International Journal of Latest Trends in Engineering and Technology
Vol.(8)Issue(1), pp.622-635
DOI: http://dx.doi.org/10.21172/1.81.082
e-ISSN:2278-621X

PRIVACY ISSUES IN WIRELESS MOBILE COMPUTING: A REVIEW

Osamah Ali Mohammed Ghaleb**, Hasib Daowd Esmail Al-ariki** and Mohammed A.S. Mosleh
Department of computer science, S.N.Rsons college, Coimbatore.
JSS Research Foundation, *Department of Electronics and Communication, Sri Jayachamarajendra College of Engineering, Mysore.*
School of IT & Science, Dr. G.R.Damodaran College of Science, Coimbatore.

Abstract: This paper aims to examine privacy issues in mobile computing technology as the main challenge that face businesses operate in such environment, due to the capability of this technology to collect a lot of personal environment consumers may afraid from an invasion of their personal privacy. Based on academic studies we will discuss the privacy challenges in different mobile computing application and how this challenge concerns mobile consumers and influence their perceptions toward accepting mobile computing applications in this environment. Numerous privacy issues are discovered, businesses operate environment should consider these issues and address various privacy issues risk their consumers. Numbers of privacy protection solutions in mobile computing environment will be discussed, businesses should adopt appropriate solutions in order to gain consumers trust and increasing their interesting; and continues compete in such environment successfully; otherwise growth of mobile computing applications will be at the risk.

Keywords: privacy, Wireless Mobile Computing.

I. INTRODUCTION

The emergence advance of wireless communication and position identifying technologies offer new opportunities to businesses to transform the traditional electronic commerce applications into mobile computing application. Deployment of positioning-based systems technologies such as Radio Frequency Identification (RFID) and Global Positioning System (GPS)and combining this technology with mobile computing devices introduce new marketing applications such as mobile marketing and location-based services (LBS) that provide great mutual benefits for businesses and consumers, consumer are able to make transactions and receive customized tailored service based on his preferences, time, location and context in convenience way; businesses also has opportunity to widely access to large number of new customers; businesses can utilize the advance in mobile communication and computing technologies and gain customer satisfaction, thus led to improving business competitive position and increasing the revenue. Mobile computing and networking developments not only provide benefits in the area of mobile commerce applications, it also used in other applications areas such as safety/emergency, healthcare, libraries,…, etc. and provide a lot of convenience benefits to users.

In the other side advanced mobile technologies LBS, mobile RFID also raise a many of privacy issues that represent a new challenges to government, businesses, and users; if these

challenges, not addresses with a possible technical and regulatory solutions to protect personal information privacy properly; it will introduce new kind of privacy risks and threats that may lead to losing of different participants trust and confidence; and thus will preclude the widespread of technology (Gadzheva, 2007).

Security, privacy, and trust are critical three related issues in mobile technology, in order to protect user privacy we must improve the security of different mobile applications if this issue was resolve next the business should consider the solutions related to the privacy of different participants properly in order to gain participants trust. Privacy is an important aspect of mobile technology in order to gain the opportunity to benefits from this emergence technology, user trust which an important factor to determine the future of this technology must be gained, so it's a feasible to invest in the privacy solutions to ensure the protection of personal privacy. In this paper our focus will be on the privacy challenges in mobile commerce applications; we supposing that the security problems can be solved by different technical and managerial solutions. We will not go into technical details related to the privacy. This paper categorized into four sections, first section will discuss in general the privacy threats and risks in mobile technology; in second section privacy challenges for different type of mobile technology used in m-commerce applications- mobile marketing, mobile RFID, and LBS- will be discusses; next section, by review different cases about using mobile computing applications we show how privacy impact the acceptance of mobile technology; next, recommended solutions to protect privacy in mobile applications will be discussed briefly; and finally we present a comprehensive summary discuss major aspect related to our topic.

Location-based Service (LBS): according to Turban, Leidner, and Wetherbe (2007), LBS defined as "the delivery of advertisements, products, or services to customers whose location is known at a given time",pp.231.

Mobile Commerce: conducting E-Commerce transactions using a combination of advance computing and communication technologies, by utilizing different position determining applications, location tracking technology using mobile phone devices, (Gura˘u and Ranchhod, 2009).

Mobile Computing: according to Gao, Sultan, and Rohm (2010), the Mobile Marketing Association (MMA) defines mobile marketing as "the use of wireless media as an integrated content delivery and direct response vehicle within across media or stand-alone marketing communications program",(MMA,2006).

Mobile RFID:"is a new application to use a mobile phone as RFID reader with wireless technology and provide new valuable services to a user by integrating RFID and ubiquitous sensor network infrastructure with mobile communication and wireless internet", (Kim and Lee,2006).

Privacy, as cited by Paolo and Langheinrich (2010), Western defines privacy as "the desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitudes and their behavior to others", Western (1967).

Radio Frequency Identification (RFID):"is a technology that is used to identify objects and users and automatically takes advantage of contextual information such as user's location is expected to become an important and a core technology of ubiquitous infrastructure." (kim et al., 2006).

II. LITERATURE REVIEW

Due to the development of mobile computing and telecommunication technologies, there are a lot of researchers studied the privacy issues which are the major challenge raises in such technology in, since the applications in mobile environment have the capability to collect a lot of personal information and utilize this information to provide different benefits to both businesses and consumer in more flexible and convenient way (Beatrix, 2007; Guraˇu & Ranchhod, 2009; Geir & Vladimir, 2007). As mobile technologies enables to provide a great benefits to both consumers and businesses, at the same time it raises a number of privacy issues that threat the consumers and the growth of this technologies, many researchers studies discussed the privacy issues that are related to collection, usage, transmission, storage, retention and disclosures of consumer information as the main challenge that make consumers afraid from usage of services mobile computing applications, such Privacy issues represent new challenges to different parties participants in providing mobile services (ex. consumers, companies, service provider,…,etc), and if this issues are not addressed may lead to losing consumer trust and risk the business of companies that violate consumer privacy (Gadzheva, 2007). Businesses that try to benefit from the use of mobile computing technologies should consider the privacy issues which are the main challenge to the growth of mobile computing applications and services (Chen, Ross, and Huang, 2008). other topics relate to privacy in mobile computing is privacy regulations as critical aspects deals with protection of consumer privacy, there are a lot of researches about privacy regulations in mobile computing environment, existing literature focus on the importance of developing privacy regulation framework and fair information practices to protect consumer rights of privacy (Nancy, 2008; Sarabdeen, 2008). As suggested by Nancy (2008), consumer privacy issues can be solved through applications of fair information practices and privacy-enhancing technologies; To protect consumer privacy in mobile computing businesses should develop their privacy own policies and adhere to privacy laws and regulations; Nancy (2008) study the European Union and the United States regulatory framework for RFID applications and their finding was as that although there are a number of lows in EU. & US. Related to protection consumer's privacy, there are still many privacy concerns are not addressed by regulations of both countries. Nancy (2008) also has studied the US. Laws which regulate direct marketing, mobile phones and consumer privacy for mobile advertising and she observed that protecting consumer privacy in the US. Are largely the responsibilities of the individuals? Although there are a number of federal lows restrict the collection and sharing of personal information, there are some exceptions in restriction policies and regulatory gaps are wide; Sarabdeen (2008) discussed the EU. Regulations to protect consumer privacy in mobile advertisements these regulations require the companies to get consent before collection personal data about users, also EU. Regulate framework to issues that breach the right to consumer privacy such as unsolicited marketing and unauthorized using of collected personal information. As suggested by Sarabdeen, businesses should adhere to EU. Privacy laws to protect consumer privacy and maintain its legality otherwise it violate consumer privacy this may make business exposure to risk and loss its image and legality.

Using academic literature, this paper will illustrate privacy challenges in various mobile applications and services, privacy impacts on mobile computing acceptance and finally discussing solutions to protect consumer privacy.

2.1 Wireless Mobile Computing and Privacy

There are a lot of literature describing the concept of privacy by different definitions but all definitions agree on the right of individuals to control how their personal information are collected and use. in the area of mobile computing privacy issues in different mobile applications are studies by many researchers (Karyda, Gritzalis, Park and Kokolakis, 2009; Chen, Ross, and Huang, 2008;Guraˇu and Ranch hod, 2009; Sarabdeen, 2008; Nancy, 2008)

and others, are discussed the privacy issues related to mobile computing applications, all of them are consider the privacy is the main challenge may effect on the success or failure of mobile technology. Since the widespread of mobile application depends directly on collecting personal information and use this information to provide superb tailored individual services, as we see collected personal information are the backbone of mobile computing applications so the success in this environment mainly depends on the protection of various individuals privacy; Sarabdeen (2008) consider the issues of privacy are a major challenge for the businesses which try to maximize the use of mobile environment for their benefit.

Next, we describe major privacy threats in the mobile computing environment; these threats may negatively affect user's behaviors toward the adoption of mobile computing applications. Protecting individuals privacy should be manage effectively by different participants in this environment.

Common privacy threats in mobile computing

The use of mobile phones as a tool to provide personal and social benefits also raise a series of threats to make the management of personal information complex process (Gura˘u & Ranchhod, 2009); according to Nancy (2008), privacy threat sources either internally or externally these threats may risk the consumer privacy and make consumer less interested to adopt mobile computing services if not addressed. Privacy threats are classified into three general areas which are:

Location tracking threats

Advance in LBS and RFID applications allow the businesses to collect information about mobile users' locations and track their movement from one location to another. In RFID applications, RFID tag can be monitored and the user location information may be accessed by unauthorized intruders and this may exposure user to risk, (Kim & Lee, 2006). Gadzheva (2007), defined other threat related to location tracking according to Gadzheva, from location information one can deduce the identity of the person, this is another privacy invasion threat since a lot of persons see their identity information as a secret.

Information collection, usage and disclosure threats

The advance of mobile positioning and location-based systems enable the marketers to collect information based on person, time and context of specific mobile user, collection of such information without the consent of mobile users is a threat may annoyance users and negatively affects their behaviors toward using mobile services (Beatrix , 2007); other threats are usage and disclosure of the collected information, according to Chen et al. (2009), collecting and using information based on user consent is a self-regulatory approach enable users to control their privacy but when collected personal information used for other purposes than those accepted by user and disclosure of such information to other parties without inform user may be considered unethical issues and compromise personal privacy

Spamming, skimming and eavesdropping threats

The advance of mobile phones and introduction of SMS and mobile web browser create new marketing channel for marketers but also generate a privacy threat to consumer represented by spamming, spam make mobile user exposure to specific viruses by hackers who attack mobile phone users, example of mobile phones spyware FlexiSPY developed by company called Vervata this virus used to monitor personal information of mobile user such as history of calls and send this information to Vervata servers and accessible by consumers via special

web sites (Guraˇuet al. 2009). Another threat is skimming and eavesdropping, transmission of personal information in wireless environment done via a wireless communication medium since information is transmitted via digital radio packets, and at this medium due wireless security problems an intruder can hacking user information and using this information in ways that harm user (Geir & Vladimir, 2007).

2.2 Privacy Issues in M-Commerce

Utilizing advance mobile applications and communication technologies enable businesses to conduct electronic commerce transaction in a mobile computing environment, mobile applications not only allow the businesses to collect personal information about users it also enhances the business capability to collect information about a current physical location of the user (SREENIVASN & Nazri, 2010). Utilizing the collected location information provides benefits to both businesses and consumers, but this information may lead to an invasion of personal privacy. The mobile commerce also raised a number of privacy threats, common m-commerce privacy threats as described by Guraˇuet al. (2009) are "unsolicited calls, MMS, or intrusive advertising on websites accessed through mobile devices; collecting information about consumer profile and/or behavior without consumer consent; incapacity to control the inclusion of personal or behavioral information in marketing databases (the opt-in/opt-out principle); and using consumer information for other purposes than those explicitly accepted by consumers".
In this section, we categorized privacy issues associated with m-commerce applications are three main areas which are location-based services (LBS) applications, mobile RFID applications, and mobile marketing applications; we try to discuss privacy issues related to each type of these applications

2.2.1 Privacy Issues in Mobile Marketing

The advance of wireless technologies in addition to the wide spread use of rich media mobile devices around the world enable businesses to offer mobile advertisement which is more convenient to user and best marketing medium, this medium offer new opportunities for advertisers to create new revenue model though mobile consumers (Beatrix, 2007). The businesses choose to transform from traditional advertisement methods to this new advertisements medium due to the availability of context, instantly, location awareness and personalization over this medium,(Sarabdeen, 2008). The advance in using mobile advertisement as new marketing model raised a number of privacy issues due to the capability of the mobile technology to collect, store, use and disclosure a massive amount of personal information, since the security and protection of the collected information are the main concerns of users, if these concerns are not addresses it may preclude the growth of mobile advertisement channel; the main challenges to advertisers is to manage this information properly and ensure the protection of consumer privacy (Nancy, 2008; Beatrix, 2007). In this section, we discuss mobile advertising privacy issues that should be considered by advertisers.

The main issue in mobile-based advertisements is the development of privacy legal framework and businesses compliance with laws this framework that should be considered to protecting mobile users privacy parallel with implementation of appropriate technologies that give user some control to manage his privacy, thus will ensure gain the benefits from the mobile marketing and at the same time increase users trust in mobile advertising technology (Beatrix, 2007).

According to Nancy (2008), there are two main privacy concerns in mobile marketing which are:"the collection, use, and disclosure of consumers' personally identifying information that accompanies mobile advertising; and the generation of unsolicited mobile advertising". To protect consumer privacy in mobile marketing Nancy, suggest the self-regulatory approach which base for fair information practice and in such practice the privacy protection becomes individuals' responsibility, fair information practice gives the mobile user the rights to receive a clear notice and agrees to the collection, use, disclosure of his personal information.

According to Beatrix (2007), the main privacy concerns in mobile advertising are sent advertisement message to mobile user without getting users consent, collect personal information about mobile users without user agreements, even user allow to business to collect information about them, businesses create profile data about each user and use this personal data in other ways that are unacceptable by user rather than the ways he or she previously agreed-on to use, and finally the disclosure of collected personal data without user knowledge or consent. All these concerns are breach mobile consumer privacy and should be addressed by advertisers properly; Beatrix, suggest to main basic principles, in addition, to complying with privacy laws and regulations in order to protect personal privacy, the first principle, company should have technologies enhance privacy this technology should enable mobile user to control and mange his personal information, second principle is that business should adopt Permission-based advertising approach, this approach give mobile user some privacy control by enabling user to consent to receive advertisement message, select what information about them to be collected, agree on the way of using his personal information and knowledge or consent on to whom his personal information business can disclose. Although there are legal issues in Permission-based advertising approach- it is a challenge to determine the level and type of mobile user consents before collecting personal information- businesses should deal with such issues.

Al-alakand Alnawas (2010) study the effect of privacy and trust concerns on intention to Purchase in mobile marketing, the context of the study was in Jordan, and they were found that in mobile SMS advertising there is a positive relationship between Permission-based advertising and intention to purchase.

Sarabdeen (2008) discussed the possible violations of right to privacy in mobile marketing, he study the relationship between the mobile advertising and privacy, according to his analysis mobile marketing is one of the success advertising techniques to generate revenue as compared with other marketing techniques; Sarabdeen, suggest use this marketing technique with care to users privacy due to high chance to consider that an advertisement may be seen as invasion of personal privacy; also Sarabdeen study the privacy regulation and the relationship between legality of the mobile marketing practices and the level of protection guaranteed in the legislation, he found that although there are number of countries were regulated the laws that regard the right to privacy in mobile marketing, companies must be compliance with this laws in order to gain the benefits from mobile marketing while they ensure their legality; the laws require businesses to gain permission from users to receive advertising messages and collection usage and storage of personal information and share this information with other parties should be consented from user, as long as companies adhere to mobile privacy laws the mobile marketing remain legal otherwise companies violate the consumer privacy and thus risk their businesses.

2.2.2 Privacy and location-Based Service (LBS)

Location-Based Service (LBS) is the next generation of mobile marketing; businesses can exploit this technology to enhance mobile advertisement which described by Sarabdeen (2008), as one of best innovative of marketing mediums which enable businesses to target customers with personalized instance messages according to their current location at any time. LBS will produce social, consumer, and commercial benefits, LBS is used for emergency purposes as well as enhanced business applications such as location-sensitive billing, traffic updates, workforce management, and asset tracking. The same technology that offers a lot of benefits also raised a number of privacy and data protection concerns due to the ability of such technology to collect, retention, use and disclose a location data and other types of personal data where users are continuously tracked. Consumer trust is a problem with technologies that detect user location in all times, according to Gadzheva (2007), privacy concerns associated with the use of Location-Based Services may ultimately prevent consumers from gaining the 'anytime anywhere' convenience. So business should consider the issues related to the protection of personal privacy in order to overcome the limitations of LBS privacy problem and gain the benefits from this technology.

Chen, Ross, and Huang (2008) are studying the major benefits and concerns in location-based mobile services, they show that the growth of applications that enable the derives developments of location-based mobile service and how companies in different countries exploit the advance of communication and positioning systems to offer a lot of services to consumers ranging from entertainments to emergency services in way that convenient to user; Chen et al. also are discussed how the developments of location-based services that are provided through different mobile devices raise a number of issues that businesses should consider to understand of consumer behavior, according to Chen et al. this issues are not technical by supposing technical limitations were solved by technology. Privacy issue was one of the three observed issues (other issues are trust and justice); Chen et al. categorized privacy issues into three area which are personal privacy "the right to control information about one's self", physical privacy "the right to limit others' access to a person's presence, body, or property" and decisional privacy "the right to make decisions for oneself, without interference from others", they discussed the concerns about to the usage, storage and transmission of different personal, physical and decisional privacy and how this issues effect on the consumer behavior to adopt the location-based services, they propose that the greater consumer concerns about each type of privacy issues led to less likely location-based services are to be adopted.

The main privacy threat in LBS technology in addition to common threats in mobile marketing is identity and location Privacy

Location information is the sensitive private information, collect location information and using and disclosure in combination with other personal information much knowledge can be deduced about the person and allow his or her location to be tracked, anytime and anywhere (Gadzheva, 2007). The deduced information about the specific person can be used in the positive way to provide benefits to this person, for example, send ads to user mobile related to the current user location and his taste, but the negative issue related to the invasion of privacy of such type of personal information. According to Geir and Vladimir (2007), the location privacy property is associated with identity privacy in the sense that to know the position of an identified entity may have much more value to an intruder than just to know that there is an unidentified entity at the same position. Location information can be linked to specific activity as described by Paolo et al. "a place is often tightly connected to an activity (e.g., a shopping mall, an office), an interest/belief (e.g., a church, a political rally), or a personal attribute (e.g., a prison, a clinic)''. Some individuals consider that tracking location

and deduced identity information are a breach of their personal privacy and may exposure them to threats.

2.2.3 Privacy Issues in Mobile RFID

Mobile RFID provides RFID service to users who use mobile devices that are equipped with RFID reader as one of RFID applications and automatically takes advantage of contextual information such as user's location (Kim & Lee, 2006).

Nancy (2008)illustrate how mobile phones equipped RFID can be used to facilitate deliver LBS and other m-advertising, this provide benefits to both consumer and businesses, mobile equipped with RFID enable communication between advertisers and consumer, according to Nancy, RFID embedded with consumer mobile combining with RFID reader placement in specific environment enable the advertisers to track consumer location, collect data about consumer behavior in specific environment and deliver advertising to consumer mobile phone, the advertisement based on current geographic location at a specific time; as we see mobile RFID is just another mobile computing application provide a lot of benefits but also raise a number of privacy concerns that should be consider by businesses of services by such kind of mobile computing technology; the privacy issues related to mobile RFID such as user tracking and usage of collected personal information and to adopt this technology in various applications, so businesses needs to develop and implement technical security solutions, develop their privacy policies and compliance with regulations related to privacy of mobile RFID in order to protect consumer privacy (Nancy, 2008).

Common privacy Threats in Mobile RFID

Kim et al. (2006) discuss a number of privacy threats in mobile RFID technology which are the following:

Location threat: with RFID tag embedded with personal mobile user can be monitored and their location may unauthorized disclosed;

Preference threat: tagged objects are uniquely identifying the characteristics of an object that may enable businesses to deduce the specific consumer preferences;

Constellation threat: "the tags form a unique RFID constellation around the person. Adversaries can use this constellation to track people, without necessarily knowing their identities", Kim et al. (2006);
Transaction threat: transaction privacy is related to identity privacy and to location movement privacy in the sense that if user movements are known then a lot of transaction information may be deduced.
Other consumer privacy risks associated with using mobile RFID to deliver LBSand mobile advertising as described by Nancy (2008) are summarized in table 1.

Privacy Risk	Explanation
Data Protection	The potential for advertisers and other third parties to collect consumers' personally identifying information from the RFID tags in their phones. However, if a read-only function is assigned to the RFID-reader in the phone and the reader does not communicate a unique identification of the phone in the process of reading a tag in the user's environment, use of the phone as a reader does not raise data protection issues because this process should not reveal any personal information.

Tracking	The potential to reveal the geographic location of the consumer by virtue of location tracking capabilities related to having an RFID-equipped phone with a RFID tag that transmits a unique Identifying a number, which may be enhanced by having a phone that has also been equipped with other location tracking technologies (e.g., GPS)?
Spamming	The increased risk of receiving unsolicited m-advertising (e.g., voice telemarketing calls, SMS or text message ads, multi-media ads, pop-up or banner ads generated by their phones). Also, the increased risk of having adware or spyware software downloaded on their phones that could be used as a mechanism to deliver spam.
Skimming & Eavesdropping	The risk that consumers' personally identifying data stored on their phones will be accessed by others without authorization or that transmission of personal data will be intercepted while it is in transit by unintended and unauthorized parties (e.g., rival advertisers, criminals engaged in identity theft or fraud).
Profiling Using Personal Data	The risk that consumers' personal data will end up in commercial data banks and be added to consumer dossiers by virtue of the ability of RFID systems to collect data automatically and to then communicate that data easily over the Internet. Effectively, a consumer may lose control of the collection and sharing of his personal data, raising the risk of identity theft and fraud.
Profiling Using Anonymous Data	The risk that data about consumers will be gathered and used to create group profiles that are applied to groups of consumers in order to generate targeted marketing to desirable groups of consumers according to the marketer's objectives. The privacy concern to consumers is the lack of transparency of the process if consumers are not given access to information about the knowledge profiles that are applied to them and that determine whether or not they are being included or excluded from receiving favorable marketing opportunities, etc.

Table 1 consumer privacy risks in mobile RFID (source: Nancy, J. When Mobile Phones Are RFID-Equipped, 2008).

2.3 Privacy issues and its Impacts on Mobile Computing Technology Acceptance

In this section we investigate different studies as studies about the consumer attitudes can affect their acceptance of mobile computing applications; we try to discover how privacy threats can affect the mobile computing growth and how it relates to the consumer acceptance of the mobile technology.

There is a number of academic literature have studied the challenges that face consumer acceptance to mobile marketing technology including trust and privacy concerns consumers (Gao, Sultan & Rohm, 2010). As cited by Al-alak and Alnawas (2010), although there are number of studies found that users acceptance to SMS advertising was high, also there are other studies found that user acceptance to SMS advertising depends on many factors some of these factors will negatively affect users behavior toward receiving SMS ads, since they

regarded that as an annoyance behavior (example of such factors is privacy regardless, since receiving SMS ads without permission and there some users considers their mobile phones as very private and personal device and they do not want their personal information to be shared and controlled by unknown entities led to annoyance among receivers). In the area of mobile computing acceptance there are limited research focus on privacy issues factors and there are no previous studies focus on privacy issues in mobile commerce and mobile marketing in the Arab world (Al-alak et al., 2010), among the few studies on mobile computing issues in the Asian countries we take three cases from Malaysia, Jordan, and China;

Sreenivasn and Nazri (2010), studied the effects of privacy and trust factor on m-commerce acceptance and usage among Malaysian consumers, there research was based on Unified Theory of Use and Acceptance of Technology (UTAUT) Model, developed by Venkatesh et al. (2003), they are used the questionnaire methodology to collect information and the scope of research was a students from various universities in Malaysia. Data are analyzed And research hypotheses related to privacy and trust factor are accepted, they found that the trust will have a significant positive effect on customer intention for the purchase of products and services; unauthorized disclosure of customer location data to third parties will negatively affect trust of m-commerce purchase of products and services; the use of unsolicited e-mail and advertising based on customer location will negatively affect trust of m-commerce; and business policies and government regulations that protect privacy of location will positively affect trust of m-commerce.

Al-alak et al. (2010), studied the impact of trust, privacy concern and consumers' attitudes on Intention to Purchase in mobile marketing field, the research was built upon Theory of a Reasoned Behavior (TRA) and the Theory of Planned Behavior (TPB), the methodology was questionnaire and the context of the study was A random sample of 10 public and private Jordanian universities students, research hypothesis focus on study the relationships between privacy factors in direct mobile marketing and intention to purchase. The finding of research showed there are existed a negative relationship between personal use, extensive advertising, privacy concern, and intention to participate and purchase intention.

Gao et al. (2010), examine the factors affects the consumer acceptance of mobile marketing, the context of the study was Chinese youth consumers. Using TAM model the effects of antecedent factors- risk acceptance; and personal attachment in addition to marketing-related mobile marketing activities- providing information; accessing content; and sharing content- as mediating factors that affects the acceptance of mobile marketing are analyzed. Risk acceptance defined as “the propensity of individuals to provide personal information in order to enter into online marketing promotions to receive gifts, enter a contest or get future discounts”. The study was found there is a relationship between the level of risk acceptance and mobile marketing activities since a high level of risk acceptance leads to higher level mobile activities related to providing information to businesses for marketing-related purposes and accessing content. They also found there is a relationship between the consumer trust and privacy concerns, such as given consumers some degree to control the disclosures of their information reduce the privacy concerns.

The result of Gao et al. (2010), the study recommended the mobile businesses to consider the risk acceptance and personal attachment as important factors have greater effects on mobile marketing acceptance, and support the effect of regular mobile phone usage on orienting consumers toward accepting mobile marketing initiatives.

2.4 Solution to Improve Consumers Privacy Protection

In previous sections, we discussed a various privacy issues in mobile communication and computing environment, as we say these issues are the main challenges to businesses that are want to maintain the benefits offered by mobile technologies and to success in widespread and compete in such environment. Individuals, privacy protection is critical importance so businesses need to consider the solutions to reduce privacy threats; solutions to protect individuals privacy in mobile computing environment are a rich research field and there are a lot of literature in different mobile computing applications areas(Beatrix, 2007;Sarabdeen, 2008; James, 2008; Karyda, Gritzalis, Park and Kokolakis, 2009; Nancy, 2008). Since our paper focus on the area of privacy challenges in mobile computing, we will not go to study privacy solutions efforts in details we try to briefly discuss the recently implemented and suggested solutions that can adopt to protect individual's privacy and reduce associated threats.

An important issue that should be considered when companies start to develop solutions to reduce privacy threats is demographic aspects, demographic factors such as culture, sex, and age affect individuals perceptions regarding privacy issues; individuals perceptions toward privacy risks differ from one individual to another and from country to another country so businesses should adopt the most effective solutions that are based on specific demographic context. The study of Gura˘uand Ranchhod (2009) about the consumer privacy issues in mobile commerce found that there is a relationship between the national environment and the consumer personal profile, and their perceptions of the privacy threats in mobile commerce and also their perceptions regard the strategies the adopt to protect their privacy. Gura˘uet al. suggested that the solution for ensuring consumer privacy protection is an interaction between three elements which are consumer strategy-individual consumers privacy protection strategy-, business practice-set of policies developed by commercial businesses to protect consumer privacy-, and national legislations developed by governments.

According to Karyda et al. (2009), the solutions need to privacy protection is not only for compliance with privacy regulations, they have considered that privacy solutions are culture-dependent and according to their suggestion as that in addition to privacy regulation, privacy protection requires different approaches such as self-regulations and privacy enhancing technologies. Nancy (2008) studied the solutions to protect consumer privacy in RFID-based mobile phones and she also recommends on adopting the same three approaches in order to protect consumer privacy.

Karyda et al. (2009)suggested set five basic information practice should be considered to implement self-regulatory approach of fair information practice to protect information privacy, according to Karyda et al. this basic practice are:

- Notice and awareness.
- Choice and consent.
- Access and participation.
- Integrity and security.
- Enforcement and redress.

Businesses should consider the above solutions, in order to gain consumers trust and gain benefits from mobile computing, companies should implement the appropriate solutions in a way that give consumers some control to manage their privacy and enable companies to safeguard consumer information privacy, otherwise, the privacy threats may preclude the growth of mobile computing technologies.

III. CONCLUSION

In our paper we discussed privacy issues in the mobile computing environment; we concentrate on consumer privacy concerns related to the implementation of mobile technologies. depends on academic literatures we examine the privacy issues in different mobile computing application, we noted that the emergence advance in mobile computing technology provide a great mutual benefits to consumers and businesses, due to the capability of this technology to collect a lot of context, time, location and preferences personal information it also raised numerous of privacy concerns that threat mobile users, manages consumers personal privacy is a challenge to businesses that want to utilize the advancement of mobile technologies. First, we show major privacy threats that concerns mobile phones users who use their mobile phones to do different commercial transactions and receive different services, these threats are classified into three types which are location threats; information collection, transmissions store, use and discloser threats; and Spamming, skimming and eavesdropping threats. Next we discussed how these threats are raised in different mobile computing applications, as it's critical application of mobile computing we focus on three different mobile commerce applications used to deliver different services to mobile users; first application we discussed is mobile marketing which utilizes the advance in mobile computing and communication technologies to advertisers to deliver commercial advertisements to mobile users as new marketing channel. Due to the need of collecting a various kinds personal information about mobile users to facilitate the delivery of mobile advertisements and services, mobile technology has the capability to do information collections and deliver services to consumers, this marketing channel provides benefits to users; such as deliver, but it also make the consumers afraid from an invasion of their personal privacy by intruders, so it's important to gain consumers trust and increase their willingness to adopt mobile marketing applications. In mobile marketing medium major privacy issues that concern mobile consumers are a delivery of unsolicited advertisings; unauthorized collections, using, and disclosure of consumers' personal information; and using personal information for other purposes than these it collected for without user consent. Second mobile computing technology that used for commercial and non-commercial purposes is location-based services (LBS), the advance in location-aware, positioning systems and mobile computing offer new opportunity for businesses to deliver various services range from emergency services to deliver tailored advertising. LBS applications used by many businesses as a next mobile marketing generation, since it has the ability to determine the current location of consumers and collect this information then it used to deliver services to consumers based on their current location, context, and preferences. Although LBS applications provide a lot of personal and social benefits, it create a new privacy threats that concern users, one of major privacy issues in LBS is location privacy; location information form a threat for users if it accessed or used by unauthorized users; also from location information businesses can deduce the individual identity which may annoyance users and invasion to their personal privacy; spamming and disclosure of location information to other parties without user knowledge it also consider a breach to personal privacy. Last mobile computing applications we discussed in our paper is RFID-based mobile, in mobile RFID, RFID tag and reader is equipped with mobile phone devices, this technology enable businesses to use a mobile devices as a tool to collect a lot of personal information about mobile users and tracking them; deliver LBS advertisings to users, thus lead to improve businesses-customers relationship and increasing revenue and growth. For now mobile phones corporations develop RFID-based mobile but this technology is not widely used and implemented to deliver different personal services, one major issue related to this technology is privacy concerns, such applications of this technology have the capability

to collect a wide range of personal information and tracking mobile users where they go, user tracking add a new threats to personal privacy of mobile users, we discussed privacy threats in RFID-based mobile in section 2.2.2 in some details. Businesses should address this privacy issues in their mobile applications, otherwise, it will lose their consumers' trust and therefore the growth of mobile technology will be slow if not fails completely. We discussed the available solutions to protect consumers' privacy in section 2.4

In section 2.3 we discussed the influence of privacy issues on mobile computing technology acceptance; we examine three studies about consumer acceptance to different mobile computing applications, we take these studies as cases to identify if there is a relationship between mobile technology acceptance and consumer privacy, these studies discussed the consumer acceptance to mobile SMS advertising, mobile marketing, and mobile commerce; the contexts of three studies was from different countries (China, Jordan, and Malaysia), from this studies we noted that there exists a relationship between consumer acceptance to mobile applications and consumer privacy, Privacy issues play role in acceptance mobile computing applications such SMS advertising and M-commerce services; since where the personal privacy protection is high to some level increase consumers trust which positively affects their attitude toward adopting of different mobile computing applications and services.

In section 2.4, we examine available solutions businesses can adopting in order to protect their consumers' information privacy and gain them trust. Business first should consider different privacy challenges we discussed in our paper, and addresses the privacy threats that related to its environment taking into account demographic context to their consumers, since demographics aspect affect the consumer's perceptions of privacy threats and also influence the strategies they will adopt to protect their personal privacy.

Security, privacy, and trust are three related aspects should be considered in businesses that implement mobile computing application, we assume security issue was solved by using technical and managerial solutions, the purpose of security systems is to protect bossiness information (including their consumers information), and maintain the information integrity, availability and consistency; implement security systems is just one step to protect consumer privacy, managing information privacy in mobile computing environment is a complex process and implementing of technical solutions alone is not sufficient to ensure consumer privacy protection. Privacy solutions can be implements as an interaction between three aspects which are technologies-enhance privacy; self-regulatory approach and governmental privacy regulation developments and implementations

Using different technologies businesses can give their consumers some degree of control over the collection, using, sharing their personal information, consumers using different notifications; consent and choice; and security control practice will reduce their privacy concerns and increasing trust.

Another issue is that businesses should develop their privacy policies relate to their consumers' privacy concerns; and finally, companies should adhere to governmental and privacy associations regulations related to protecting its consumers' privacy, in order to maintain their legality, otherwise, it lose their image and risk their businesses

REFERENCES

[1] Al-alak, A.M., & Alnawas, A.M. (2010). Mobile marketing: Examining the impact of trust, privacy concern and consumers' attitudes on intention to purchase. International Journal of Business and Management, Vol. 5, No. 3.

[2] Beatrix, M. (2007). Privacy issues in mobile advertising. International Review of Law, Computers & Technology, Vol. 21, No.3, pp. 225-236.

[3] Chen, J., Ross, W., & Huang, S. (2008). Privacy, trust, and justice considerations for location-based mobile telecommunication services. Info - The journal of policy, regulation and strategy for telecommunications, Vol. 10, No 4, pp. 30-45.

[4] Gadzheva, M. (2007). Privacy concerns pertaining to location-based services. Int. J. Intercultural Information Management, Vol. 1, No. 1, pp.49–57.

[5] Gao, T., Sultan, F., & Rohm, A. (2010). Factors influencing Chinese youth consumers' acceptance of mobile marketing. Journal of Consumer Marketing, Vol. 27, No 7, pp. 574-583.

[6] Geir, M. & Vladimir, A. (2007). Personal Privacy in the Digital World. Telektronikk Journal, Vol. 2, ISSN 0085-7130.

[7] Gura˘u, C. L. & Ranchhod, A. (2009). Consumer privacy issues in mobile commerce: A comparative study of British, French and Romanian consumers. Journal of Consumer Marketing, Vol. 26, No. 7, pp. 496-507.

[8] James N. (2008). Direct marketing, mobile phones, and consumer privacy. Federal Communication Law Journal, Vol. 60.

[9] Karyda, M., Gritzalis, S., Park, J., & Kokolakis, S. (2009). Privacy and fair information practices in ubiquitous environments: Research challenges and future directions. Internet Research, Vol. 19 No. 2, pp. 194-208.

[10] Kim, J. & Lee, H. (2006). Privacy threats and issues in mobile RFID. Proceedings of the 1st International Conference on Availability, Reliability, and Security, (ARES'06), IEEE Computer Society, pp. 510-514.

[11] Nancy, J. (2008). Direct marketing, mobile phones, and consumer privacy: Ensuring adequate disclosure and consent mechanisms for emerging mobile advertising practices. Federal Communication Law Journal, Vol. 60.

[12] Nancy, J. (2008). When mobile phones are RFID equipped-finding E.U.-U.S. Solutions to protect consumer privacy and facilitate mobile, Telecomm.Tech. L. Rev. 107

[13] F Paolo, M. & Langheinrich, M. (2010). Privacy Challenges in Mobile Location Sharing. Second International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU), Helsinki, Finland.

[14] Sarabdeen, J. (2008). Privacy and mobile marketing. 7th WSEAS Int. Conf. on Telecommunications and Informatics (TELE-INFO '08), Istanbul, Turkey.

[15] Sreenivasn, J. & Nazri, M. (2010). A conceptual framework on mobile commerce acceptance and usage among Malaysian consumers: The influence of location, privacy, trust and purchasing power. Wseas Transactions Information and Application Journal, Vol. 7, No. 5.

[16] Tuban, E., Leidner, D., Mclean, E., & Wetherbe, J. (2007). Location Based Services and Commerce. In information technology for management: transformation organizations into the digital economy (p. 231). United States of America: John Wiley & Sons, Inc.