ISSN: 1545-679X

Information Systems Education Journal

Volume 6, Number 47 http://isedj.org/6/47/ December 1, 2008

In this issue:

An Expanded Study of Integrating Issues of Location-based Privacy with Mobile Computing into General Curriculum of Universities

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

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

Pascale Vandepeutte
University of Mons-Hainaut
Mons, Belgium

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. Expanding upon a prior paper of the authors on the learning or non-learning of information systems students in America on the evolving impact and issues of mobile computing on privacy and security, this paper offers research on the perceptions of non-information systems students. This research includes findings from surveys of non-information systems students at Pace University in America and at the University of University of Mons-Hainaut in Belgium that 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 general curriculum but also an opportunity to improve the curriculum. This study will benefit instructors in all disciplines attempting to improve their pedagogy with societal-sensitive syllabi that integrate contemporary issues of privacy and security with mobile computing.

Keywords: Curriculum Design, Location-Based Privacy, Mobile Computing, Pervasive Computing, Radio Frequency Identification Devices (RFID)

Recommended Citation: Lawler, Molluzzo, and Vandepeutte (2008). An Expanded Study of Integrating Issues of Location-based Privacy with Mobile Computing into General Curriculum of Universities. *Information Systems Education Journal, 6* (47). http://isedj.org/6/47/. ISSN: 1545-679X. (Preliminary version appears in *The Proceedings of ISECON 2008:* §2312. ISSN: 1542-7382.)

This issue is on the Internet at **http://isedj.org/6/47/**

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 2008 best papers group. Best papers received preliminary reviews by three or more peers placing them in the top 30% of papers submitted and final reviews placing them in the top 15% by three or more former best papers authors who did not submit a paper in 2008.

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.

An Expanded Study of Integrating Issues of Location-based Privacy with Mobile Computing into General Curriculum of Universities

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

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

Pascale Vandepeutte
pascale.vandepeutte@umh.ac.be
e-Business, University of Mons-Hainaut
Mons, Belgium

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. Expanding upon a prior paper of the authors on the learning or non-learning of information systems students in America on the evolving impact and issues of mobile computing on privacy and security, this paper offers research on the perceptions of non-information systems students. This research includes findings from surveys of non-information systems students at Pace University in America and at the University of University of Mons-Hainaut in Belgium that 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 general curriculum but also an opportunity to improve the curriculum. This study will benefit instructors in all disciplines attempting to improve their pedagogy with societal-sensitive syllabi that integrate contemporary issues of privacy and security with mobile computing.

Keywords: Curriculum Design, 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 (Haskin, 2006). 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 integral to consumers (Castells, Fernandez-Ardevol, Qiu and Sey, 2007). Miniature mobile computing is contributing to a new period of pervasive computing (Denne, 2007).

Location-based services on mobile computing devices continue to emerge in convenient 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 (Hesseidahl, 2008). 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 benefit (Minch, 2004) in a market that is expected to be approximately $3 billion in America (Reardon, 2006) and $620 million in Europe (Berg Insight, 2006) in 2010.

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 (Sharma and Vascellaro, 2008 & 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 (Grossman, 2007). 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). Issues may include employee monitoring (Hamblen, 2007). RFID is not infrequently considered by pundits and researchers as synonymous with surveillance (Soat, p.44, 2006 & Curtin, Kauffman and Riggins, 2007). 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 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 and non-information systems practitioners in including location-enabled privacy and security in the design of mobile computing systems. Instructors in information systems and non-information systems may be challenged in educating students if these issues are not integrated into current curriculum 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 and non-information systems practitioners and instructors of information systems and non-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 students, and students themselves who may become information systems professionals or non-information systems professionals interfacing with information systems professionals 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 non-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) and may not be important to students (Ponemon, 2007). Practitioners in information systems and non-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 society, as learning in institutions 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 in America and Europe have to encourage instructors to evaluate if not enhance curriculum 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 analyze the knowledge of undergraduate and graduate non-information systems students of the impact of mobile computing on location-based privacy. Analysis of this knowledge enables further input into the learning or non-learning of these students on privacy and regulation in their general curriculum, expanding the earlier study of data mining and information ethics in information systems curricula (Lawler and Molluzzo, 2006 & Molluzzo and Lawler, 2007), 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) and needs of regulations and of systems (Weitzner, Abelson, Berners-Lee, Feigenbaum, Hendler and Sussman, 2008). The goal of the final study is to furnish a framework for instructors in all disciplines, non-information systems and systems, in integrating issues of location-based privacy with mobile computing into societal-sensitive syllabi for students who will be the future of global society if not 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

In a 2007 study, Molluzzo and Lawler (2008) analyzed the knowledge of undergraduate and graduate *information system students* of the impact of mobile computing on location-based privacy. In the current study, this analysis is extended to two groups of *non-information systems undergraduate students*, one group in the United States, the other in Europe. The 2007 survey instrument was quite long. Therefore, a subset of the original questions was chosen for the present study. Analysis of the non-information systems students (see Section 5) and comparative results between the information systems students and the non-information systems students (see Section 6) are based on these common questions.

The survey administered to students in the United States (all attending Pace University) was administered online using Zoomerang in November, 2007. These students were mostly first and second year undergraduates taking an introductory computing course that is required of all students at Pace. In the spring of 2007, the survey was administered to the European students, all of whom were undergraduate business majors at the e-Business School of the University of Mons-Hainaut, Belgium, using hard-copy during one of their classes. There were 75 completed United States surveys and 19 completed European surveys. The survey instructions asked the respondents to limit their responses to their experience using mobile computing devices (MCDs), excluding dedicated audio devices, such as the iPod. The survey was administered anonymously – the respondents' names were not collected by the authors.

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

Of the European students, 13 were female and 6 were male; of the United States students, 49 were female and 26 were male. The academic majors of the United States students were varied: business (48%), liberal arts (13%), computing (8%), nursing (4%), and other (27%). The European students were all business majors. The average age of the United States students was 19, while the average age of European students was 22. European students reported using their mobile devices for an average of 6 hours per day. United States students reported using their mobile devices on average for 7 hours per day.

The United States and European groups were combined for the analysis that follows. In Section 6, we analyze some of the differences between these students and the information systems students that were the basis of the 2007 study (Molluzzo and Lawler,2008).

Objective Questions

Objective questions were asked regarding the respondents use of MCDs

Frequency of Use: Respondents were asked to "rate how frequently you use your Mobile Computing Device and for what reasons. The answers were based on a five-point Likert scale. Table 1 in Appendix C summarizes the results. Each entry in the table is a percent of those answering the question either "Frequently" or "Very Fre-

quently. The most frequently used service is for Social Contacts with Business/School not far behind. The lowest used service was for Games.

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. Table 2 shows the percent of respondents answering "Frequently" or "Very Frequently". The least used features were driving directions and e-banking, possibly because of the low average age of the respondents. Also possibly because of the respondents' low average age, texting was the most frequently used feature, with e-mail and instant messaging following.

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, three people (out of the 75 United States students) store their Social Security Numbers, five people store unencrypted account passwords, three people store credit card numbers, and five 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. The only statement with which a majority of respondents "Agree" or "Strongly Agree" (55%) is that a "location-based mobile computing device can monitor your exact location." Even this number is very low considering that GPS technology is constantly in the news. Table 3 in Appendix C summarizes the results. It is very interesting that such large percentages of students do not consider wireless Internet access and GPS systems as possible threats to their privacy.

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 in line with the Privacy questions, which indicate a low degree of awareness of important privacy issues when using MCDs. 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, 100% do not read their carrier's privacy policy; 74% do not know what their provider will do if their information is compromised. The results are in Table 4 in Appendix C, where numbers represent percents who answered No to the questions.

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 (30% Agree or Completely Agree) or the government (34% Agree or Completely Agree)) will protect their privacy. A fairly low percentage, 56%, either Agree or Completely Agree that they are concerned about identity theft. Interestingly, however, only 25% 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 advertising did not get a strong vote of confidence from the respondents. Only 7% of the respondents either Agree or Strongly Agree that they would like mobile advertising messages. Even if the advertising were targeted and personalized, only 15% of the respondents Agree or Strongly Agree. Table 5 in Appendix C summarizes the results. .

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 12% encrypt all data, 10% encrypt all business-related data, and 11% encrypt all sensitive data. Also, only 17% use encryption when connected to a wireless network. However, 44% lock access to their MCD using a strong password and 32% set the MCD to auto-lock when not in use for a specified time. Many respondents, 62%, keep their MCD hidden when traveling, but only 29% do not access private or business data in public places. Finally, only 30% of

respondents remove all data on their MCD before discarding or turning it in.

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

- I feel strongly about privacy. (41%)
- 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. (54%)
- I do not feel strongly about privacy. (5%)

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 different distribution from our results – 41%, 54%, 5%. However, our population college students) might be more informed about privacy issues than the general population.

Note that the only students who do not feel strongly about privacy were from Europe. This could be a result of the fairly strict privacy laws of the European Union.

6. STATISTICAL COMPARISONS

This section compares the differences between the 77 information systems students from the 2007 study (Molluzzo and Lawler) and the non-information systems students from the present study. Also discussed are some differences between the United States and European populations.

Many of the questions in the survey utilized a 5-point Likert scale. However, because of the small sample sizes, for purposes of comparison the 5-point scale was compressed. The three lowest Likert scores (Strongly Disagree, Disagree, Neutral, for example) were converted to 0 and the two highest (Agree and Strongly Agree, for example) were converted to 1. This enabled use of the chi-squared test for independence on 2x2 tables. Note that all significance measures are for two-sided p-values.

Information Systems vs. Non-Information Systems Students: There were statistically significant differences between these groups at the $p < .001$ level of significance in three of the uses of their MCD devices. These uses were for emergency, storing digital media, and e-banking. See Table 6 in Appendix C.

Non-computing or non-information systems students tend to use the social functions of their MCDs more than computing students. For instant messaging, text messaging, contacting family and friends there were significant differences in use at the $p < .001$ level. For social contact uses there was a significant difference at the $p < .01$ level. See Table 6 in Appendix C.

There were also some significant differences in what students store on their MCDs. There is a difference at the $p < .001$ level of significance in storing their age and storing their school name. There is a difference at the $p < .01$ level in storing their place of employment. See Table 6 in Appendix C.

There was a significant difference in the awareness of how MCDs can affect privacy. Computing or information systems students were significantly more aware (at the $p < .001$ level) that wireless access and GPS services can intrude on privacy. Non-computing or non-information systems students were also significantly more concerned about identity theft (at the $p < .001$ level.) There was also a difference at the $p < .05$ level in the knowledge that an MCD can monitor your exact location. See Table 7 in Appendix C.

The only Wireless provider question in which there was a significant difference (at the $p < .05$ level) was whether they like the idea of mobile advertising. Non-computing or non-information systems students like the idea more. See Table 7 in Appendix C.

There were also significant differences in the ways the two groups protect their MCDs. In the use of encryption, either in storing sensitive data or when connecting to a wireless network, there were differences at the $p < .001$ level of significance. Similarly, there was a difference at the $p < .01$ level in the groups' encryption of business data on their MCDs. Also there was a difference at the $p < .05$ level of significance in encrypting all the data on their MCDs. Finally, there was a difference at the $p < .05$ level of significance in whether the students remove all data on

their MCD before discarding the device or turning it in. See Table 8 in Appendix C.

These results show that information systems majors are more aware of location-based privacy issues than is the general student population. Clearly the general population needs to be made aware of the privacy and security issues surrounding the use of MCDs.

United States vs. European Students: Because of the small sample size of European students (n = 19), we report here only those results that were significant at the $p < .01$ or $p < .001$ levels. Even in these cases, it is not advisable to make generalizations from the results.

On the use of MCDs for accessing weather, business/school, and family and friends; only one European student in all three categories answered yes ($p < .001$). We are not sure what this means. Obviously further investigation is necessary. Several other MCD use differences were observed at the $p < .01$ level of significance. For example, for emergencies, storing and sharing digital media, and searching European student use if far less than that of United States students. See Table 9 in Appendix C.

Only one other difference at the $P < .05$ level of significance was observed. Apparently, European students are not as concerned about identity theft as are their United States counterparts. This difference could be due to the European Union's stronger privacy laws.

7. FRAMEWORK OF SYLLABI

The findings of the 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 and in the general curriculum.

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.

8. IMPLICATIONS OF STUDY

An implication of the findings of the study is the information systems students' clear knowledge of the fundamental functionality of mobile computing devices compared to a lesser knowledge of these issues by non-information systems majors. The non-information systems students were not as knowledgeable in both the processes and practices of mobile computing firms. These findings imply a likely lower sensitivity of non-information systems students to the larger impact of mobile computing technology on society as compared to information systems students.

Another implication of the study is an inconsistency in the higher knowledge of both groups of 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 study include the potential opportunity to improve the mobile computing syllabi of information systems and business or non-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 study imply minimally that an improvement is needed in mobile computing and information systems and business or non-information systems syllabi, and a framework for improvement of the syllabi is modeled in Appendix D of this study.

9. LIMITATIONS AND OPPORTUNITIES FOR RESEARCH

An 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 general student population seems to be much less aware of both the processes and practices of mobile computing firms.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 information systems students in the processes of location-based mobile computing technology in contrast to lower personal *precaution* with the technology. These 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.

This study also shows that non-computing or non-information systems students are much less aware of privacy issues surrounding MCDs than are computing or information systems students. Because mobile computing is becoming a very large part of the public's personal and business lives, the study indicates that the general population needs to be made aware of such issues. One way to do this is to incorporate notions of privacy in mobile computing into the general curriculum and specifically into the curriculum of information systems students who will be the stewards of such technology in the future.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 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.

10. CONCLUSION

The research of this study analyzed the learning and non-learning of non-information systems students on location-based privacy with mobile computing and compared these findings to an earlier study of information systems students. Findings from the study of the student subjects at Pace University and at the University of Mons-Hainaut indicated a lower level of knowledge of the functions of mobile computing devices, location-based privacy and security of these devices among non-information systems students as compared to information systems students. Findings indicated the implied importance of improving information systems curricula in the schools of computer science and information systems by integrating societal sensitive syllabi. The authors of this study continue to welcome other universities that might be interested in partnering on new studies of location-based services with mobile computing.

11. 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.

12. 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.

Castells, M., Fernandez-Ardevol, M., Qiu, J.L. and Sey, A. (2007) Mobile Communication and Society: A Global Perspective, The MIT Press, Cambridge, Massachusetts, 77.

Curtin, J., Kauffman, R.J. and Riggins, F.J. (2007) "Making the 'MOST' Out of RFID Technology: A Research Agenda for the Study of the Adoption, Usage and Impact of RFID," Information Technology Management, 8, 92,100.

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.

Denne, S. (2007) "After Being Over-Hyped, RFID Starts to Deliver," The Wall Street Journal, November 7, B5F.

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.

Grossman, L. (2007) "Tag, You Are It: They Are Cheap, They Are Tiny, and They Are Everywhere. But Are RFID Chips Good for Humanity?," Time, October 29, 57.

Hakkila, J. and Chatfield, C. (2005) "It Is Like If You Opened Someone Else's Letter – User Perceived Privacy and Social Prac-

tices with Short Message Service (SMS) Communication," Proceedings of Mobile-HCI'05, Salzburg, Austria, September 19-22, 219-222.

Hamblen, M. (2007) "Privacy Concerns Dog Information Technology (IT) Efforts to Implement RFID: Employees Often Rebel Against Plans to Include Chips in Corporate Identification (ID) Badges," Computerworld, October 15, 26.

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.

Haskin, D. (2006) "On the Go and in the Game: Six (6) Emerging Technologies Will Change the World of Communication by Letting Mobile Professionals Stay On-Line and in Touch," Information Week, August 21, 47-51.

Hesseldahl, A. (2008) "A Rich Vein for 'Reality Mining': Researchers and Companies Are Finding Novel Uses for Information Extracted from Cell-Phone Ads," Business Week, May 5, 052-053.

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.

Molluzzo, J. and Lawler, J. (2007) "Integrating Issues of Location-Based Privacy with Mobile Computing Into International Information Systems Curricula," Information Systems Education Journal, 6(32).

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.

Ponemon, L. (2007) "The Voice of Experience," CIO, October 15, 80.

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.

Reardon, M. (2006) "Mobile Phones That Track Your Buddies," www.news.com/2102-1039_3-6135209.html.

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.

Sharma, A. and Vascellaro, J.E. (2008) "Phones Will Soon Tell Where You Are," The Wall Street Journal, March 28, A13-A14.

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.

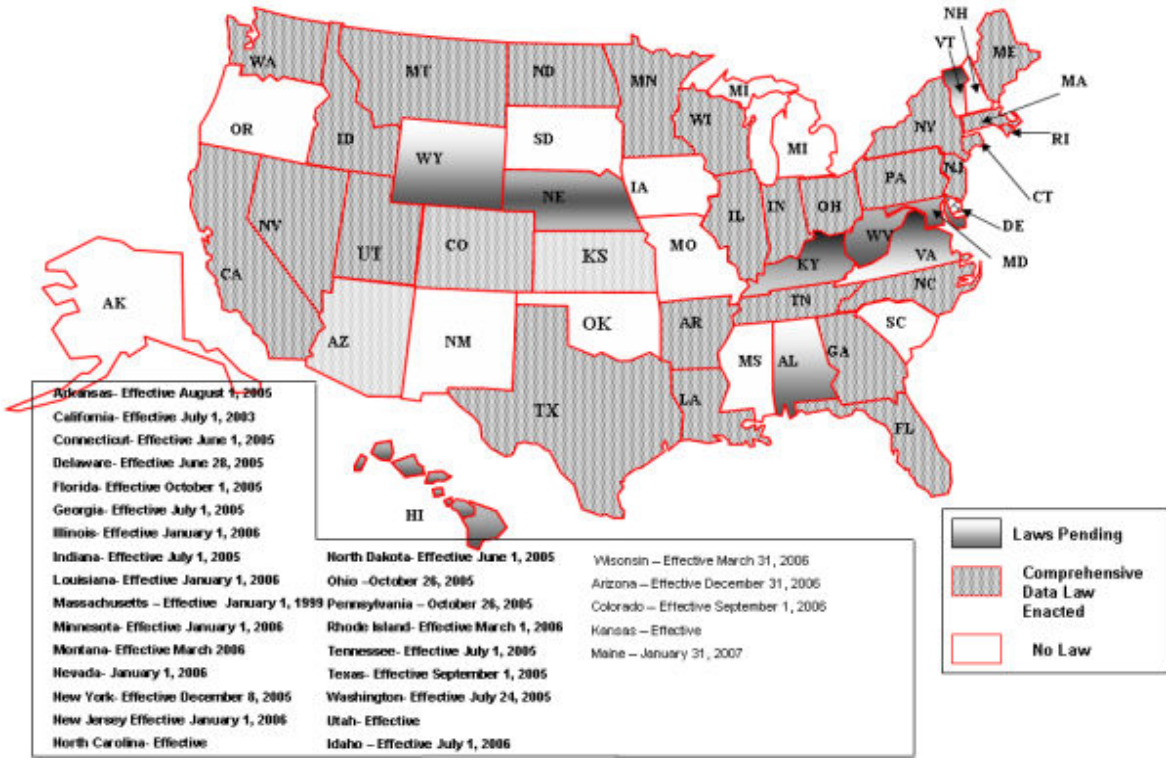
Tentori, M., Favela, J., Gonzalez, V.M. and Rodriguez, M.D. (2005) "Supporting Quality of Privacy (QoP) in Pervasive Computing," Proceedings of the Sixth Mexican International Conference on Computer Science (ENC'05), IEEE Computer Society, 1-3.

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.

Weitzner, D.J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J. and Sussman, G.J. (2008) "Information Accountability," Communications of the ACM, 51(6), 82-87.

_____ (2006) "Strategic Analysis of the European Mobile Location Based-Services (LBS) Market, Berg Insight.

Appendix A
Domestic Data Protection and Privacy Legislation, April 2006



Source: Millbank, Tweed, Hadley & McCloy LLP and Citi (2007), Presentation on BPO, ITO and AO, IDC Outsourcing Forum, New York, New York, April 12, p. 20 [Adapted].

Appendix B
International Data Protection and Privacy Legislation, April 2006

Source: Millbank, Tweed, Hadley & McCloy LLP and Citi (2007), Presentation on BPO, ITO and AO, IDC Outsourcing Forum, New York, New York, April 12, p. 18 [Adapted].

Appendix C
Tables

Table 1 – Frequency of Use (Percents)

Use	Frequently or Very Frequently
Business/School	69
Emergency	35
Media	63
Search	60
Games	10
Social Contacts	83

Table 2 – Use of MCD Features (Percents)

Use	Frequently or Very Frequently
Driving Directions	19
Destination Guides	29
Weather	34
E-Banking	16
E-Mail	65
Instant Messaging	61
Photo/Video Sharing	33
Text Messaging	76

Table 2 – Location-Enabled Features (Percents)

Table 3 – Privacy (Percents)

Question	Agree or Strongly Agree
Provider Can Monitor Exact Location	55
MCD Location Data Can Be Marketed to Other Firms	46
Email Can Intrude on Privacy	48
Wireless Internet Access Can Intrude on Privacy	47
GPS Can Intrude on Privacy	36

Table 4 – Wireless Provider Policies (Percents)

Question	No
Do you read the privacy policies before signing the contract?	100
Have you expressly Opted-out on your mobile contract?	78
Do you know the procedure your provider uses to safeguard your personal information?	80
Do you know what your provider will do if your information in compromised?	74
Was your MCD ever misplaced or stolen?	68

Appendix C (continued)
Tables

Table 5 – Trust and Advertising (Percents)

Question	Agree or Strongly Agree
I am comfortable that my provider will protect my privacy.	30
I am concerned about location-based privacy when using my MCD.	25
I am concerned about identity theft.	56
I am confident that government regulations will protect my privacy.	34
I like the idea of mobile advertising messages.	7
I like the idea of mobile advertising if the advertising is meaningfully personalized to me.	15

Table 6 – Significant Differences in Uses Between Computing and Non-Computing Students

Use	p < .0001	p < .01	p < .05
Emergency	***		
Storing Digital Media	***		
E-banking	***		
Texting	***		
Contacting Family and Friends	***		
Social Contacts		**	
Storing User's Age	***		
Storing User's School Name	***		
Storing User's Place of Employment		**	

Table 7 – Significant Differences in Privacy Awareness Between Computing and Non-Computing Students

Question	p < .001	p < .01	p < .05
Wireless Access can intrude on Privacy	***		
GPS Can Intrude on Privacy	***		
I am Concerned About Identity Theft	***		
MCD's Can Monitor My Exact Location			*
I Like the Idea of Mobile Advertising			*

Appendix C (continued)
Tables

Table 8 – Significant Differences in Control Questions Between Computing and Non-Computing Students

Question	p < .001	p < .01	p < .05
Encrypt All Data Stored on MCD			*
Encrypt All Sensitive Data Stored on MCD	***		
Encrypt All Business Data Stored on MCD		**	
Use Encryption When Connecting to a Wireless Network	***		
Remove All Data Stored on MCD Before Discarding or Handing In			*

Table 9 – Significant Differences Between U.S. and European Students

		p < .001	p < .01	p < .05
Uses	Weather	***		
	Contacting Business or School	***		
	Contacting Family and Friends	***		
	Emergency		**	
	Storing and Sharing Digital Media		**	
	Searching		**	
Concern Question	I Am Concerned About Identity Theft			*

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 Management
Ethics of Profiling
Ethical Use and Mining of Consumer Data
Integrity Management
Levels of an Ethical Organization

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

Reference Research Sites for Syllabi

www.bentley.edu/research
www.bsr.org – Business for Social Responsibility
www.cdt.org – Center for Democracy and Technology
www.corpwatch.org – Watchdog on the Web
www.depaul.edu/ethics - Institute for Business and Professional Ethics
www.ebnsc.org – Corporate Social Responsibility in Europe
www.epic.org – Electronic Privacy Information Center
www.esrc.ac.uk – Economic and Social Research Council in United Kingdom
www.ethics.org – Ethics Resource Center
www.ietf.org – The Internet Engineering Task Force
www.oecd.org – Organization for Economic Cooperation and Development
www.ponemon.org – Ponemon Institute LLC
www.privacyconference.co.uk – International Data Protection and Privacy Commissioners – United Kingdom
www.privacyinternational.com – Privacy International
www.privacyjournal.com – Privacy Journal
www.rfid-world.com – RFID World
www.w3.org/p3p/ - The Platform for Privacy Preferences
www.worldcsr.com – World Social Responsibility

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.