Laws on Right to Privacy in 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 and location based instant messages. The businesses utilize these features well to suit their business operations. 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 right to personal privacy. This article using content analysis method analyses the possible violation of right to privacy in mobile advertising. The analysis would seek to know the legality of the mobile marketing practices and the level of protection guaranteed in the legislation. The Laws in European Union Countries, Australia and the United Arab Emirates were analyzed for this purpose. The finding suggests that there are legal provisions on the issue of right to privacy and as long as the businesses adhere to the laws, mobile marketing will remain legal. The European Directives on data protection are very influential and many countries have followed the provisions of the Directives.

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 out numbered 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 increases tremendously as compared 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 message sent without consent is regarded as highly intrusive into their right to privacy. The feeling of violation of privacy is further aggravated with the fact that their device has limited message capacity and 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 whether the business practices of mobile marketing are in line 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. In push type of marketing, the users receive messages due to existing relationship or the users 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 than 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 analyze the size of the audience, the purity of the user profile information and the frequency of the advertisement that may be sent to the customers.

The businesses found that the traditional advertising mediums like Television and Radio do 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 involved in a company. This allows the company to build long brand-customer relationship. This ultimately influences 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 makes 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 importance 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, the 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 generates digital footprints about a user and allows 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% of the respondents said that they were receiving unsolicited advertising materials. 74% expressed concern and 82% believed 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 cause intrusion into one's right to privacy.

3 Privacy Regulation

The term privacy is from the Latin word "*privatus*" which means withdraw from public life, and or to have seclusion from the public [9]. The Oxford Concise English Dictionary defines privacy as a state in which one is not observes or distrubed by others; or - freedom from public attention. A proper definition to privacy is yet to be drawn even if there are number of people attempted to define. The

difficulty of defining privacy was expressed by one of the writes as " privacy, like an elephant, is more readily recognised than described" [10]. Privacy is recognised as a fundamental right in Article 12 of the United Nation's Universal Declaration of Human Rights 1948. Accordingly "no one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attach upon his honour and reputation. Everyone has the right to the protection ". Judge Cooley initially had tried to give a simple definition to privacy as “right to be let alone”[11]. 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”[12]. Other commentators defend privacy as necessary for the development of varied and meaningful interpersonal relationships [13] or as the value that accords us the ability to control the access others have to us [14] or as a set of norms necessary not only to control access but also to enhance personal expression and choice [15] or some combination of these [16]. Privacy ensures that no body obtains information of a person, pays attention to it, and gains access to a person. According to *Westin*, this is very important because the individual will retain the right to determine when, how, and to what extent information… is communicated to others [17]. Bloustein, E., states that right to privacy is concern about the human personality. By providing protection of privacy, individual's independence, dignity and integrity can be protected and reserved [18]. Privacy can be divided into:

1. Information or data privacy: rules concerning gathering and using personal data;
2. Bodily privacy: protection extended to drug testing and the like;
3. Communications privacy: privacy with respect to communications by telephone, e-mail, and other modes; and
4. Territorial privacy: this will govern invasions, e.g., into one’s work place.

Among all the types of privacy the information or data privacy has become one of the most crucial issues of great concern following the advances of Information and Communication Technology (ICT). More and more people use ICT to order goods and services. In the course of these activities, huge amount of private information is being generated, and that the information generated is used to build personal profiles. The ability of the technology to build up personal profile in a matter of minutes, at minimal cost deters the netizens from full utilization of the technology in particular for commerce purposes. Personal data privacy that the consumers are concerned includes individual’s claim to control the collection, disclosure and use of personal data. Information or data privacy allows the individuals to determine when, and to what extend, information about them is communicated to others.

3.1 Privacy Law of European Union

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 seeking 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. Personal data under the Directives are defined to mean “any information recorded in a document in which it can practically be processed wholly or partly by any automatic means or otherwise which relates directly or indirectly to a living individual who is identified or identifiable from that information or from that and other information in the possession of the data user including any expression of opinion about the individual and any indication of the intentions of the data user in respect of that individual. This definition includes any information or opinion of a living person who is identified or identifiable as personal data. The flaw of this definition is that it does not include other data which may be used to identify a living individual. Personal data also includes any expression of opinion about the individual and any indication of the intentions of the data user in respect of that individual. In the Hong Kong case of *Eastweek Publisher Limited and Eastweek Limited Applicant and Privacy Commissioner for Personal Data Respondent* [2000] 1 HKC 692, the court held that a photograph which was taken in a street and later published in fashion magazine is not personal data as the data user or controller has no interest in identity of the individual. It was not practicable for the identity of the individual to be ascertained by the data user on the information he held. The case may be only relevant if it is shown that it does not restrict to cases where the data subject is identifiable by the data user or controller.

The principles in article 6 are:

1. The personal data must be processed fairly and lawfully. Therefore, the data must always be obtained from the data subject directly. The collection of data using the new technology without the express consent will also be in contrary to this principle. However, article 3.2 excludes the requirement of obtaining data from the data subject directly if the data is collected for operations concerning public security, defence, State security, and the activities of the State in areas of criminal law and journalistic purposes.

2. The collection must be for specified explicit and legitimate purposes: This provision requires that the data is not to be processed in a manner inconsistent with the purpose for which they were obtained. the data user or controller not to use or process the excessive data simply because those data can be useful for future purposes. In the UK's Data Protection Tribunal in *Runnymed Community Charge Registration Officer* v. *Data Protection Registrar* held that where information is required in relation to certain individuals it is not reasonable to hold excessive information about all individual.

The case of *Innovations (Mail Order) Ltd* v. *Data Protection Registrar*, the appellant operated a mail order business. It solicited customers in varieties of way. For compliance of purchase, the details of customer's name and address were provided. The information provided was used to solicit further customers. In addition, the company made the information available to other organization for the purpose of "list broking" where this activity was not informed earlier to the consumers. The Registrar in deciding against the company held that the intended use was informed not during contract. The information came too late to the consumers. in appeal, the Tribunal upheld the decision of the Registrar and said that "list broking" purposes was not purpose which would be obvious to the data subject. Therefore disclosure of non-obvious use need to be informed well in advance. The consent obtained can be through "opt-in" or "opt-out" method. By using "opt-in" method, the consumers are required to provide positive indication to the subsequent use of their personal information. The "opt-out" method, on the other hand, requires the data subject to inform the companies that he is not consenting to the use of his data for the subsequent purposes. Even if the marketers or the companies prefer to use the "opt-out" method for the purpose of cost cutting, the "opt-in" will provide more protection for the consumers. As a normal practice of merchants, the customers will be informed of the fact that data supplied may be used for specific purposes and given the opportunity to object to this practice. However, if the data is to be used later for a non-obvious purpose, then explicit consent is inevitable.

In case of sensitive data, "explicit consent" is necessary. "Explicit consent" requires the consent to be absolutely clear. The EU Directive states that sensitive data would include racial or ethnic origin, political opinion, religious believe, (and) philosophical or ethnical persuasion, and sexual life. Eugere, Clarke, George, and Ho stated that sensitive information may include racial or ethnic origins, political opinion, membership of political association, religious beliefs or affiliation, philosophical belief, membership of professional or trade organisation, membership of trade union, sexual preference or practices, criminal record, and individual health information [19]. It should be noted that most sensitive information is readily available or known only if it is disclosed by the data subject and despite of this fact, explicit consent is necessary when that data will be collected or processed or used.

3. The data collected must be adequate, relevant and not excessive in relation to the purpose, for which the data was collected: The data users should not collect more than adequate information for the required purpose. Once the purpose of collecting the information ceases, the personal data must be erased, unless erasure is prohibited by any law. In *Community Charge Registration Officers of Runnymede Borough Council, South Northamptonshire District Council and Harrow Borough Council* v *Data Protection Registrar*(DA/90 24/49/3) , the tribunal found that whilst the holding of some additional information was permissible in certain circumstances, the holding on a database of a substantial quantity of property information obtained from voluntary answers on the canvass forms was far more than was necessary for the purpose.

4. Personal data shall be accurate and, where necessary, kept up to data: The user of information must take all reasonable steps to make the data accurate and updated. What are reasonable steps depends on the circumstances of every case.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects. According to article 7 the EU Directive sets up the appointment of a Controller who is to ensure that the data quality principles are complied with. The Controller will only allow the processing of personal data if

a) The subject consented unambiguously;
b) Processing is necessary for the performance of a contract to which the data subject is a party;
c) Processing is necessary for compliance with a legal obligation to which the Controller is subjected;
d) Processing is necessary in order to protect the vital interest of the data subject;
e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official duty; and
f) Processing is necessary for the purpose of the legitimate interests pursued by the controller or by the third party.

7. Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (article 17), and

8. Personal data shall not be transferred to a country or territory outside the European Union unless the country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to processing of personal data. Article 25 (1) is considered as the most crucial section that received criticism from various sectors and agencies. What a third country requires is adequate protection which is more restrictive than the OECD Guidelines requirement for equivalent degree of protection. The adequacy of level of protection guaranteed by a third country shall be assessed based on the circumstances. Article 26(2) states that in deciding adequacy of protection consideration shall be given to the nature of the data, the purpose, and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rule of law, and the professional rules and security measures implemented in that particular third county. The adequacy of level of protection guaranteed by a third country is to be determined by the Commission and such decision binds the member countries. The ambiguity under the Directive is whether the adequate level of protection must be satisfied by a country's overall privacy law or particular categories of specified personal data.The Directive under article 26(1) also listed down circumstances in which the transfer of data may be allowed even if there is no adequate protection. The circumstances are:

a) The data subject consented unambiguously,
b) It is necessary for the performances of a contract between the data subject and the controller or the implementation of free contractual measures taken in response to the data subject's request,
c) It is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party,
d) It is necessary on important public interest ground or for legal claims, and
e) It is necessary to protect the vital interest of the data subject.

It is to be noted that the above mentioned circumstances should only be used to the benefit of the data subject rather than to a third country data user.

From the above discussion it is clear that the Directives require 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 device is not shared whatever 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 [19].

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, and that could be considered as a kind of intrusion [20]. 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 states that retention of personal data is illegal. If the user gives consent then it is possible to retain the personal data for future use.

The "consent" to be meaningful and effective, it should be an "informed consent". It also becomes necessary to make the consumers be 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 various parties involved in the mobile value chain, it has become 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. 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. By incorporating these clear steps, businesses 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 [21]. 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, and 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 her 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 thousands 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 [22]. 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 businesses cost the users up to 2 Pounds per text [23].

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 indicting 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, it should mean that the company is spamming.

3.2 Privacy Laws in Australia

The regulation of right to privacy in Australia is available through public sector and private sector laws. The Privacy Act 1988 and related regulations address the privacy issues in the public sectors However, to protect the right to privacy, the common law in Australia cannot be of much use since 'right to privacy'was not recognised even if it may protect data in other ways, for example, information given in a 'secret' commercial context. It should be noted that lately there has been judicial activism in Australia that recognises some level of protection for privacy violation. The Constitution is

entirely silent on the matter of privacy. The Commonwealth Privacy Act 1988 applies the 11 Information Privacy Principles (IPPs) to all Commonwealth Government departments and the Government of Australian Capital Territory (ACT). The Privacy Act 1988 protects personal information held by the Federal Public Sector. Section 14 of the Privacy Act 1988 sets out very detailed information on privacy principles that are briefly discussed as follows:Principle 1 requires that personal information must not be collected by unlawful or unfair means. The information must be collected for the purpose that is lawful and directly related to a function or activity of the collector. Principle 2 ensures that the collector of personal information takes necessary steps to make the data subjects aware of the purpose for which the information is being collected. However, this principle is not applicable if the information is obtained indirectly from a third party or provided on a voluntary basis. The duty of the collector to make the data subject aware of the purpose for which the information is collected must be performed before the information is collected. According to data principle 3 a collector who collects information through a process of solicitation shall take reasonable steps to ensure the information collected is relevant, up to date and complete. The data principle 4 imposes an obligation on a record-keeper to ensure the protection of the record against loss, unauthorised access, use, modification or disclosure, and against other misuse. If the information is required to pass on to a third party, all reasonable steps must be taken to prevent unauthorised use or disclosure of information contained in the record. According to Principle 5, a record keeper is to take steps to enable the data subject or any other person, to ascertain whether the record-keeper has possession or control of any records containing personal information. The record-keeper shall make the information collected available for inspection by members of the public. Principle 6 states that a record-keeper has possession or control of a record that contains personal information; the individual concerned shall be entitled to have access to that record. Principle 7 imposes an obligation on the record keeper to ensure the accuracy, completeness, relevance and currency of the information. The record-keeper is required to make appropriate corrections, deletions and additions to ensure that the record of personal information confirms with this obligatory principle. According to the 8th principle, a record-keeper who has possession or control of personal data shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date and complete. Principle 9 states that a record-keeper who has possession or control of a record that contains personal information shall not use the information except for the purpose to which the information is relevant. The 10th privacy principle prohibits a record-keeper from using the personal information obtained for a particular purpose or any other purpose. This principle is not applicable, if the individual concerned has consented to the use of the information for that other purpose or it is required or authorised by or under law. Principle 11 prohibits a record-keeper from disclosing the information to a third party unless the certain conditions set out as below are satisfied.The Privacy Act 1988 requires "consent" from the data subjects before their information can be collected, stored or used. The Office of the Privacy Commissioner commenting on the requirement of "consent" stated that the consent of the data subject to be valid the data subject should be informed specifically and the consent given must be voluntary. Some argue that meeting these tests of informed consent places too much of a burden on organisations. In the event that required consent is given by the data subject for collection, use or disclosure of information, the data user should employ additional safeguards to protect the information from unrelated uses or disclosures. Safeguard could include prohibitions on using the information for other purposes without the individual's consent and strict accountability measures. The data protection principles give the data subject a sense of security as regards to the protection of personal information. Section 5 of the Act provides that each Information Privacy Principle shall be treated as if it were a section of this Act and section 16 of the Act states that an agency shall not do an act, or engage in a practice, that breaches an Information Privacy Principle. Breaching any of these principles would mean an interference with privacy. It is acknowledged that none of these principles can be followed in every situation. The Privacy Commissioner instructs organisations to take all 'reasonable steps' to follow them. The Act established the Office of Federal Privacy Commissioner, who will administer the Act, promote privacy, and give policy advice to government, monitor compliance, and make binding order, including giving compensation to injured parties.

The private sector is regulated by the Privacy Amendment Act 2000. It covers personal information or opinion that can identify a person. It

ISSN: 1109-9526 Issue 5, Volume 5, May 2008

provides special protection for sensitive information. However, it applies to information that is recorded in some form, which can include an electronic record. Sensitive information are information about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a profession or trade association, membership of a trade union, sexual preferences or practices, criminal record or health information [24]. The Privacy Amendment Act 2000 introduces the co-regulatory approach. This approach is intended to foster industry-developed codes, but there will be underpinned by legislation that will establish key privacy principles that will serve as a default framework in the absence of industry codes. As a rule, most organisations in the private sector will be required to either adopt a code or comply with the legislative privacy principle. The legislation seeks to set reasonable consistent privacy standards. Meanwhile it tries to give businesses the flexibility to develop an approach to privacy protection that is relevant to their day-to-day practice and that meets community expectation about the handling of personal information. The Privacy Amendment Act 2000 was extended to private organisations through Privacy Amendment (Private Sector) Act 2000. It requires organisation and private sectors to develop their own codes of conduct regarding privacy, which will then be approved by the Federal Privacy Commissioner. However, once it has been approved the code will replace the National Privacy Principles for those organisations bound by the code. The Commissioner can revoke a code. The code can include its own complaint handling mechanism, if it does, it must provide for the appointment of a code adjudicator to determine complaints. It is believed that a code that incorporates complaints handling mechanism can give industry a sense of ownership. If a code does not provide for a complaint handling mechanism, the Office of Federal Privacy Commissioner will handle complaints and the Commissioner will be the code adjudicator [25]. The Act 2000 introduces the National Privacy Principles (NPPs) that aim to deliver, *inter alia*, promotion of greater openness between businesses and users. They cover the whole information lifecycle from collection to storage, maintenance, use and disclosure.Under the law, the mobile marketers can only collect information if the customers or users have given consent. The customers' consent can be reasonably considered as implied as long as it is clear to them the reason for the collection. It may be necessary to the businesses to advise the customers about how the information will be handled. The customers will have access to the information collected. He may look at the information, obtain a copy of the information, take note of the information, listen to the information, and get an electronic copy of information stored on a computer system or a database.This Privacy Amendment Act 2000 gives individual a right to know on what information an organisation holds about and a right to correct that information if it is wrong. By this Act consumers have the right to know the reasons for collection of their personal information by private sector. They will also know the kind of information it holds about, the usage and the parties who will get the information. Consumers can also make a complaint if they think that their information is not being handled properly. Some of the privacy principles like data security and data quality will be applied to organisations that already hold data when the Privacy Amendment Act 2000 is implemented.The Privacy Amendment Act 2000 regulated the way private organisations can collect, use, keep secure and disclose personal information. This gives a right to know why a private sector organisation is collecting one's personal information, what information it holds about him, how it will use the information and who else will have access to that data. The Act covers private sector "organisations which includes businesses with annual turnover of more than $ 3 million [26].

Privacy regime in Australia has taken almost every effort to ensure data privacy protection for the public and private individuals and organisations. Continuous reviewing process of the relevant rules and regulations, and redress mechanisms are in operation as it endeavours to be comprehensive and competitive in the region. Apart from the legislative assurance of consumer data under the privacy legislation, there are various guidelines on the collection, use and disclosure of personal data for various purposes. Australia has set of rules and regulation in place so that the public trust on new technology and related activities can be expected to be moving smoothly.

3.3 Privacy Law in UAE

In UAE, the Federal Constitution, the Penal Code and the new Data Protection Law seek to ensure that mobile users' privacy is 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 confidence cannot be disclosed without the consent of the person who imparted in confidence.

The combined 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, selling 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 getting consent of the users is an important prerequisite 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 (DIFC) 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 are businesses that advertise their products and services freely. 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 may be blatantly negligent or ignorant about the existence of law and therefore they are running into risk of being sued 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 that an 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 seeking 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 as it will give a choice to a user whether to participate or not. Companies violating the laws and trying to get the marketing materials or their brand to be placed in the hand of the consumers may risk their businesses.

ISSN: 1109-9526 Issue 5, Volume 5, May 2008

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] Raymond, W., *Keywords: A Vocabulary of Culture and Societ*y, London: Fantana Press, 1978.

[10] Young, J.B., *Privacy*, John Wiley & Sons, 1978.

[11] Thomas Cooley, *Laws of Tort*, No Publisher, 1988.

[12] Warren and Brandeis, The Right to Privacy, *Harvard Law Review*, Vol.4, 1890, p. 193.

[13] Fried, C., *An Anatomy of Values*, Harvard University Press, 1970.

[14] Gavison, R., Privacy and the Limits of Law, *Yale Law Journal*, No. 89, 1980, pp. 421-71.

[15] Schoeman, F., *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, 1984.

[16] DeCew, J., *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*, Cornell University Press, 1997.

[17] Westin, A. *Privacy and Freedom*, Anthenum Press, 1963.

[18] Bloustein, E., Privacy as an Aspect of Human Dignity, *NYUL Rev*, No. 39, 1964, pp 971-980

[19] Eugere, Clarke & George, H., Privacy in an e-Business World: A Question of Balance, *Journal of Law and Information Science*, Vol.l No.1, 2000, pp. 5-11

[17] Hewett, W.G. & Whitaker, J., Data Protection and Privacy: The Australian legislation and its implications to IT Professional, *Logistic Information Management*, Vol 15, No. 5/6, 2002, pp 369-376.

[18] European Commission, Preserving Privacy, Protecting Personal Data, *http:// www. ec.europa.au/information_society/policy/index_en.htm*, 2007.

[19] European Commission, Human Rights and Benefits,*http://www.ec.europa.au/information_society/policy/index_en.htm*, 2002.

[20] Evelyne Beatrix Cleff, Privacy Issues in Mobile Advertising, *BILETA 2007 Annual Conference*, Hertfordshire, 2007, pp. 1-10.

[21] Gemma Hummerston, Marketers Raided for Breaking SMS Laws, *Decision Marketing*, 2007, p. 9.

[22] 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.

[23] Peter Tarasewick et al, Issues in Mobile E-commerce, *Communications of the Association for Information Systems*, Vol.8, 2002, pp. 41-64.

[24] Office of Federal Privacy Commissioner, *http://www.privacy.gov.au* , 4 May, 2008.

[25] Malcolm C., Privacy Amendment (Private Sector) Act 2000, www.privacy.gov.au., 4 June, 2008.

[26] Caslon.com, Caslon Analytics Profile: Australian Privacy Regimes 2006, *http://caslon.com.au/austprivacyprofile3.htm*, 30 May, 2008.

[27] Jawahitha, S., Personal Data Protection Bill: Implications for E- Consumer Data Privacy in Malaysia, *WSEAS Transactions on Business and Economics*, Vol. 3 No.6, 2006, pp. 504-509

[28] Fiona Jenkins, Mobile Marketing, *Young Consumer*, Vol.1, 2006, pp. 60-63.

[29] Eduardo Ustaran, Mobile Marketers Get to Grips with Privacy Directive, *New Media Age*, 25 Sept 2003, pp.17.

[30] Mobile Marketing Business, Keep it Legal, *http://www.mobilemarketingmagazine.co.uk/legal/index.html*, 15 Oct 2007.

[31] Angela M. and Noor Raihan A. H., An Agent Based Approach to Procurement: A Review, *WSEAS Transactions on Computers*, Vol. 6 No.7, 2007, pp. 1013- 1019.

[31]Noor Raihan A. H., G Michael M. and Ali K., Retaining Online Consumers: Evidence from South East Asia, *WSEAS Transactions on Systems*, Vol. 6 No. 3, 2007, pp. 541-548.

[32] Mitch McCasland, Mobile Marketing to Millennials, *Young Consumers*, No.2, 2005, pp. 8-13.