



UNIVERSITY
OF WOLLONGONG
AUSTRALIA

University of Wollongong
Research Online

University of Wollongong in Dubai - Papers

University of Wollongong in Dubai

2008

Privacy and mobile marketing

Jawahitha Sarabdeen

University of Wollongong, jawahith@uow.edu.au

Publication Details

Sarabdeen, J. 2008, 'Privacy and mobile marketing', in M. Demiralp, W. B. Mikhael, A. A. Caballero, N. Abatzoglou, M. Tabrizi, R. Leandre, M. I. Garcia-Planas & R. S. Choras (eds), *New Aspects of Telecommunications and Informatics: Proceedings of the 7th WSEAS International Conference on Telecommunications and Informatics (TELE-INFO '08)*, WSEAS Press, USA, pp. 76-81.

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library:
research-pubs@uow.edu.au

Privacy and Mobile Marketing

DR. JAWAHITHA SARABDEEN

Department of Business

University of Wollongong in Dubai

P.O.Box: 20183, Dubai

UNITED ARAB EMIRATES

jawahithasarabdeen@uowdubai.ac.ae <http://www.uowdubai.ac.ae>

Abstract: - Mobile advertisement is one of the best marketing mediums ever invented so far. It has the ability to target the users anywhere and anytime with personalized, location based and instant messages. The amazing features of mobile marketing led the users feel that their personal property got intruded without prior permission thus creates concerns over violation of personal privacy. This article using content analysis method analyses the possible violation of right to privacy in mobile advertising. The objective of analyzing is to know the legality of the mobile marketing practices and the level of protection guaranteed in the legislation. The finding suggests that there are existence legal provisions on the issue of right to privacy and long as the businesses adhere to the laws, mobile marketing is legal.

Key-Words: - Mobile Devices, Marketing, Privacy, Business Practices, Violation, and Regulation

1 Introduction

The marketers choose to go on mobile advertisements as it has availability of context, immediacy, location awareness and personalization [1]. Marketers find these features attractive and they will be able to deliver brands in the hand of the mobile users anytime and anywhere. The mobile technology also allows the businesses to find out the reasons for the users' being there. When the businesses find out that the user is for a match or movie or concert, they could deliver suitable advertisement with additional information or discounts. It is said that the mobile device is the most popular gateway for information and that outnumbered the personal computers and televisions combined [2]. Informa Telecoms and Media expected that mobile ads could reach \$ 11 billion by year 2010. The Kelsey Group Inc forecast that spending on mobile search and display advertisements will reach \$1.4 billion in 2012 [2]. The mobile advertisement revenue increase tremendously compare to other marketing techniques. For example the mobile advertisement growth in Japan crossed 10 billion in the first 10 years of existence which never happened in any other advertising medium [3].

The mobile devices are felt as unique because it is so personal, users have the sense of possession and they are highly engaged with the contents [4]. Thus any messages sent without consent is regarded as highly intrusive into their right to privacy. The feeling of violation of privacy further aggravated with the fact their device has limited message

capacity of mobile devices due to unwanted messages they are unable to receive legitimate messages. The users in some countries have to bear the cost of receiving messages. Bearing the cost of an intrusive message fuels the issue of violation of privacy in mobile advertising. Thus this article analyses the mobile marketing practices and the user concerns of privacy violation. It further discusses the laws and regulation of privacy protection in European Union countries and the United Arab Emirates (UAE) to see level of protection for the right to privacy. The analysis is also carried out to see where the business practices of mobile marketing are inline with the legislative protection.

2 Mobile Marketing and Privacy Issues

The mobile devices have been designed to have added features like WAP 2.0 browsers and MMS support that could display media-rich advertisements. There are mobile devices with super-mega pixel camera, television, recognition technology and mobile teleconferencing facilities. The technologies have response capacities that allow the users to respond to the advertisements [4]. Thus the advertisers could allow users to opt in to receive messages or text in to vote or buy or call to get information or chat. Most of the mobile advertisements are based on search driven. It could be from declared intent or based on user's context or preference. The marketers have pull and push techniques in their advertisement campaigns. Push

type of marketing the users receive messages due to existing relationship or the user have agreed to receive the marketing materials. In Pull types of advertisements the marketing materials are being sent to mobile users on a one time basis. Pull strategy is being used more often compare to push strategy [5]. In mobile advertisement there is a value chain. The value chain consists of the advertiser, marketing agencies, enablers, content service providers, the carriers and the consumers [3]. The advertisers always analyse the size of the audience, the purity of the user profile information and the frequency of the advertisement may be sent to the customers.

The businesses found that the traditional advertising mediums like Television and Radio does not have the element of interactivity. On the contrary the mobile advertisements can make the customers participate very well with the company and thereby can easily create the element of interactivity [6]. Since the advertisements help the companies to create awareness and attitude towards a brand, they try all possible way to make sure that they reach the real customers and make the customers interacted with the businesses and their brands. In 2004 UEFA European Football Championship the Adidas International in Netherlands managed to collect about 60,000 subscribers by enabling them to download photos of athletes, short movies and providing them with real time score. With the repeated downloading the customers are very much involve with a company. This allows the company to build long brand-customer relationship. This ultimately influence the customer action related to purchasing [6]. Adidas International has successfully seen that the mobile devices create an excellent platform to strengthen customer relationship.

In addition the advertisements try to build customer loyalty, strengthen demographic data base and thereby maximize campaign effectiveness. The McDonald Fast Food Restaurant in UK carried out text-messaging campaign by offering tickets and backstage passes for UK TV Song Contest [7]. Similarly Emap youth magazine in UK make the youth attracted to its advertisements by celebrity gossip, fashion and style tips. The businesses to take full advantage of the mobile devices, try to increasingly give important to the maximization of customer satisfaction. The mobile advertisements to be successful, the businesses also try to reach the real customers and provide information with the quality. By analytically matching the users' interest with context preference, they businesses try to promote their products and services. The collecting,

storing of users' information, matching and analyzing users data and eventually sending the marketing materials are the primaries in mobile advertisements.

The issue of privacy is a major challenge for the businesses which try to maximize the use of mobile environment for their benefit. The mobile technology facilitate store, transfer, and manipulate a vast amount of data. These data could be used to describe, build and define an individual digitally. Like the Internet the use of the mobile technology generate digital footprints about a user and allow the interested parties to locate a particular user. In 2001 Ekos Poll in Canada on Business Usage of Consumer Information for direct marketing revealed that 85% percent of the respondent said that they were receiving unsolicited advertising materials. 74% expressed concern and 82% believe that their consent must be obtained before sending any kind of marketing advertisements. 61% felt that all kind of telemarketing should be stopped even if it means they miss good opportunity [8]. On a similar issue the Western European customers found the SMS based advertisements are irritating and breaching their privacy. Advertisement lasting even 30 seconds would be considered as intrusive [7].

Right to privacy is considered as the heart of liberty and it is essential for the well-being of the individual. Right to privacy not only allows the control of physical spaces but also allows controlling the personal information. The traceable, callable and reachable nature of mobile devices provided a lot of chances for violation of users' rights to privacy. The mobile communication is direct to the owner, immediate and very close to the people's daily lives. These features let the businesses to personalize their marketing content and create easy interaction and eventually causes intrusion of one's right to privacy.

3 Privacy Regulation

There is no uniform accepted definition of privacy even though many attempted to define. Judge Cooley initially had tried to give a simple definition to privacy as "right to be let alone"[9]. Warren and Brandeis in 1890 supporting Judge Cooley's definition mentioned that this right refers to one's personality that provides for the protection of the person and for securing to the individual what Judge Cooley tried to define as "right to be let alone". They further asserted that regardless of the extrinsic value of one's ideas, thoughts or creations "the individual is entitled to decide whether that which is his shall be given to the public"[10].

Other commentators defend privacy as necessary for the development of varied and meaningful interpersonal relationships [11] or as the value that accords us the ability to control the access others have to us [12] or as a set of norms necessary not only to control access but also to enhance personal expression and choice [13] or some combination of these [14]. Intrusion into the data privacy of users by the technological means is been an issue for decades and many countries have taken steps in shaping their legal framework to address the issue. The European Union drafted 2 related Directives to address this issue. They are the EU Data Protection Directive (95/46/EC) and the Privacy and Electronic Communications Directive (2002/58/EC) [15]. Consumer rights, prosperity and well-being are the core values of European Union and that is very well reflected in its rules and regulations. The European Union Commission is trying to achieve the core values while encouraging competition. Thus the legal framework given by the EU Commission tries to strike a balance between the private interest of right to privacy and the legitimate demand of businesses for personal data. These Directives were incorporated in all the member countries. The Directives requires on the company to get consent before collection personal data of the users. The consent to be effective it becomes necessary to provide full details about the company and the purposes for which the data are being collected. The law imposes a duty on the businesses when they do data collection to inform the customers how the information is going to be used and by whom. This gives the opportunity to the users to decide whether to participate in a particular marketing campaign. The Directive defines the “personal data” broadly. This broad definition enables the legislators to include new intrusive technologies. Since the mobile is not shared what ever information that could be collected are related to that particular individual. When information was collected for one purpose it is to be destroyed once the purpose is accomplished. In practice there are companies they do not destroy them rather keep them as assets and use them to offer personalized services. These activities could easily violate the provisions of both Directives [17].

Article 13(1) of the Privacy and Electronic Communications Directive allows permission based direct marketing. However, it can only be allowed in respect of subscribers who have given their prior consent as per article 13(2) of the same Directive. It further requires that the subscribers should be given option to opt-out at any time. The permission based direct marketing in Electronic Communication Directive is said to be soft approach because it

allows the businesses to send marketing materials to the existing users on similar products and services without getting prior consent. However, this right is not conferred to a third party. In order to operate in “opt-out” option the customer must be someone who bought a similar product or service. The practical difficulty would be to display the whole terms and conditions in the limited screen size. The businesses believe that personalized information could benefit both the customers and businesses. When the customers receive information relating to their interest, they may not feel that their privacy got violated.

However, the same type of information may be considered as intrusive to some others or to the same customer in a different situation. For fear of breach of privacy the users may not provide adequate data or may provide false data that in turn affect the competency of databases. The chances for violating the users’ privacy through mobile advertisements are high because mobile devices are not shared, they are always with users and the users use them very often. Thus every message sent is attended immediately that could be considered as a kind of intrusion [17]. Therefore, the Directive imposes an obligation on the businesses to get pre-consent for the collection use and disclosure of the data collected about the users or the customers. The EU Directive on Privacy and Electronic Communication, 2002 retention of personal data is illegal. If the user gives consent then it is possible to retain the personal data for future.

The “consent” to be meaningful and effective it should an “informed consent”. It is also become necessary to make the consumers aware of the terms and condition under which the personal data can be collected, processed and used whenever the businesses send any marketing materials. The user should be given an option for opt-out in processing of personal data or receiving communication. As there are varies parties involve in the mobile value chain it became necessary for the businesses to make sure that the users consented for the data collection or use when they subscribe for the service with the service providers.

For example, Emap Youth Magazine in sending the advertisements makes sure that the opt-out is there in all the messages. Once any user joins the magazine’s club, he will get the following message with the option to withdraw from the mailing list.

Congrats! Ur now part of the Bliss Txt Addicts. Watch this Space 4 Xclusive info & gossip. Can stop messages @ Ne i replying STOP.

Fig 1: Opt-Out Option

When a subscriber sent a message to drop him from the mailing list, there will be a confirmation of his request with an option to rejoin the subscriber.

U hav just sent a DROP msg, so U will not receive Ne more Bliss msgs. If U change ur mind reply REJOIN.

Fig 2: Confirmation on Opt Out

By incorporating this clear steps business could easily reach the real customers without violating the legal requirement. In addition to comply with the legal requirement Emap segmented all databases by brand, age and sex to ensure zero mistakes [18]. This practice helps the company to ensure that they are not spamming the users because both Directives prohibit unsolicited marketing or spam. It is very important for the companies to make sure that their marketing communication is solicited. If not the advertisement will be unsolicited that could violate the laws. To avoid any legal implications, perhaps a double opt-in would be better. Here the new subscriber is sent an authorization message confirming their intention to receive communication. Tapping of the consumer sensibility and lifestyle is also common in business. The business may predict that the purchaser of a luxury car might also be interested in exotic vacation, high-end sporting equipments and financial investment vehicle. Sending of mobile messages based on presumption might lead to violation of privacy. In this case the customer may not give the consent to receive any information or the consent given is only for receiving information about the luxury cars. Any other messages could violate the provision of the laws. In 2001, DoCoMo, the Japanese service provider obtained an injunction against a dating service for sending 900,000 unsolicited text messages to its I-mode users in a single hour. Similarly Verizon in USA filed an action against Acacial National Mortgage for sending thousand of wireless advertisements to Verizon's customers. The parties settled this case out of court and the mortgage company agreed to stop sending any more messages [19]. In 2007, the Irish data protection officials raided about 10 mobile phone text marketing businesses due to public complaints. The

unsolicited messages sent by these business cost the users up to 2 Pounds per text [18].

The businesses which are sending unsolicited messages will face the risk of being sued by the users, the service providers or the regulators. The unsolicited marketing not only breaches right to privacy but also passes the cost on the innocent users. Any advertisement without mentioning the terms and condition or without indicating that the information could go to the company's databases or without opt-out option or no mention of who should bear the cost will easily breach the data protection law. The opt-out will show that the percentage of people who are not willing to participate. If more users opt-out should mean that the company is spamming.

In UAE, the Federal Constitution, the Penal Code and the new Data Protection Law try to ensure that mobile users' privacy are not violated. The Federal Constitution in article 31 clearly mentions that secrecy of communication and the information of individual shall be protected. The provision could easily be applied to any kind of information or data. Thus selling, disclosure and using of private information may be considered as a violation of constitutional provision. To support this article the Penal Code in section 378 states that disclosure or use of any information or picture or view of a person's private life is a crime. Similarly section 379 states that any information received in confident cannot be disclosed without the consent of the person who imparted in confidence.

The combine effect of these provisions is that any information or data received need to be kept in private and it cannot be used or disclosed in any way without the consent of the data subject. The legal principles in these provisions are general and broad enough to cover privacy issues in mobile marketing. Thus collection, use, sell and distribution of any personal or private data could easily violate the right to privacy. Dubai, the commercial state of UAE, has two other legislation to regulate data privacy. They are Dubai Electronic Transactions and Commerce Law (No.2 of 2002) and Data Protection Law (DIFC Law No.1 of 2007). The former punishes a person who intentionally discloses any information included in records or files. The latter legislation addresses data protection issues in detail. This latter law follows the EU Data Protection Directive (95/46/EC). The provisions are similar to the 1995 EU directive which introduced "opt-in" system where consent of the users are important to collect, store and use the personal data of data subject. The "data" could include any information relating to an identifiable natural

person. Article 8 states that Data Controllers must ensure that personal data which they process is processed fairly, lawfully and securely; processed for specified, explicit and legitimate purposes in accordance with the data subject's rights and not further processed in a way incompatible with those purposes or rights.

It further states that the data collected must be adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed. An obligation is also placed to make sure that the collected data are accurate and, where necessary, kept up to date and kept no longer than for the purposes for which the personal data was collected. It provides extra protection for sensitive data. The data protection law in article 11 as in EU Directive mentions that the data controller is not allowed to transfer data to a third country if that country does not have adequate level of protection for that personal data. The law provides various right for the data subject, inter alia, right to access, right to deny collection of data and right to correct the data collected. The law also establishes a Data Commissioner to oversee the administration of the law. One of the important features in this law is Article 35. According to this article a data subject could file a case for compensation. By this provision a gap in law has been fixed because all the other laws impose criminal liability only. The major set back of the data protection law is its scope. The data protection law is adopted to regulate the companies operating within the Dubai International Financial Center and it is hoped that extension of law to other companies will bring better protection for the users.

Nonetheless the Constitutional provision on privacy and the provisions in the Penal Code could still regulate all the industries. Mobile marketers need to adhere to the existing legal framework to avoid liability. However, there exist businesses advertise their products and services. These businesses never had a relationship with the user nor the user gave consent to receive mobile marketing materials. The advertisements come with no possibility of opt-out and no mention of cost and terms and conditions. These companies are may be negligence or ignorant about the existence of law and therefore they running into risk of being suit for violation of laws.

4 Conclusion

Mobile marketing is very fascinating and interesting new medium to advertise one's products or services. This medium needs to be used with care and

diligence as there are high chances the one's advertisement could be considered as violation of users' privacy. Many countries passed laws regulating mobile marketing and that laws require the marketing companies to adhere to certain set of rules and regulation. Thereby they are trying to balance the public interest in the protection of privacy and business interest in legalized marketing. The laws generally require businesses to operate in "opt-in" framework where consent of collecting, storing and using the users or the customers' personal data is important. The information given for one purpose should be used only for that purpose and any further use should also be consented. Further in all the marketing messages the option to "opt-out" should be present and it will give a choice to a user whether to participate or not. There are companies violating the laws and trying to get the marketing materials or their brand to be placed in the hand of the consumer may risk their businesses. The violators could be sued by regulators, customers and various other parties. If they were to be held liable then it would affect the company badly both financially and in term of image and reputation.

References:

- [1] Reymond A. Boadi, Preliminary Insights into M-commerce Adoption in Ghana, *Information Development*, Vol.23, No.4, 2007, pp. 253-265.
- [2] Computerworld.com, Google Launches Mobile Advertising Plan, <http://www.coputerworld.com/action/article.>, 19 Sept, 2007, p.1.
- [3] Chetan Sharma, Sell Phones: What Will Make Mobile Advertising Tick?, <http://Chetansharma.com/sellphone.htm>. No Date, pp. 1-3.
- [4] Mobile Marketing Association, Mobile Advertising Guideline, <http://www.mmaglobal.com/mobileadvertising.pdf>, 2007, pp. 1-17.
- [5] Maria De Miguel Molina, Self-regulation of Mobile Marketing Aimed at Children: An Overview of the Spanish Case, *Journal of Theoretical and Applied Electronic Commerce Research*, Vol.2, No.3, 2007, pp. 80-93.
- [6] Fareena Sultan and Andrew Rohm, The Coming Era of "Brand in Hand" Marketing, *MIT Sloan Management Review*, Vol.47, No.1, 2005, pp. 83- 90.
- [7] Shintaro Okazaki, Mobil Marketing Adoption by Multinationals: Senior Executives' Initial

- Responses, *Internet Research*, Vol.15, No.2, 2005, pp. 160-180.
- [8] Tom Mitchinson, Privacy: It's Just Good Business, <http://www.ipc.on.ca>, 2002, pp. 1-3.
- [9] Thomas Cooley, Laws of Tort, *No Publisher*, 1988.
- [10] Warren and Brandeis, The Right to Privacy, *Harvard Law Review*, Vol.4, 1890, p. 193.
- [11] Fried, C., *An Anatomy of Values*, Harvard University Press, 1970.
- [12] Gavison, R., Privacy and the Limits of Law, *Yale Law Journal*, No. 89, 1980, pp. 421-71.
- [13] Schoeman, F., *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, 1984.
- [14] DeCew, J., *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*, Cornell University Press, 1997.
- [15] European Commission, Preserving Privacy, Protecting Personal Data, http://www.ec.europa.eu/information_society/policy/index_en.htm, 2007.
- [16] European Commission, Human Rights and Benefits, http://www.ec.europa.eu/information_society/policy/index_en.htm, 2002.
- [17] Evelyne Beatrix Cleff, Privacy Issues in Mobile Advertising, *BILETA 2007 Annual Conference*, Hertfordshire, 2007, pp. 1-10.
- [18] Gemma Hummerston, Marketers Raided for Breaking SMS Laws, *Decision Marketing*, 2007, p. 9.
- [19] Ross D.Petty, Wireless Advertising Messaging: Legal Analysis and Public Policy Issues, *Journal of Public Policy and Marketing*, Vol.22, No.1, 2003, pp. 71-82.
- [20] Peter Tarasewick et al, Issues in Mobile E-commerce, *Communications of the Association for Information Systems*, Vol.8, 2002, pp. 41-64.
- [21] Fiona Jenkins, Mobile Marketing, *Young Consumer*, Vol.1, 2006, pp. 60-63.
- [22] Eduardo Ustaran, Mobile Marketers Get to Grips with Privacy Directive, *New Media Age*, 25 Sept 2003, pp.17.
- [23] Mobile Marketing Business, Keep it Legal, <http://www.mobilemarketingmagazine.co.uk/legal/index.html>, 15 Oct 2007.
- [24] [16] Mitch McCasland, Mobile Marketing to Millennials, *Young Consumers*, No.2, 2005, pp. 8-13.