regulation. Legislation is similarly introduced by states but with inconsistent protective regulations. Some states are keener than others in privacy regulation (Songini, April 9, 2007), so that legislation introduced by the

states is as confused or nebulous as legislation by the federal government. The FCC continues to be unclear in enforcement intent on location-based information and privacy standards.

In Europe, legislation includes the 1997 Telecommunications Privacy Directive that insures communication privacy of consumers and the 2002 Directive on Privacy and Electronic Communications that insures the privacy of cellular location information of the consumers (Ackerman, Kempf and Miki, pp.12-13, 2003). Article 9 of the 2002 Directive distinguishes between communication or traffic information and exact location information. This article insures that the processing of location information for further marketed services is enabled only if customers give opt-in consent and may be disabled, however temporarily, by such customers if they opt-out through a method that is not confusing and is simple to them (Ackerman, Kempf and Miki, p.13, 2003). Further legislative initiatives include future pan-European regulation of electronic communications and a permanent secretariat in Belgium (Reding and Viola, 2007). At the same time, though the 1997 Directive and the 1995 Data Protection Directive indicated that traffic information be deleted following billing cycles of the customers, in order to protect privacy, the 2002 Directive caused confusion by exempting telecommunication carriers and wireless providers. In fact, European governments initiated legislation in 2007 to not delete but to collect this information and also location information, in order to fight terrorism (Shannon, V., 2007). As in America, this introduces issues in a privacy sensitive society in which RFID is largely not regulated by the European Union (O'Brien, 2007) but may be regulated by governmental legislatures.

Appendices A and B display the landscape of domestic and international legislation on privacy as of 2006.

The impact of this confusion and enforcement in European and especially American legislation is that telecommunication carriers and wireless providers may be inconsistent in policies on location-based privacy. Incidents of identity theft, intrusion, phishing, spamming and stalking may be more likely because of inconsistent security. Mobile computing, if not pervasive computing, may be inhibited if consumers are not protected in the privacy and security of their information, movements, and of services to them, because of inconsistent and nebulous legislation and industrial standards. These circumstances may challenge information systems practitioners in including location-enabled privacy and security in the design of mobile computing systems. Instructors in information systems may be challenged in educating students if these issues are not integrated into current curricula design.

Instructors may be challenged further in location-based privacy and security in the context of mobile computing, as context is not clearly defined in the literature and is complex in the metaphor of pervasive computing. In informational privacy, a consumer controls his information. For example, if the consumer is a doctor and the information is location information, he/she may decide to share exact information about his/her specific location with other doctors, inexact information about his/her generic location with hospital nurses and other inexact generic information about his/her generic location with outpatients (Tentori, Favela, Gonzalez and Rodriguez, p.3, 2005). The doctor must make these decisions based on considerations of circumstantial context. The considerations of context depend upon multiple computationally diverse factors for a consumer of mobile computing devices that are inherently personal and private to this consumer. Such context depends upon the design of an elaborate infrastructure (Aho, Hopcroft and Ullman, 1983) distinct from the historic infrastructure of systems for mere informational privacy (Dwyer, p.8, 2007). Literature indicates that designing information systems for informational privacy is inconsistent with the demands of designing systems for pervasive computing that accommodate location-enabled privacy (Ackerman, 2000).

Information systems practitioners and instructors of information systems students may be challenged by the complexity of location-based information and privacy. Design of an infrastructure of a system for context may consist of extensive evaluation of the flexibility of the system needed for privacy *as perceived by consumers* (Tentori, Favela, Gonzalez and Rodriguez, p.2, 2005). Inference of information triggered by initial

information, such as a husband inferring that a wife is buying clothing based on her location in a shop (Dwyer, p.6, 2007), may necessitate further evaluation of levels of privacy, in order to regulate the systems (Tentori, Favela, Gonzalez and Rodriguez, p.2, 2005). Information systems practitioners may have to develop increased controls and templates (Dwyer, Hiltz and Jones, 2006) to safeguard location-enabled privacy in such systems. These practitioners, instructors of information systems students, and students themselves may have to learn a methodology to implement a new legal, political, societal and technical design of location-enabled privacy and security systems, in order to be responsive and sensitive to the marketplace and society.

This study thus attempts to explore the knowledge of information systems students in the evolving global impact of mobile computing on location-based privacy, in order to discern not only existence of a new methodology in the curricula but also the sensitivity of the students and the instructors to the marketplace and to society. Though privacy threats in the technology continue to be documented in the practitioner (Soat, 2006) and scholarly (Lee and Kim, 2006) literature, privacy is not infrequently considered cavalierly by carriers, firms and providers in industry (Soat, p.38, 2006). Practitioners in information systems may not know the impact of issues of location-based privacy in the metaphor of pervasive computing. They may not know inference issues, legislative and regulatory issues, nor regulations. They may not know optimal paths to solutions through a synthesis of standards, such as those of the Center for Democracy & Technology (CDT), the Electronic Frontier Foundation (EFF), the Electronic Privacy Information Center (EPIC), the Internet Engineering Task Force (IETF) and the Platform for Privacy Preferences Project (P3P) and also of the European Commission Safeguards in a World of Ambient Intelligence (SWAMI) Project, the European Regulators Group (ERG) and Privacy International. This lack of knowledge, or the likelihood of it, necessitates further learning not only by these practitioners but by students who will be the future of the field, as learning in schools of information systems is frequently focused on issues and solutions that are not societal but stovepipe technical.

To be sensitive to location-enabled privacy in our pervasive computing society, schools of computer science and information systems in America and Europe have to encourage instructors to evaluate if not enhance curricula for students and programs for practitioners in the learning of mobile computing, privacy and security

3. FOCUS OF STUDY

The focus of this study is to explore the knowledge of undergraduate and graduate students of the impact of mobile computing on location-based privacy. Exploration of this knowledge enables input into the learning or non-learning of these students on privacy and regulation in their curricula, expanding the earlier study of data mining and information ethics in information systems curricula (Lawler and Molluzzo, 2006), field studies (Cvrcek, Kumpost, Matyas and Danezis, 2006; Hakkila and Chatfield, 2005) and other international studies of the Economic & Social Research Council (ESRC) e-Society (www.york.ac.uk/res/e-society). Insight from this input may facilitate improved design of mobile computing systems for management of privacy in governmental and marketplace settings. Such settings may further inform issues of perceived privacy threats (Palen and Dourish, 2003). The goal of the final study is to furnish a framework for information systems instructors in integrating issues of location-based privacy with mobile computing into societal-sensitive syllabi for students who will be the future of information systems technology. This framework will be timely as few studies have focused on the implementation and the issues of location-related services in a pedagogical manner.

4. RESEARCH METHODOLOGY

The Mobile Privacy Survey was administered online using Zoomerang during the last two weeks of April and the first two weeks of May, 2007. Because of the survey's length, it was administered online. It would have taken too much class time to ask faculty to administer it during classes. An email containing the link to the survey was sent to approximately 1500 (500 undergraduate and 1000 graduate) students attending the Seidenberg School of Computer Science and Information Systems. The Seidenberg

School has undergraduate and graduate programs through the Doctor of Professional Studies in Computing. Within the School there are programs in Computer Science, Information Systems, Technology Systems, Telecommunications, Internet Technology, and Software Development and Engineering. Thus, the survey was limited to students studying some aspect of computing. There were 77 completed surveys, representing an approximate 5.1% completion rate. The survey instructions asked the respondents to limit their responses to their experience using mobile computing devices (MCD), excluding dedicated audio devices, such as the iPod. The survey was administered anonymously – the respondents' names were not collected.

The survey was divided into several sections: Background questions to gather some demographic data; Objective questions on the importance of using mobile devices for various purposes; Knowledge questions on respondent awareness of the privacy issues of location-based data collection; Concern and Control questions about the protection of consumer privacy by government and wireless providers; and a Summary question to gauge the respondents' overall concern for privacy.

5. ANALYSIS OF FINDINGS

Background

Most respondents (77%) were graduate students, with the remaining 23% undergraduate students; 64% were male and 36% female. Three mobile device types were identified by the respondents: Laptops (26), Cellular phones (31), and PDAs (18). 69% of respondents used their mobile device 4 hours or less per day; 20% between 5 and 8 hours per day; and 11% used their device nine or more hours per day.

Objective Questions

Objective questions were asked regarding the respondents use of MCDs.

Importance: Respondents were asked to "rate the importance of your objective in having a mobile device." The answers were based on a five-point Likert scale. The most important rated uses were Emergency, Search, Business, and Social Contacts. Although the use of mobile devices for streaming media is constantly in the news, the respondents rated that use fairly low with only 32% believing media is Important or Very Important. However, this could be the result of the high number of graduate students (average age of 34) responding to the survey. Table 1 in Appendix C summarizes the results. Each entry in the table is a percent of those answering the question. Note that tables not shown in Appendix C are available from the authors by request.

Frequency of Use: Respondents were asked to "rate how frequently you use your mobile computing device for each service" listed. The most frequently used services were Search, News, Business, and Weather. Some social and entertainment categories were rated very low, such as Games, Health, Religion, and Politics.

Use of Location-Enabled features of MCD: Respondents were asked to "rate the frequency with which you use the location-enabled features of your mobile computing device." The answers were based on a five-point Likert scale. The most frequently used features were Destination Guides, Theater Locations, Restaurant Locations, and Driving Directions. Although 86% of the respondents reported that having a mobile device for emergencies was Important or Very Important (see the previous discussion on Importance), only 7% of respondents frequently used the 911 feature of their devices. This emphasizes the value placed on the emergency use of mobile devices by consumers.

MCD Feature Access: Respondents were asked to "rate the frequency with which you access the following specific features of your mobile computing device." The answers were based on a five-point Likert scale. The most frequently used feature of respondents' MCD is communication: 59% use their MCD Frequently or Very Frequently for email, 30% for Text Messaging, and 25% for Instant Messaging. It is also noteworthy that only 24% use their device Frequently or Very Frequently for E-Commerce Products. This could be an indication that the e-Commerce sector has not yet impacted the mobile computing market as much as it would like.

Communication: Respondents were asked to "rate the frequency with which you communicate with those indicated." The answers

were based on a five-point Likert scale. Again, answers here indicate the main use is personal communication with Friends (72%), Family (64%), and Personal (59%) rated as Frequent or Very Frequent.

Private Information: Respondents were asked "What private information do you store on your mobile computing device(s)?" A list of possible data was presented. Although some personal information is inevitably stored on a MCD, it is interesting to note that some respondents save highly confidential data on their MCD. For example, two people (out of 77) store their Social Security Numbers, four people store unencrypted account passwords, five people store credit card numbers, and seven store bank account numbers.

Knowledge Questions

Privacy: The respondents were asked several questions that rate their knowledge about various privacy concerns using MCDs. The answers were based on a five-point Likert scale. Because the respondents were computing majors and had been trained in some of the technologies and their consequences, it makes sense that they overwhelmingly Agree or Strongly Agree with every statement. Table 2 in Appendix C summarizes the results. The numbers again represent percents.

Wireless Provider Policies: The respondents were asked several questions on their relationship with their wireless provider. These were Yes-No questions. The respondents' answers here are puzzling in light of the Privacy questions, which indicate a high degree of awareness of important privacy issues when using MCDs. However, this set of questions indicates a high degree of complacency and lack of knowledge among the respondents regarding the actual privacy policies of their mobile carriers. For example, 72% do not read their carrier's privacy policy; 68% do not even read their mobile contract before signing it. A partial explanation could be that a great number of the respondents (86%) never had their personal information compromised. The results are in Table 3 in Appendix C, where numbers represent percents.

Concern and Control Questions

Trust and Advertising: The respondents were asked to "rate their level of agreement with the given statement." The answers were based on a five-point Likert scale. Respondents show mistrust that their provider (35% Agree or Completely Agree) or the government (26% Agree or Completely Agree)) will protect their privacy. A very high percentage, 91%, either Agree or Completely Agree they are concerned about identity theft. Interestingly, however, only 34% Agree or Completely Agree that they are concerned about location-based privacy. It seems the respondents do not yet consider location-based data to be personal information.

Mobile service providers should note that 79% of respondents either Agree or Completely Agree that their confidence in their provider would lower if there were a security breach. In addition, 68% of respondents Agreed or Completely Agreed that they would terminate their contract in the event of a security breach.

Mobile advertising did not get a strong vote of confidence from the respondents. 93% of the respondents either Strongly Disagree or Disagree that they would like mobile advertising messages. Also, 90% Strongly Disagree or Disagree that they would like a mobile advertising alert when near a product. Even if the advertising were targeted and personalized, 69% of the respondents Strongly Disagree or Disagree. Table 4 in Appendix C summarizes the results. Each entry is a percent of those answering the question.

Protecting Your Mobile Device: The respondents were asked how they protect their mobile device? They were provided with a list and were asked to check all that apply. Not many respondents encrypt data on their MCD. Only 33% encrypt all data, 29% encrypt all business-related data, and 43% encrypt all sensitive data. Also, only 56% use encryption when connected to a wireless network. However, 65% lock access to their MCD using a strong password and 61% set the MCD to auto-lock when not in use for a specified time. Many respondents, 64%, keep their MCD hidden when traveling, but only 47% do not access private or business data in public places. Finally, only 54% of

respondents remove all data on their MCD before discarding or turning it in. Again some of these responses show a disconnect between the respondents' level of awareness of privacy issues and their actual privacy-preserving practices.

Summary Question: Respondents were asked "which of the following statements best describes your feelings about privacy?"

- I feel strongly about privacy. (61%)
- I feel strongly about privacy but may benefit from surrendering my privacy at times if my privacy is not abused by a firm or service. (36%)
- I do not feel strongly about privacy. (4%)

These questions are based on Alan Westin's categorization of people into *privacy fundamentalists* (first question), *privacy pragmatists* (second question), and *privacy unconcerned* (third question.) In a Harris poll conducted in 2003 (Taylor, 2003), the percentages of respondents in the three categories were 26%, 64%, 10%. This is a considerably different distribution from our results – 61%, 36%, 4%. However, our population (computer majors) is more informed about privacy issues than the general population.

Statistical Analysis

So far, with one exception which is discussed below, no significant statistical results have been found from the pilot study. It is believed this is the result of either the relatively small sample size (n = 77) or the fact that the respondents are well-educated in the area of security. The only exception is in the difference between male and female respondents in the number of hours they use their mobile devices. Tables 5 and 6 show the crosstabs and Chi-Square results. Note that that $p < .001$.

It is hoped that with the cooperation of several more universities, the study can be extended to a larger sample size. In addition, a shorter version of this survey will be administered to first and second year students at Pace University who are taking the university-core introductory computing course. Part of that course is the study of computer and online security. The amended survey will study that group relative to questions of mobile privacy.

6. FRAMEWORK OF SYLLABI

The findings of the pilot study indicate the implied importance of a framework of syllabi to be considered for location-based privacy and security with mobile computing in the curricula of schools of information systems.

This framework could be designed in modules consisting of architecture and applications of mobile computing, design and development of mobile computing applications, privacy of mobile computing applications, security of mobile computing architecture and applications, and mobile computing societal and technological trends. The modules on architecture and applications, design and development of mobile computing applications, and mobile computing societal and technological trends are generally in a syllabus on mobile computing that is focused on pure technology. The module on privacy of mobile computing applications, consisting of citizen and consumer constructs, and ethical, governmental, methodological, and technological constructs, is generally in a syllabus on mobile computing that is focused on society and technology. The module on security of mobile computing architecture and applications, consisting of information protection and security, security protocols and security techniques, is generally in a syllabus that is focused on security of technology. This study indicates that a framework that could be designed to develop the modules into a *syllabus* may contribute to improved learning of location-enabled privacy and security with mobile computing technology.

This framework may be the foundation for a fuller program of study that integrates the modules into *syllabi* that may contribute to further learning for information systems students and might facilitate certification of the schools as centers of excellence in information assurance of mobile computing technology by the National Security Agency.

The framework of the syllabi is furnished in outline in Appendix D.

7. IMPLICATIONS OF INITIAL STUDY

An initial implication of the findings of the study is the students' clear knowledge of the fundamental functionality of mobile computing devices. The information systems students were knowledgeable in the *processes* of mobile computing firms. This knowledge

was, however, indicated to be not as clear and to be lower in the probable privacy and security *practices* of the firms. The students were not as diligent in inherent issues with business and marketing practices with mobile computing technology as they were with the processes of the technology. These findings imply a likely lower sensitivity to the larger impact of mobile computing technology on society.

Another implication of the study is an inconsistency in the higher knowledge of the students in the processes of location-based mobile computing technology in contrast to lower personal *precaution* with the technology. The students were not as diligent as expected in the confidentiality and protection of information on mobile computing devices, which is not distinct from the inconsistency of non-student subjects in follow-up of intrusions of privacy (Sraeel, May, 2007). Though they felt the generic importance of privacy, the students were not fully protective of their devices through recognized security techniques. This lower diligence in precaution was not an encouraging example for the management of the privacy and security of mobile computing technology. The findings imply a lower sensitivity to the non-technological impact of mobile computing as a societal tool, a theme that continues in the study.

Other implications of the initial study include the potential opportunity to improve the mobile computing syllabi of information systems instructors, in order to mitigate deficiencies in knowledge. The students may learn more of the impact of marketing and business practices that mobile computing firms and retailers might apply from innovations in mobile computing technologies (Haskin, 2007), if schools improved their information systems syllabi. Information systems students may also learn more of privacy and security issues and techniques with mobile technology (Taylor, 2007). Moreover, they may be encouraged as future practitioners and professionals by their instructors to be more sensitive to regulatory and societal themes. These findings of the preliminary study imply minimally that an improvement is needed in mobile computing and information systems syllabi, and a framework for improvement of the syllabi is modeled in Appendix D of this study.

8. LIMITATIONS AND OPPORTUNITIES FOR RESEARCH

An initial implication of the findings of the study is the students' clear knowledge of the fundamental functionality of mobile computing devices. The information systems students were knowledgeable in the *processes* of mobile computing firms. This knowledge was, however, indicated to be not as clear and to be lower in the probable privacy and security *practices* of the firms. The students were not as diligent in inherent issues with business and marketing practices with mobile computing technology as they were with the processes of the technology. These findings imply a likely lower sensitivity to the larger impact of mobile computing technology on society.

Another implication of the study is an inconsistency in the higher knowledge of the students in the processes of location-based mobile computing technology in contrast to lower personal *precaution* with the technology. The students were not as diligent as expected in the conAnother implication of the study is an inconsistency in the higher knowledge of the students in the processes of location-based mobile computing technology in contrast to lower personal *precaution* with the technology. The students were not as diligent as expected in the confidentiality and protection of information on mobile computing devices, which is not distinct from the inconsistency of non-student subjects in follow-up of intrusions of privacy (Sraeel, May, 2007). Though they felt the generic importance of privacy, the students were not fully protective of their devices through recognized security techniques. This lower diligence in precaution was not an encouraging example for the management of the privacy and security of mobile computing technology. The findings imply a lower sensitivity to the non-technological impact of mobile computing as a societal tool, a theme that continues in the study.

Other implications of the initial study include the potential opportunity to improve the mobile computing syllabi of information systems instructors, in order to mitigate deficiencies in knowledge. The students may learn more of the impact of marketing and business practices that mobile computing firms and retailers might apply from innovations in mobile computing technologies

(Haskin, 2007), if schools improved their information systems syllabi. Information systems students may also learn more of privacy and security issues and techniques with mobile technology (Taylor, 2007). Moreover, they may be encouraged as future practitioners and professionals by their instructors to be more sensitive to regulatory and societal themes. These findings of the preliminary study imply minimally that an improvement is needed in mobile computing and information systems syllabi, and a framework for improvement of the syllabi is modeled in Appendix D of this study.

9. CONCLUSION

The research of this study explored the learning and non-learning of information systems students on location-based privacy with mobile computing. Findings in a preliminary stage of the study of the student subjects at Pace University indicated the higher level of knowledge of the functions of mobile computing devices, but the lower levels of knowledge and learning of issues of location-enabled privacy and of security with the devices. Findings indicated the implied importance of improving information systems curricula in the schools of computer science and information systems by integrating societal sensitive syllabi. Further research in a final stage of study will include an increased number of instructors and student subjects at Pace University and at the University of Mons-Hainaut in Belgium in 2008 that will solidify the findings of this study. The authors of this study welcome other universities that might be included in the survey of information systems students on location-based services with mobile computing.

10. ACKNOWLEDGEMENTS

The authors acknowledge Alina Joshi, a graduate student in the Seidenberg School of Computer Science and Information Systems, who helped develop and implement the survey instrument in this study.

11. REFERENCES

Ackerman, L., Kempf, J. and Miki, T. (2003) "Wireless Location Privacy: A Report on Law and Policy in the United States, the European Union, and Japan," DoCoMo USA Labs, October 28, 6,7,10,12,13,14.

Ackerman, M. (2000) "The Intellectual Challenge of CSCW: The Gap between Social Requirements and Technical Feasibility," Human-Computer Interaction, 15(2/3), 179-203.

Aho, A.V., Hopcroft, J.E. and Ullman, J.D. (1983) Data Structures and Algorithms, Addison-Wesley Longman Publishing Company, Boston, Massachusetts.

Arar, Y. (2006) "Consumer Watch: Is That a Sales Pitch in Your Pocket?," PC World, November 20, 1-3.

Blau, J. (2007) "Europe's Mobile Advances: From Mobile VoIP to Cell Phone TV, Europeans Are Pushing Wireless Features and Functionality," Computerworld, May 14, 36.

Brandt, A. (2006) "Privacy Watch: Phishers Put Their Lures on Cell Phones," PC World, November 20, 1-2.

Burt, J. (2007) "Study: Time Is Right for Mobile Marketing," eWeek, January 15, 33.

Cvrcek, D., Kumpost, M., Matyas, V. and Danezis, G. (2006) "A Study on the Value of Location Privacy," Proceedings of WPES'06, Alexandria, Virginia, October 30, 109-118.

Dwyer, C. (2007) "The Inference Problem and Pervasive Computing," The Ivan G. Seidenberg School of Computer Science and Information Systems, Pace University, 6,8.

Dwyer, C., Hiltz, S.R. and Jones, Q. (2006) "Discovering Boundaries for Mobile Awareness: An Analysis of Relevant Design Factors," Proceedings of the Twelfth Americas Conference on Information Systems, Acapulco, Mexico, August 4-6, 7.

Eggen, D. (2006) "Justice Department Database Stirs Privacy Fears," Washington Post, December 26, 2-3.

Government Technology (2007) "Europe and United States (U.S.) Mobile Use Compared," Government Technology, May 27, 1.

Hakkila, J. and Chatfield, C. (2005) "It Is Like If You Opened Someone Else's Letter – User Perceived Privacy and Social Practices with Short Message Service (SMS) Communication," Proceedings of Mobile-

HCI'05, Salzburg, Austria, September 19-22, 219-222.

Hamilton, A. (2007) "Wireless Street Fight: Web 2.0 Moves into Your Neighborhood as Firms Vie to Deliver Local Content to Your Cell Phone," Time, February 26, 48.

Haskin, D. (2007) "Fast and Furious: What Does Your Wireless Future Hold? Blistering Speeds and More-Sophisticated Networks, Thanks to Advances in Mobile Broadband," Computerworld, May 14, 44,46.

Hines, M. (2007) "Black Hat Exposes RFID Security Risk," Infoworld, March 5, 9-10.

Holahan, C. (2007) "The Sell-Phone Revolution: Stay Tuned for a Message from Your Cell Phone, Which Seems to Know an Awful Lot About You," Business Week, April 23, 94-97.

Lawler, J. and Molluzzo, J. (2006) "A Study of Data Mining and Information Ethics in Information Systems Curricula," Information Systems Education Journal, 4(34), 3-14.

Lee, H. and Kim, J. (2006) "Privacy Threats and Issues in Mobile RFID," Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06), IEEE Computer Society, 1-5.

Lundquist, E. (2007) "The Next Killer Application?: It Will Be in the Mobile Segment, if CTIA Is Any Indication," eWeek, April 2/9, 6.

Lundquist, E. (2007) "The View from Europe: United States Lags in Some Areas, But Hiring Woes Are Similar," eWeek, March 19, 9.

Minch, R.P. (2004) "Privacy Issues in Location-Aware Mobile Devices," Proceedings of the 37th Hawaii International Conference on System Sciences," IEEE, 1.

M: Metrics Inc. (2006) "United States Mobile Subscriber: Monthly Consumption of Content and Applications," M:Metrics Inc., Benchmark Survey, April, 16.

O'Brien, K.J. (2007) "European Union Will Not Regulate Radio Tags, Despite Concerns on Privacy," International Herald Tribune, March 16, 11.

Palen, L. and Dourish, P. (2003) "Unpacking 'Privacy' for a Networked World," Proceedings of CHI 2003, 5(1), Ft. Lauderdale, Florida, April 5-10, 129.

Pratt, M.K. (2007) "Your Gadgets Are Springing Leaks: Handheld Electronics Travel Everywhere in Your Company, Spilling Data Along the Way," Computerworld, March 19, 34-36.

Reding, V. (2007) "European Policy Strategy Proposed for RFID," Government Technology, March 15, 1.

Reding, V. and Viola, R. (2007) "European Union Moves Forward on Regulation of Electronic Communications," Government Technology, February 28, 1.

Romano, N.C., Jr. and Fjermestad, J. (2007) "Privacy and Security in the Age of Electronic Customer Relationship Management," International Journal of Information Security and Privacy, 1(1), 103.

Shannon, M.M. (2007) "Shannon's Eleven: Top Technical Trends to Watch in 2007," Communications of the ACM," 50(1), 19-20.

Shannon, V. (2007) "Europe's Plan to Track Phone and Net Use," The New York Times, World Business Section, February 20, 1.

Soat, J. (2006) "The Problem That Will Not Go Away: Your Privacy Mistakes Are Now Everybody's Business," Information Week, November 20, 34-44.

Songini, M.L. (2007) "California Lawmakers to Vote on Five Bills to Regulate RFID Technology," Computerworld, April 9, 20.

Songini, M.L. (2007) "Washington State and Department of Homeland Security (DHS) May Use RFID in Licenses," Computerworld, April 2, 6.

Sraeel, H. (2007) "Protecting Data On-Line Is a Top Priority for Consumer," Bank Technology News, April, 8.

Sraeel, H. (2007) "In the United States, Privacy Is Not Always Convenient or Wanted," Bank Technology News, May, 8.

Stross, R. (2006), "Cellphone as Tracker: X Marks Your Doubts," The New York Times, Business Section, Sunday, November 19, 3.

Tavani, H.T. (2004), Ethics and Technology: Ethical Issues in an Age of Information and

Communication Technology, John Wiley and Sons, Hoboken, New Jersey, 92,121,124,140,144,146.

Taylor, C. (2007), "As RFID Tracking Booms, Privacy Issues Loom," Business 2.0, May 11, 1-3.

Taylor, C. (2007), "Europe's Digital Revolution Speeds Up," Government Technology: Digital Communities, April 27, 1.

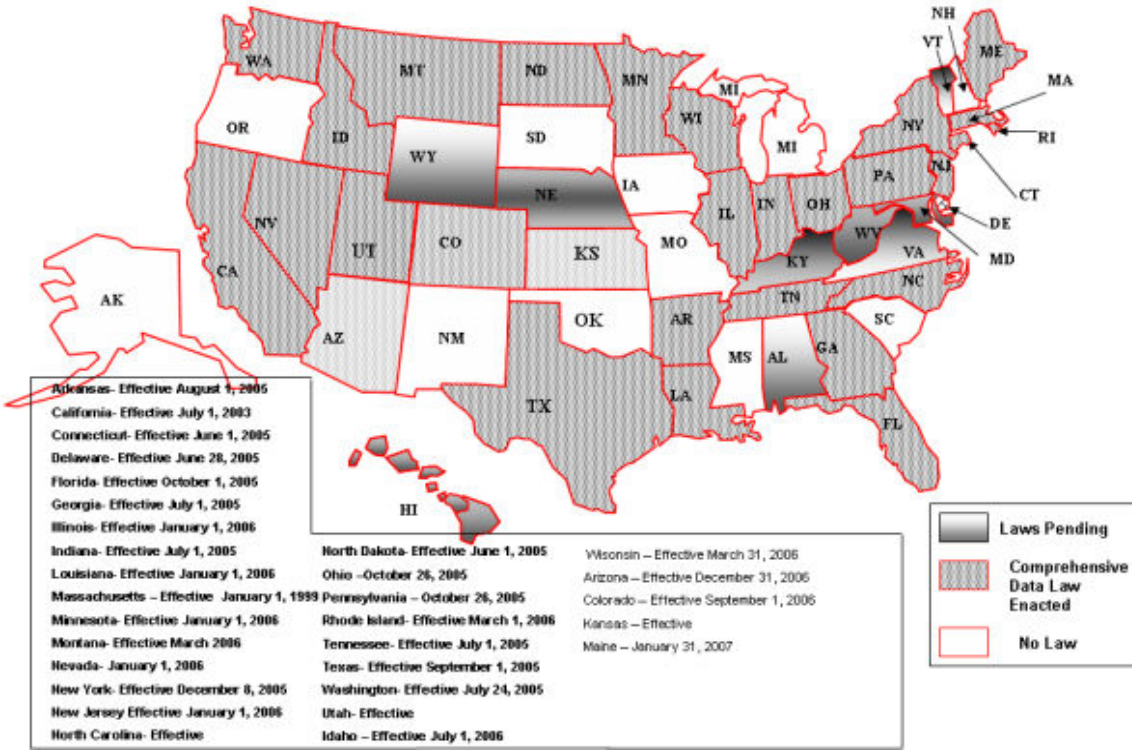
Taylor, H (2003), "Most People Are "Privacy Pragmatists" Who, While Concerned about Privacy, Will Sometimes Trade It Off for Other Benefits", http://www.harrisinteractive.com/harris_poll/index.asp?PID=365, accessed June24, 2007.

Tentori, M., Favela, J., Gonzalez, V.M. and Rodriguez, M.D. (2005), "Supporting Quality of Privacy (QoP) in Pervasive Computing," Proceedings of the Sixth Mexican International Conference on Computer Science (ENC'05), IEEE Computer Society, 1-3.

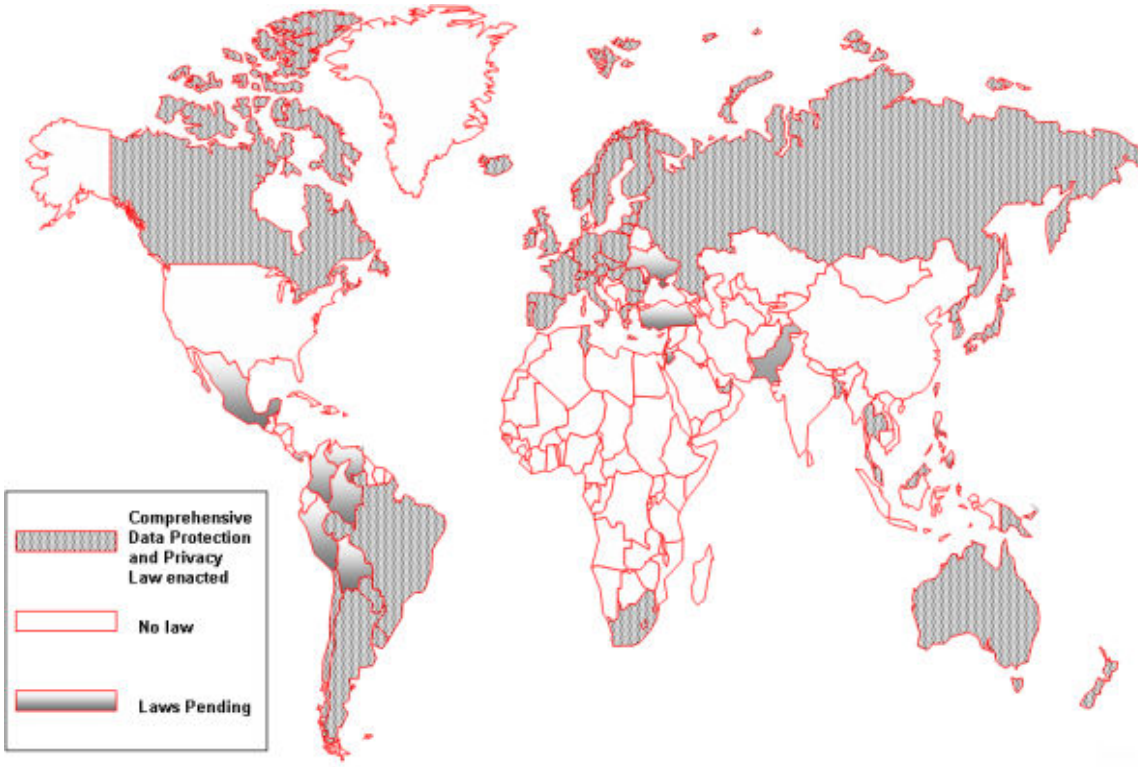
Tentori, M., Favela, J., Gonzalez, V.M. and Rodriguez, M.D. (2006), "United States Mobile Subscriber: Monthly Consumption of Content and Applications," M:Metrics Inc., Benchmark Survey, April, 16.

APPENDICES

Appendix A - Domestic Data Protection and Privacy Legislation, April 2006



Appendix B - International Data Protection and Privacy Legislation, April 2006



Appendix C – Tables

Table 1 – Importance (Percents)

Use	Don't Care	Not Important	Somewhat Important	Important	Very Important
Business	4	16	22	22	36
Emergency	0	8	6	21	65
Media	14	25	29	20	12
Search	5	13	16	26	40
Social Contacts	3	12	27	31	27
Other Uses	9	17	39	21	14

Table 2 – Privacy (Percents)

Question	Strongly Disagree	Disagree	Neither Agree Nor Disagree	Agree	Strongly Agree
Provider Can Monitor Exact Location	1	9	18	45	27
Provider Can Mine Information While Using MCD	8	4	13	50	25
MCD Gathered Data Can Be Marketed To Other Firms	11	4	17	48	20
E-mail Can Intrude On Privacy	5	7	23	41	24
Wireless Internet Can Intrude On Privacy	5	7	11	46	31
GPS Can Intrude On Privacy	1	3	20	43	33
RFID Can Intrude On Privacy	5	8	16	41	29
Location Data Retention Policies Can Intrude On Privacy	4	3	20	50	23

Table 3 – Wireless provider Policies

Question	Yes	No
Do you read the contract before signing the contract?	32	68
Do you read the privacy policies before signing the contract?	28	72
Have you expressly Opted-out on your mobile contract?	36	64
Do you read provider security policies before signing the contract?	41	59
Do you know the procedure your provider uses to safeguard your personal information?	28	72
Do you know what your provider will do if your information in compromised?	15	85
Was you personal information ever compromised by a breach in your provider's security	14	86
Was your MCD ever misplaced or stolen?	17	83

Table 4 – Trust and Advertising

Question	Strongly Disagree	Disagree	Neither Agree Nor Disagree	Agree	Completely Agree
I am comfortable that my provider will protect my privacy.	7	11	48	24	11
I am concerned about location-based privacy when using my MCD.	7	17	41	25	9
I am concerned about identity theft.	1	3	5	39	52
I am confident that government regulations will protect my privacy.	23	26	26	22	4
A security breach by my provider would lower my confidence in the provider.	4	4	13	28	51
I would terminate my contract in the event of a breach in security.	3	9	20	22	46
I am concerned that a virus or malware will attack my MCD.	8	16	29	23	24
I like the idea of mobile advertising messages.	73	20	5	1	0
I like the idea of mobile advertising alert messages when I am near a product.	65	25	7	3	0
I like the idea of mobile advertising if the advertising is meaningfully personalized to me.	49	20	23	8	0

Table 5 – Crosstab

Crosstab

Count

		Question 4: Gender:			
			Female	Male	Total
Question 6: On average, how many hours each day do you use your mobile devices?	1.0	0	8	25	33
	3.5	0	8	12	20
	3.7	1	0	0	1
	5.5	0	2	6	8
	7.5	0	4	2	6
	9.5	0	2	3	5
	11.5	0	1	0	1
	15.0	0	1	1	2
Total		1	26	49	76

Table 6 – Chi-Square Tests

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	83.126[a]	14	.000
Likelihood Ratio	17.839	14	.214
N of Valid Cases	76		

a. 19 cells (79.2%) have expected count less than 5. The minimum expected count is .01.

Appendix D - FRAMEWORK of Syllabi

Location-Based PRIVACY with Mobile Computing

Module 1: Architecture and Applications of Mobile Computing

Bluetooth
Global Positioning Systems (GPS)
Radio Frequency Identification Tags (RFID)
Short Messaging Services (SMS)
Wireless Application Protocols (WAP), Broadband (WiMax) and Local Area Networks

Module 2: Design and Development of Mobile Computing Applications

Graphical User Interface (GUI)

Java 2 Micro Edition (J2ME)
Multimedia
Palm Operating System (OS)
Symbian Operating System (OS)
Windows CE

Voice over Internet Protocol (VoIP)

Module 3: Privacy of Mobile Computing Applications – ***Enhancement to Syllabi***

Citizen and Consumer Constructs

Definitions of Privacy
Functions of Privacy

Ethical Constructs

Ethics of Profiling
Ethical Use and Mining of Consumer data

Governmental Constructs – United States

United States Constitution

Court Decisions
Federal Legislation
State Legislation

Governmental Constructs – European Union

European Commission Directives

Member Nation Legislation

Methodological Constructs

Chief Privacy Officers (CPO)

Digital Identity, Identity Layers, Liability and Rights Management
Human Factor Failures

Platform for Privacy Preferences
Pretty Good Privacy (PGP)

Privacy Organization Standards

Privacy Policies

Technological Constructs

Privacy Aware Technologies (PAT)

Privacy Invasive Technologies
Privacy Software Technologies

Module 4: Security of Mobile Computing Architecture and Applications – ***Enhancement to Syllabi***

Chief Security Officers (CSO)

Information Protection and Security

Authorization
Availability
Confidentiality
Integrity
Non-Repudiation

Public Key Infrastructure (PKI)

Security Protocols

Secured Socket Layers (SSL)
Transport Layer Security (TLS)
Wireless Transport Layer Security (WTLS)
Multifactor Security
Digital Watermark
Key Recovery

Smartcard Security
Mutual and Spatial Authentication
RFID Security
Mobile Agent Security

Security Techniques

Ciphering
Cryptography
Hashing Algorithms

Security Policies

Solutions and Threats to Security and Trust

Module 5: Mobile Computing Societal and Technological Trends

"Big Brother"

Biometrics
e-Passports
Loyalty and Travel Cards
National Identity Cards

Privacy and Surveillance in Era of Terrorism

Sources:

Gilbert, N. (2007), "Dilemmas of Privacy and Surveillance: Challenges of Technological Change," The Royal Academy of Engineering, March.

Lawler, J. and Molluzzo J.C. (2006) "A Study of Data Mining and Information Ethics in Information Systems Curricula," Information Systems Journal, 4 (34)

Talukder, A.K. and Yavagal, R.P. (2007) Mobile Computing: Technology, Applications and Service Creation, McGraw Hill, New York.