User Privacy in Mobile Advertising

Hyunsook Kweon
University of Maryland, Baltimore County, Baltimore, MD, United States., hyun10@umbc.edu

Dongsong Zhang
Information Systems, University of Maryland, Baltimore County, Baltimore, MD, United States., zhangd@umbc.edu

Lina Zhou
University of Maryland, Baltimore County, Baltimore, MD, United States., zhoul@umbc.edu

User Privacy in Mobile Advertising

Hyunsook Kweon
University of Maryland, Baltimore County
hyun10@umbc.edu

Dongsong Zhang
University of Maryland, Baltimore County
zhangd@umbc.edu

Lina Zhou
University of Maryland, Baltimore County
zhoul@umbc.edu

ABSTRACT

With the pervasiveness of mobile devices in our daily life continuously increasing, mobile advertising is emerging as an important marketing strategy. However, due to its intrusive nature in practice, there has been a growing concern over users' privacy in mobile advertising, especially push-based mode, which can affect consumers' acceptance and effectiveness of mobile advertising. Aiming to gain a deeper understanding of not only users' concerns of privacy intrusion in mobile advertising, but also the potential solutions to addressing those concerns, we conducted a survey in this study. The findings of this study provide a few useful insights for researchers, advertisers, and businesses on both the importance and methods of privacy protection in mobile advertising from a user perspective.

Keywords

Mobile advertisement, privacy, privacy protection

INTRODUCTION

The advancement of mobile telecommunication technology, rapid growth of mobile device users, and emergence of mobile applications are creating new opportunities for marketers and advertisers to advertise products and services to consumers through mobile devices (e.g., cell phones). Mobile advertising (M-advertising, m-ad) is operationally defined as distributing advertising messages electronically to prospects' mobile handheld devices. With the pervasiveness of mobile devices in our daily life continuously increasing, mobile advertising is becoming an important and practical marketing strategy. Stafford and Faber (2005) identified four commonly used mobile advertising strategies, which include relationship marketing/customer loyalty, media/entertainment, direct response-customer acquisition, and brand awareness. On the one hand, m-advertising is relatively inexpensive compared to other advertising venues and is much more efficient to reach target consumer groups or individuals virtually at any place, anytime, or based on the physical location of consumers (Siau and Chen, 2003). In particular, a large portion of mobile advertising adopts a push-based approach that automatically delivers electronic advertisement to users' mobile devices based on their current location. On the other hand, the strategy of wide dissemination of mobile advertising would not be effective without user acceptance. There have been growing concerns about the protection of users' privacy in mobile advertising due to its intrusive nature and practice (Cleff, 2007). Therefore, it is essential to understand how mobile advertising may intrude users' privacy, how users perceive privacy issues in mobile advertising, and what preferred solutions to protecting privacy in such a context are.

Privacy should not be viewed as an absolute concept. It has been defined in terms of control over the disclosure and use of personal information in order to ensure an effective right for privacy (Siau and Chen, 2003). According to the Private Rights Clearinghouse, privacy includes not only people's personal information such as name, date of birth, home address, and social security number, but also their relationship

status, photos, political and religious views, shopping habits, driving history, medical records, credit score, and so on (Chen and Rahman 2008). An invasion of privacy occurs when a person's personal information is disclosed to others by the third party without his/her consent. Unfortunately, privacy has been increasingly threatened as a result of the rapid growth of portable handheld devices (e.g., cell phones) and wireless network technology.

Privacy issues are sensitive, difficult to study, and poorly understood. Studying privacy in the mobile world is quite difficult because collecting information about users' privacy concerns can be cumbersome and unreliable (Fang and LeFevre, 2010), let alone to address them. This study attempts to empirically investigate users' perception of privacy issues in mobile advertising and preferred solutions for privacy protection. The findings of this research provide some insights for researchers and businesses on how to address privacy concerns in mobile advertising in order to achieve its potential. They can help marketers and the related industry to develop more effective techniques, policies, and strategies for privacy protection.

The remainder of the paper is organized as follows. First, we review the literature on privacy in mobile advertising. We conducted a relatively comprehensive review on this line of research by surveying prior related studies published after 2005 in IEEE and ACM digital libraries, as well as in other relevant sources such as Personal and Ubiquitous Computing journal. Then, we introduce the research methodology used in this study, followed by data analysis and results. Finally, we discuss the findings and their implications of this research.

BACKGROUND AND RELATED WORK

According to International Telecommunication Union, there were 5.9 billion people subscribing to mobile cellular phone services around the world in 2011. In the early stage of mobile advertising, most of advertising sent simple text messages as SMS and/or MMS. With the evolution of the technology, multimedia messages such as audio and video clips are incorporated into mobile advertisement (Tähtinen, 2005; Park, Shenoy and Salvendy, 2008). M-advertising can be the most powerful one-to-one advertising method if it is used properly (Leppäniemi and Karjaluoto, 2005). One major characteristic of mobile commerce is the ubiquity. People can access Internet and conduct business at anytime and anywhere through mobile devices and wireless networks. Another characteristic is uniqueness – in most cases, a mobile phone belongs to and is used by a single user (Tao, 2008). Today, people consider mobile devices as a must-have item and carry them all the time. Due to this phenomenon, marketers are able to reach individual customers regardless of their time and location. Because of a large number of mobile phone service subscribers, marketers can reach a massive number of people. They can use consumer feedback to customize their messages and offerings and collect information about consumers' preferences to improve future product and service advertising. This provides an exceptional advantage for marketers by enabling them to reach potential customers in a very personalized way through the usage of demographic information collected by wireless service providers and information about the current location of a mobile user. Thus, advertising can be carried out very precisely and with a clear focus on a target group (Haghirian, 2005; Gao, Rau, and Salvendy, 2010). However, it also brought the flip side like hacking, phishing, illegal spamming, and privacy invasion (Finneran, 2006; Coursaris, Hassanein, and Head, 2003). Therefore, consumer trust is important to the growth and success of mobile advertising. Users' privacy concern may significantly affect their trust and perceived risk, further affecting their usage behavior and even acceptance of mobile advertisement (Siau and Chen, 2003).

Mobile Advertising Types

Mobile advertising can be classified based on different perspectives. Gao et al. (2010) have identified different kinds of mobile advertisement from a media perspective, including short messaging service (SMS) advertisements, multimedia messaging service (MMS) advertisements, wireless application protocol (WAP) advertisements, mobile web advertisements and mobile game advertisements. Limited to 160 characters in

length, SMS is a proven fast, effective and low cost way to reach consumers (Merisavo, Kajalo, Karjaluoto, Virtanen, Salmenkivi, Raulas and Leppäniemi, 2007). Advances in mobile technology have since enabled the evolution of multimedia messages (MMS) based on WAP (Wireless Application Protocol). Multimedia messages, different from SMS, can keep recipients captivated and open to receive communication (Beneke, Cumming, Stevens, and Versfeld, 2010). MMS messages are sent by using a combination of SMS and WAP. Initially, sending devices encode a multimedia message similarly to sending a MIME (Multipurpose Internet Mail Extensions) e-mail, which is then forwarded to a carrier's MMSC (Multimedia Messaging Center) storing the content of the MMS message. MMSC generates a MMS notification message comprising the header information of the MMS message and an HTTP URL link. This MMS notification message is then sent to the mobile device via WAP Push protocol over SMS. The sent message automatically triggers the WAP browser on that device to open the URL and to download the content of the MMS message. Currently a few mobile network operators offer direct connection to their MMSC forward servers for content providers. This makes many content providers use WAP push because it is the only method available for delivering rich content to mobile devices.

Based on how it is delivered, m-advertisement can also be categorized into push- or pull-based advertising. Push-based advertising refers to the automatic delivery of advertisements to consumers' mobile devices without receiving their explicit inquiries first. In contrast, pull-based advertising refers to sending advertisement messages to consumers only after receiving their explicit requests on a one-time basis (Cleff, 2007). In other words, the former is outbound communication originated from a marketer, while the latter is inbound communication initiated by a consumer (Unni and Harmon, 2007). From a marketing perspective, push-based advertising is more attractive than pull-based advertising because a marketing company can proactively send advertisement messages to consumers who may not even be aware of advertised products, instead of passively waiting for consumers' requests.

There are different approaches to enabling push-based advertising, such as profile-based push based on collected consumer preferences and usage behavior stored in consumer profiles and *location-based push* (i.e., sending advertisements to consumers based on their current location). Originally, location-based service technology was developed in the U.S. to provide emergency services for mobile phone users. In 1996, the U.S. Federal Communications Commission (FCC) mandated that all mobile phone carriers must be able to detect the geographic location of a caller by 2001 (i.e., the E911 mandate). Designed for valuable emergency or law enforcement purposes, this location tracking technology opens the door for a multitude of location-based services that take advantage of knowing exactly where individual consumers are located.

Location-Based Services

Location-Based Services (LBS) can be categorized into two types, namely location-tracking services and location-aware services. Location-tracking services are based on other parties' tracking of a user's location, and location-aware services rely on a device's awareness of its own location (Barkuus and Day 2003; Barkuus, Brown, Bell, Sherwood, Hall and Chalmers, 2008; Clark, 2004; Mancini, Thomas, Rogers, Price, Jedrzejczyk, Bandara, Joinson and Nuseibeh, 2009; Schilit, Hong and Gruteser, 2003). For example, Aalto et al. (2004) introduced a location-aware mobile advertising system called B-MAD (Bluetooth Mobile Advertising). It was based on Bluetooth positioning and WAP Push. First, a Bluetooth sensor discovers other nearby Bluetooth devices through the globally unique Bluetooth device addresses. Then, the sensor sends the addresses over a WAP connection to an Ad Server, together with a location identifier. The Ad server maps the addresses to user phone numbers and checks from the database if there are any undelivered advertisements associated with the location that have not been delivered to those users. Next, the undelivered advertisements will be sent to a Push Sender for delivery as WAP Push SI (Service Indication) messages. Restaurants in a shopping mall may automatically send en electronic coupon to a consumer's cell phone when he/she enters the mall during lunch time.

Early applications of location-based services were in the form of text messages (SMS). With the advent of unlimited messaging plans, SMS remains one of the preferred advertising choices for advertisers. LBS are becoming increasingly available because of the latest advances of technologies such as Global Positioning Systems (GPS) and cellular identification (Barkuus et al., 2008; Jorns and Quirchmayr, 2008; Pratas, Anggraeni, Wardana, Prasad, Rodrigues, and Prasad, 2009; Tsai, Kelley, Cranor, and Sadeh, 2010; Schilit, Hong and Gruteser, 2003). The new-generation GPS have been embedded in the latest smart phones to support location-based services (Jorns and Quirchmayr, 2008). Getting location information of consumers is inexpensive and requires no investment in special location equipment by the interceptor. In addition, location information is now provided at a finer granularity than ever before, and can be aggregated and used to track habits, preferences, and movements of individual consumers (NG-Kruelle, Swatman, Rebne and Hampe, 2002). By using location-centric mobile advertising based on the precise geographic location, advertisers are able to focus on a specific group of consumers and offer a range of personalized area-specific services. For example, the arrival of a highly publicized product may trigger a mobile ad for a nearby store (Renegar, Michael, and Michael, 2008). The ability to tie specific purchases to an individual allows service companies, retailers and consumer industries to build consumer profiles and conduct selective marketing.

Privacy in Mobile Advertising

In spite of its tremendous potential and benefits, mobile advertising also poses several risks to consumer privacy that may lead to negative consequences such as financial loss and damage to reputation. The existing studies on privacy issues in mobile advertising have drawn mixed propositions. Some scholars argue that people have more privacy concerns in location-tracking services than in location-based services such as 'find the nearest restaurant' services (Tsai et al., 2010; Zhang, Cui, Li, Yuan, and Wang, 2010). People are often concerned about their privacy being invaded by revealing their home addresses, or being found by someone that they do not want to see or when they want to be alone. Misuse of personal data by exposing an individual's real-time location or movements can lead to an increased invasion of privacy with negative and/or nuisance implications. For example, disclosure of location information of individuals may cause embarrassment or humiliation, or result in others to make incorrect inferences that unfairly blacken a person's reputation (Barkuus et al., 2008). In contrast, other researchers report that people are less concerned about their locations being tracked, as long as they find that the received service or product information is useful (e.g., Barkuus and Dey, 2003). Their argument is that enticed by rewards and the presumption of value, individuals are willing to compromise their privacy to gain convenience even by sharing their personal financial and preference information.

Regardless, it is important for advertisers to find solutions to protecting privacy in mobile advertising. Existing studies have proposed various methods, such as blacklist, granularity, group-based, location-based, and time-based methods (Fang and LeFevre, 2010; Schilit, Hong and Gruteser, 2003; Tsai, Kelley, Drielsma, Cranor, Hong and Sadeh, 2009), notice and consent (Barkuus and Day, 2003), and authorization by the third party (Xu, He, Wu, and Xu, 2009), to reduce the risks to user privacy. In addition, different levels of personal information access for privacy protection can be established and applied, such as family only, friends only, and public access. Due to the extremely personal nature of mobile device, Beneke et al. (2010) suggest that permission-based marketing be the foundation of mobile marketing so as to avoid the violation of consumers' privacy and a negative attitude being formed toward the advertisement and its source. The permission-based advertisement approach requires that a customer explicitly agrees to receive advertisements (opt-in) before an advertiser is allowed to send them. Consent can be interpreted as the terms and conditions by which personal information may be collected and processed to produce personal profiles for advertisement purposes. Consumers will have the option to opt-out of the receipt of further advertisment messages at any time without charge (Cleff, 2007). There is lack of research on users' privacy protection in mobile advertising from a user's perspective to date, which is the objective of this study.

Companies also have recognized the importance of adopting effective measures to alleviate user privacy concerns related to personal information collection, improper access, and unauthorized secondary usage to

help users build trust and reduce perceived risks (Park, Choi, and Jang, 2005). For example, creating privacy policies is one of the strategies for continuous consumer trust development.

Privacy Laws

There have been calls for authoritative regulations and laws for restricting service providers to collect customers' personal information randomly (Mettam and Adams, 1999; Strunk and White, 1979; Van der Geer, Hanraads and Luptop, 2000). These regulations should control not only the amount of information, but also the use of the collected information. Since 1970s, computer privacy laws have remained to be a major public concern. The ease and efficiency with which computers and computer networks can be used to share, store, search, and retrieve personal information are threatening to anyone who seeks to keep various kinds of sensitive information out of the public domain. In May 2011, the European Union adopted a new privacy rule that requires companies to obtain explicit consumer consent before delivering Internet advertisements. The e-privacy law requires anyone running a website to get user consent before deploying cookies that would be used for advertising purposes (Rashid, 2011).

The Location Privacy Protection Act of 2011 regulates that any company that may obtain a customer's location information from his or her smart phone or other mobile devices is required to: (1) get a customer's consent before collecting his or her location data; and (2) get the customer's consent before sharing his or her location data with the third parties. If any company obtains location information of more than 5,000 mobile devices, that company will also have to (3) take reasonable steps to protect that information from threats; (4) tell an inquiring customer whether or not other companies have his or her information, and (5) destroy that information if the customer requests. Customers are expected to have a baseline of knowledge about privacy issues obtained from advertiser disclosure statements, publicly available information from interested third parties, and personal experiences. Of course, this responsibility does not excuse advertisers from operating within moral tenets and expected industry norms or from developing codes of conduct and ethical behavior.

In summary, the privacy issue in mobile advertising has been receiving increasing attention from researchers and advertisers but the understanding of consumers' privacy concerns and their preferred solutions to privacy protection is still preliminary. To lessen privacy concerns in mobile advertising, marketers must be aware of privacy concerns of customers in mobile advertising. Moreover, the government should develop and deploy privacy laws or regulations to enhance privacy protection in mobile advertising.

RESEARCH METHODOLOGY

We conducted a survey that is aimed to better understand users' perceptions about privacy in mobile advertising and identify their preferred solutions to privacy protection. The survey was administered through both online and paper. The survey offered the participants a chance to understand privacy issues and solutions in mobile advertising. Furthermore, it could help improve future studies about privacy protection in mobile advertising. Because of the main objective of this study, a major qualification criterion for participants is to own a cell phone.

Survey Instruments

Research on privacy in mobile advertising is still in its infancy, and the state of empirical research on privacy protection in mobile advertising has generally lagged behind the technical development. Based on prior studies that we found, it seems that little research has been empirically and comprehensively examined all major effective factors that could affect or protect users' privacy in mobile advertising. The aim of this study is to identify and examine major factors that can affect privacy in mobile advertising, identify which factor users are mostly concerned, and then evaluate methods that can be used to protect privacy. The findings of this research will significantly advance our understanding of privacy protection in mobile advertising, and provide potential future research topics as well.

The complete survey questionnaire included demographic information (Part 1), prior experience with mobile advertising (Part 2), privacy perception in mobile advertising (Part 3), solutions to privacy protection in mobile-advertising (Part 4), and additional comments/suggestions (Part 5). Part 1 asked questions about demographics of participants, such as gender, age, education, and ethnicity; Questions in part 2 asked questions related to participants' experience with mobile advertising, such as how often they received mobile advertisement in the past, what kinds of advertisement they received, whether they viewed the content of ads, whether they purchased certain products or services recommended by mobile ads, and whether they mind receiving mobile advertisement messages on their cell phones, etc. Part 3 focused on participants' perception of privacy in mobile advertisement, which included questions categorized into three sub-sections: perceived control of mobile advertising, perceived concerns of receiving mobile advertising, and trust in privacy protection and law abidance by mobile advertising companies. We developed survey questions to measure these three research constructs. Questions were adapted and extended from existing research instruments, as shown in Table 1.

Constructs	Sources
Experience	(Yu and Cude, 2007)
Privacy perception	(Merisavo, Kajalo, Karjaluoto, Virtanen, Salmenkivi, Raulas and Leppäniemi, 2007)
Solutions to privacy protection	(Okazaki, Li, and Hirose, 2009; Yu and Cude, 2007)

Table 1. Survey Instruments Development

Questions in part 4 asked participants about their preferences on different methods for privacy protection in mobile advertising, such as permission-based mobile messages, establishing and deploying privacy laws, purpose specification, collection limitation, and use restriction. There were multiple questions in each part. Some sample questions are listed in the Appendix. All of the survey questionnaire items were measured by a 7-point Likert scale, with 1 being 'Strongly disagree' and 7 being 'Strongly agree'.

Participants

There were 40 qualified participants that responded to the survey. Among those participants, half were male; 50% were students recruited from a university at the east coast of the United States, and the rest were university employees and other adults recruited off campus; all participants owned a cell phone and 50% of them has previously received mobile ads, with 12.5% participants reporting to receive more than 10 mobile ads per month. There were 14 participants between 18 and 24 years old, 15 between 25 and 34 years old, 2 between 35 and 44, and 9 over 45 years old. More than 70% of participants had at least a bachelor's degree. Among the participants, 40% were Caucasian, 50% Asian, and 10% African Americans and Latinos.

Results and Findings

We tested the internal reliabilities of eight reflective research constructs. All of them achieved above 0.70 on Cronbach's alpha except for perceived control, trust in privacy, and use restriction. The reliabilities of these three constructs were improved to the acceptable level after removing one item from each (PC2, TIP2, and UR1), resulting in 0.70 for perceived control, 0.759 for trust in privacy, and .837 for user restriction. The statistics reported in Table 2 is based on the average of remaining items in the constructs.

Constructs	Mean [std.]
Collection limitation	6.4 [.81]
Individual participation	6.45 [.75]
Openness	6.37 [0.0]
Perceived control	6.0 [1.12]
Privacy law	5.78 [1.28]
Purpose specification	6.08 [1.22]
Trust in privacy	3.89 [1.76]
Use restriction	5.8 [1.6]

Table 2. Descriptive Statistics of Reflective Constructs

Among all the solutions to protecting privacy in mobile advertising, individual participation received the highest rating (mean = 6.45), which was significantly higher than that of privacy laws ($p<.01$), use restriction ($p<.05$), and purpose specification ($p<.1$). It shows that consumers want to take control of whether they should receive advertisements and what kind of advertisements they prefer to receive. In addition, collection limitation (mean = 6.4) was also perceived to be more important than privacy law ($p<.001$) and use restriction ($p<.05$).

Constructs	Mean [std.]
PP1	5.59 [1.5]
PP2	5.66 [1.4]
PP3	5.63 [1.2]
PP4	5.88 [1.4]
PP5	5.15 [1.67]
PM1	4.71 [1.55]
PM2	5.37 [1.58]

Table 3. Descriptive Statistics of Perceived Problems and Permission Request Frequency

The descriptive statistics of individual items of formative research constructs is reported in Table 3. As far as permission-based mobile messaging is concerned, participants preferred merchants to request customers' consent a priori each time before they send an m-ad over a one-time permission request ($p<.1$). The latter is commonly used in the current mobile advertising. Among the perceived concerns of receiving mobile advertising, the concern about the cost associated with receiving m-ads (mean = 5.15) is not perceived as important as other four types of concerns. In terms of perception of privacy, 86% of respondents felt that their privacy has been invaded if their receive m-ads from merchants that they have never heard of and/or visited. This result suggests a strong privacy concern about m-ads.

For the question "If you receive m-ads from merchants you have never heard of and/or visited, do you feel that your privacy has been invaded?", 87.5% responded with 'Yes' and provided the following reasons:

- Incoming messages are paid
- They are annoying and invasive
- I don't read text from unknown number.
- Don't like the idea of receiving ads or junk messages through my phone.
- I consider them as spams.
- I feel a mobile line should be private and not solicited.
- They look like phone solicitation
- We are bombarded by ads on roadsides, TV, internet. But I feel my phone is a necessity and should be private. I want no ads on it.

- I would like to control who can access my phone.
- I did not ask for them.

Among the rest who responded 'No' to the above question, 40% did not mind receiving m-ads if they are interesting and relevant. 48% of the respondents ignored all the m-ads that they have received; 38% clicked the m-ads only when the ads were related to the products/services of their interest; and 14% clicked the m-ads only when they were sent from companies that participants like. None of respondents read every m-ad that he/she has received. 23% of the respondents who had received m-ads purchased products/services that were advertised, such as watch, Karaoke machine, shoe, jewelry, and different applications and games for their mobile devices.

Regarding the impact of mobile advertising on participants' purchase decisions, 41% participants did not think that m-ads affected their purchasing decisions; 33% were not sure, and 21% acknowledged the influence of m-ads on their purchase decisions, but none of the participants considered that the influence would be very strong. Nonetheless, if m-ads include relevant and/or interesting information or discouts, the responses shifted to the positive side – 33% respondents agreed that their purchasing decisions could be influenced by m-ads.

DISCUSSION AND CONCLUSION

This study provides several important implications. First, results show that privacy concerns are salient and widespread for not only existing consumers who have received mobile ads before, but also for those who have not. That is why half of the respondents simply ignored mobile ads when they received ads. It indicates that addressing privacy concerns is essential and critical to increasing consumers' acceptance and trust of mobile advertisement. Failing to address those concerns could lead to ineffective advertising or even negative consumer perception of marketers or related businesses.

Second, few previous studies have probed the user perception and preference of possible solutions to privacy protection in mobile advertising. This study provides unique insights on how users feel about solutions, which may be helpful to marketers when they deploy privacy protection solutions. Our findings reveal that individual participation is perceived to be more important than privacy laws and use restriction. This is also reflected and confirmed by the reported preference of respondents in getting their consent in advance every time before an m-ad is delivered, which is different from traditional one-time permission-based advertising. It suggests that mobile advertisers should provide target consumers sufficient information and rights about the access and use of their personal information. The more informed the consumers are, the less concerns they would have about privacy intrusion in mobile ads.

Third, the respondents perceived privacy concerns to be more important than incurred cost associated with receiving m-ads, which further underlines the priority of addressing privacy concerns before reducing the cost of receiving m-ads.

Fourth, another interesting finding of this study is that respondents feel m-ads more acceptable and influential to their purchase decisions when they are relevant to users' interests. It suggests that mobile advertisements would be more effective if advertisers can know individual consumers' interest in advance so as to select/personalize/deliver only advertisement messages that are relevant to consumers' personal interests. It is worth developing research models that can better explain the influence of m-ads on purchase decisions in future research.

As the mobile market keeps growing, advertisers will continue focusing on how to best distribute their advertisements to targeted consumers. Rich media ads are expected to gain more popularity as web technologies evolve. It is also important to increase the public awareness of privacy issues in mobile advertising. Although legislation is the basis for privacy protection, we believe individual participation,

social norms, and technical means can also contribute to achieving this goal. Therefore, a combination of a legal system, privacy-enhancing technologies, and consumer education and involvement would be important to protecting consumer privacy.

REFERENCES

1. Aalto, L., Nicklas Göthlin, N., Korhonen, J. and Ojala, T. (2004) Bluetooth and WAP Push Based Location-Aware Mobile Advertising System, *Proceedings of the 2nd international conference on Mobile systems, applications, and services (MobiSys '04)*, June 6-9, Boston, Massachusetts, USA , ACM Digital Library, 1-10.
2. Barkuus, L. and Dey, A. (2003) Location-Based Services for Mobile Telephony: a Study of Users' Privacy Concerns *Proceedings of the 9th IFIP TC13 International Conference on Human-Computer Interaction (INTERACT 2003),* September 1-5, Zurich, Switzerland
3. Barkuus, L., Brown, B., Bell, M., Sherwood, S., Hall, M. and Chalmers, M. (2008) From Awareness to Repartee: Sharing Location within Social Groups *Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems (Chi '08),* April 5-10, Florence, Italy, ACM Digital Library, 497-506.
4. Beneke, J., Cumming, G., Stevens, A. and Versfeld, M. (2010) Influences on Attitude toward Mobile Text Message Advertisements: An Investigation of South African Youth *International Journal of Mobile Marketing*, 5, 1, 77-97.
5. Chen, G. and Rahman, F. (2008) Analyzing Privacy Designs of Mobile Social Networking Applications *Proceeding of 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (2008 IEEE/IFIP),* December 17-20, Shanghai, China, IEEE Computer Society, 83-88.
6. Clark, R. (2004) Taking the Privacy Challenge. *Wireless Asia*, 7, 3, 14-17
7. Cleff, E.B. (2007) Privacy Issues in Mobile Advertising *International Review of Law, Computers and Technology- Cyberspace: Who's (Should be) the King of the Castle?*, 21, 3, 225-236.
8. Coursaris, C., Hassanein, K., & Head, M. (2003). M-Commerce in Canada: An Interaction Framework for Wireless Privacy. Revue Canadienne des Sciences de l'Administration/Canadian Journal of Administrative Sciences, 20,1, 54-73.
9. Fang, L. and LeFevre, K. (2010) Privacy Wizards for Social Networking Sites *Proceedings of the 19th international conference on World wide web (WWW '10),* April 26–30, Raleigh, North Carolina, USA, ACM Digital Library, 351-360.
10. Finneran, M. (2006). Mobile Security--A Work In Progress. Business Communications Review, 36, 11, 18-21.
11. Gao, J., Cai, J., Patel, K. and Shim, S. (2005) A Wireless Payment System *Proceedings of the Second International Conference on Embedded Software and Systems (ICESS'05)*, December 16-18, Xi'an, China, IEEE Computer Society, 1-8.
12. Gao, Q., Rau, P.-L.P. and Salvendy,G. (2010) Measuring perceived interactivity of mobile advertisements. *Behaviour & Information Technology*, 29, 1, 35-44.
13. Haghirian, P. (2005), Increasing Advertising Value of Mobile Marketing – An Empirical Study of Antecedents *Proceedings of the Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05)*, January 3-6, Island of Hawaii, Hawaii, USA, IEEE Computer Society, 1-10.
14. Jorns, O. and Quirchmayr, G. (2008) A Middleware for Location-Based Mobile Applications with Privacy Protection *Proceedings of the 10th International Conference on Information Integration and Web-based Applications & Services* 2008 (*iiWAS '08),* November 24-26, Linz, Austria, ACM Digital Library, 111-116.
15. Leppaniemi, M., & Karjaluoto, H. (2005). Factors influencing consumers' willingness to accept mobile advertising: a conceptual model. International Journal of Mobile Communications, 3, 3, 197-213.
16. Merisavo, M., Kajalo, S., Karjaluoto, H., Virtanen, V., Salmenkivi, S., Raulas, M. and Leppäniemi, M.

(2007) An Empirical Study of the Drivers of Consumer Acceptance of Mobile Advertising *Journal of Interactive Advertising*, 7, 2, 1-18.
17. Mancini, C., Thomas, K., Rogers, Y., Price, B.A., Jedrzejczyk, K., Bandara, A.K., Joinson, A.N. and Nuseibeh, B. (2009) From Spaces to Places: Emerging Contexts in Mobile Privacy *Proceedings of the 11th international conference on Ubiquitous computing* 2009 (*UbiComp '09),* September 30 - October 3, Orlando, Florida, USA, ACM Digital Library, 1-10.
18. Mettam, G. R. and Adams, L. B. (1999) How to prepare an electronic version of your article, Introduction to the electronic age, E-Publishing Inc., New York, 281–304.
19. NG-Kruelle, G., Swatman, P.A., Rebne, D.S., Felix Hampe, J. (2002) THE PRICE Of CONVENIENCE: Privacy and Mobile Commerce *Quarterly Journal of Electronic Commerce*, 3, 3, 273-285.
20. Okazaki, S., Li, H. and Hirose, M. (2009) Consumer Privacy Concerns and Preference for Degree of Regulatory Control *Journal of Advertising*, 38, 4, 63-77.
21. Park, M., Choi, Y. and Jang, K. (2005) M-commerce Model by Enhanced Location Privacy Protocol in GSM *Proceeding of the International Conference on Next Generation Web Services Practices (NWeSP'05),* August 22-26, Seoul, Korea, IEEE Computer Society, 1-6.
22. Park, T., Shenoy, R. and Salvendy, G. (2008) Effective advertising on mobile phones: a literature review and presentation of results from 53 case studies *Behaviour & Information Technology*, 27, 5, 355-373.
23. Peters, C., Amato, C.H. and Hollenbeck, C.R. (2007) An Exploratory Investigation of Consumers' Perceptions of Wireless Advertising *The Journal of Advertising*, 36, 4, 129-145.
24. Pratas, N., Anggraeni, P.N., Wardana, S.A., Prasad, N.R., Rodrigues, A. and Prasad, R. (2009) Context-Aware Trust and Privacy Application for Mobile Identification System *Proceeding on Wireless Communications and Networking Conference, 2009 (WCNC 2009. IEEE*2009), April 5-8, Budapest, Hungary, IEEE Communications Society, 1-6.
25. Renegar, B.D., Michael, K. and Michael, M.G. (2008) Privacy, Value and Control Issues in Four Mobile Business Applications *Proceedings of the 7th International Conference on Mobile Business (ICMB '08),* July 7-8, Barcelona, Spain, IEEE Computer Society, 30-39.
26. Schilit, B., Hong, J. and Gruteser, M. (2003) Wireless Location Privacy Protection*, IEEE Computer Society*, 36, 12, 135-137.
27. Siau, K. and Chen, Z. (2003) Building Customer Trust In Mobile Commerce *Communications of the ACM*, 46, 4, 91-94.
28. Stafford, M.R. and Faber, R.J. (2005) Advertising, Promotion, and New Media, M.E. Sharpe Inc., Armonk, NY.
29. Strunk, Jr. W. and White, E. B. (1979) The elements of style (3rd ed), Macmillan, New York.
30. Tähtinen, J. (2005) Mobile Advertising or Mobile Marketing. A Need for a New Concept? *Proceeding of Frontiers of e-Business Research 2005 (eBRF 2005)*, September 26-28, Tampere, Finland, Google Scholar, 152-164.
31. Tao, Z. (2008) The Impact of Privacy Concern on M-commerce User Acceptance *Proceeding of The 3rd International Conference on Grid and Pervasive Computing Workshops* (*GPC Workshops '08)*, May 25-28, Kunming, China, IEEE Computer Society, 245-249.
32. Tsai, J.Y., Kelley, P., Drielsma, P., Cranor, L.F., Hong, J. and Sadeh, N. (2009) Who's Viewed You? The Impack of Feedback in a Mobile Location-Sharing Application *Proceedings of the 27th international conference on Human factors in computing systems (CHI '09)*, April 4-9, Boston, USA, ACM Digital Library, 2003-2012.
33. Tsai, J.Y., Kelley, P.G., Cranor, L.F. and Sadeh, N. (2010) Location-Sharing Technologies: Privacy Risks and Controls, Cyber Usable Privacy and Security Laboratory, Carnegie Mellon University, Pittsburgh, PA.
34. Unni, R. and Harmon, R. (2007) Perceived Effectiveness of Push vs. Pull Mobile Location-Based Advertising*, Journal of Interactive Advertising*, 7, 2, 1-24.
35. Van der Geer, J., Hanraads, J. A. J., and Lupton, R. A. (2000) The art of writing a scientific article, Journal of Scientific Communications, 163, 51-59.

36. Xu, F., He, J., Wu, X. and Xu, J. (2009) A Method for Privacy Protection in Location Based Services *Proceeding of the Ninth IEEE International Conferences on Computer and Information Technology 2009 (CIT '09),* October 11-14*,* Xiamen, China, IEEE Computer Society, 351-355.
37. Yu, J.H. and Cude, B. (2009) 'Hello, Mrs. Sarah Jones! We recommend this product!' Consumers' perceptions about personalized advertising: comparisons across advertisements delivered via three different types of media *International Journal of Consumer Studies*. 33, 4, 503-514.
38. Zhang, W., Cui, X., Li, D., Yuan, D. and Wang, M (2010) The Location Privacy Protection Research in Location-Based Service *Proceeding of 18th International Conference on Geoinformatics, 2010*, June 18-20, Beijing, China, IEEE Xplore Digital Library, 1-4.

APPENDIX: Survey Questionnaires

Perceived control of mobile advertising
PC1: It is important for me to be able to give permission to merchants to send me m-ads.
PC2: I would like to receive m-ads if I have provided my permission. *
PC3: Being able to refuse to receive m-ads would be important to me.
PC4: It is important for me to specify m-ads of my interest.

Perceived concerns of receiving mobile advertising: What is the biggest problem of receiving m-ads?
PP1: Loss of personal information control
PP2: Loss of privacy: it blurs the distinction between home, work, and leisure.
PP3: The time involved in dealing with it.
PP4: Cost associated with receiving m-ads

Trust in privacy and laws of mobile advertising
TIP1: I believe that m-ad service providers use my personal information only for a purpose that I have approved.
TIP2: I believe that laws should protect the consumer's personal information use by merchants.*
TIP3: I believe m-ad providers will not disclose my personal information to a third party without my permission.

Please indicate the importance of each of the following aspects to protect your privacy in m-ads:

Permission-based mobile messages
PM1: one-time permission requests from merchants is enough.
PM2: merchants should request customers' consent each time they send an m-ad.

Privacy law
PL1: The use of customers' personal information should be restricted to a limited time frame (example: PL2: businesses can use customers' information for a maximum of 6 months only).

Purpose specification
PS1. The purposes for the collection of personal information should be disclosed before collection.
PS2. The use should be limited to those pre-specified purposes and compatible purposes.

Collection limitation
CL1. The collection of personal information should be limited.
CL2. The collection of personal information should be obtained by lawful and fair means.
CL3. The collection of personal information should be obtained where appropriate, with the knowledge or consent of the individual.

Use restrictions
US1. Advertisers should not disclose personal information to the third parties. *
US2. Personal information should not be used for other than a specified purpose without consent of the individual or legal authority.
US3. Personal information should be allowed to be used only within a certain time frame without consent of the individual or legal authority.

Openness

OP1. The phone service providers should inform their customers about privacy policies.

Individual participation
IP1. Individuals should have the right to know about the collection of personal information.
IP2. Individuals should have the right to access personal information collected.
IP3. Individuals should have the right to request correction of imprecise or outdated personal information collected.
IP4. Individuals should have the right to challenge the denial of those rights.

* Item removed to improve reliability