BILETA
British & Irish Law, Education and Technology Association
2007 Annual Conference
Hertfordshire 16-17 April
UH

Privacy issues in mobile advertising

Evelyne Beatrix Cleff
Department of Law, Aarhus School of Business, Aarhus University
Email: EBCL@asb.dk

Abstract

The emergence of the wired Internet and mobile telecommunication networks is creating new opportunities for advertisers to generate new revenue streams through mobile users. As consumer adoption of mobile technology continues to increase, it is only a question of time when mobile advertising becomes an important part of marketing strategies. The development of mobile advertising, however, will be dependent on acceptance and usability issues in order to ensure permission-based advertising. Growing concerns about the protection of the users' privacy have been raised since mobile advertising may become extremely intrusive practices in an intimate personal space. This article focuses on the evaluation of legal problems raised by this novel form of advertising. It is assumed that a technological design, which is in line with the legal framework, will ensure that the benefits of mobile advertising and the consumer willingness to accept mobile advertising will increase.

Introduction

The end of the 20th century and the beginning of 21st were characterised by rapid developments of communication tools. The e-commerce hype has barely subsided, and the focus has already moved on to the mobile Internet. The new technology changed the world by revolutionising communication: Mobile computing technology as a communication tool was initially limited to voice telephony. However, due to digitalisation and the consolidation of telecommunication networks and Internet technology, mobile devices have evolved to full-scale Internet-enabled computers (Dagon et al., 2004). The convergence of those technologies provides endless possibilities for mobile computing applications and usage.

The emergence of the above described technologies has paved the way for mobile advertising (m-advertising) to become an increasingly important element in the marketing mix (Leppäniemi et al., 2004). The unique features of handheld devices, including their mobility, personalisation and location-awareness are the basis to deliver spontaneous, direct, interactive and/or targeted communications at anytime, anywhere (Kurkovsky & Harihar, 2006). The question, therefore, is not "if" but "when" will m-advertising become commonplace on mobile devices (SkyGo, 2003).

Unfortunately, the same technologies that bring all the benefits also raise a lot of privacy and data protection issues due to their capability to collect, store, use, and disclose a lot of personal information (Gratton, 2002). The emergence of personalised and location-based m-advertising, unless carefully monitored, may become an extremely intrusive practice. The possibility to utilize personal and location information in order to create customised and personalised advertising messages can easily assemble detailed user profiles. Mobile users can easily be identified through the access to their demographic data, location information, calling patterns, etc. While m-advertising may provide some benefits to consumers, the privacy risks have to be considered and appropriate data protection and privacy safeguards must be guaranteed. If consumer concerns about privacy are not addressed, the growth of m-advertising may well be jeopardised by the same lack of consumer trust that has discouraged the growth of email marketing.

Although data protection rules are relatively well established within the European Union (EU), the dynamics of the Information Age lead to a gap between the law and business practices within the digital world. Problems arise when the regulation of data protection clashes with commercial practices to maximise advertising via mobile technologies. There remain open issues, such as the level and type of consent required before the collecting of personal data as well as the sending of unsolicited m-advertising. Individuals must determine for themselves the circumstances and extent that information about them is collected and processed as well as being able to determine the frequency of received advertisements. Without the ability to

control access and distribution of personal data, privacy cannot be protected. Consequently, there is a need for technical solutions that could help mobile users to retain some privacy which must be implemented in conjunction with legislative efforts (Lahlou et al., 2005).

The success, however, is dependent on the development and execution of legislative and industrial initiatives. The law should facilitate and enforce an adequate choice mechanism. The translation of privacy laws into business practices will, on the other hand, be a great challenge for industries that will have to develop privacy-enhancing solutions enabling for informed consent. From this follows that in the mobile world, privacy is not simply a question of legislative compliance, but also one of solid business practices and technical solutions in order to avoid unsolicited m-advertising.

Mobile advertising

Background

Although there are various definitions for the concept of m-advertising, no commonly accepted definition exists. This is because not much research is done in the area of m-advertising. In the underlying article m-advertising is referred to the sending of electronic advertisement (mobile ads) to consumers carrying mobile devices. M-advertising is regarded by many as one of the most promising and profitable business opportunities amongst mobile computing applications. A recent mobile marketing survey suggests that about 7% of the mobile users would be willing to receive mobile ads *"if they were relevant"* (Ask et al., 2006). Unlike personal computers (PCs), mobile devices typically are not shared among people, which allows for precise targeting of advertising to a single person (1967, Petty Ross, 2003). Moreover, mobile users rarely leave their home without their device and use them frequently throughout the day. As a result a message sent to a mobile device commands the immediate attention of the mobile user and maybe perceived as intrusive if the message is unanticipated.

M-advertising is inexpensive and novel, and can be highly targeted towards a certain individual. The potential of mobile devices as direct marketing tools has not gone unnoticed and advertisers have realised the opportunity to use the mobile channel to 'text' information to targeted consumers. Unlike traditional print, TV, or even email advertising, companies can now reach specific consumer groups or even individuals, virtually anywhere, anytime, and based on the physical location of the mobile user. In addition, companies have more knowledge about their client pool than ever before. This provides businesses with the opportunity to reach their prospects when and where it is most appropriate for the effectiveness of a marketing campaign. M-advertising could most likely become a very powerful new marketing tool enabling businesses to customise and personalise advertising for mobile user (Gratton, 2002).

In addition to branding opportunities, advertisers can also employ a variety of response mechanisms. This is possibility due to the ability to send text (SMS), picture, audio or video messages to the user directly from the phone. Conceivable campaign types are 'quick service restaurant ad with click for coupon', 'retail store ad with sale info', airline ad with online registration', to name some examples (MMA, 2006). In addition to the above mentioned benefits of personalisation and location-awareness it is therefore also possible to send interactive communications.

Distinction must be made between advertising messages based on a 'push' as opposed to a 'pull' campaign (Leppäniemi et al., 2004). This has primarily an impact on the legal evaluation. Push advertising involves the sending of messages to the mobile user. Such messages may be unsolicited in the case where the user receives a message in the context of an existing relationship, but solicited where users have agreed to receive advertisements on their mobile device. Pull advertising, in turn, is any advertisement sent to the mobile user upon request on a one-time basis (e.g. a weather forecast).

Currently, mobile phones are often characterised by limited user interface and graphical visualisation on the screen. This will change with the spread of improved and advanced mobile devices. Mobile phones have already evolved from 'walkie-talkies' to full-scale Internet-enabled computers while becoming more powerful in terms of processing power and software equipment. Moreover, the devices will soon be equipped with Global Positioning System (GPS) and radio direction-finding technology. They are on the way to displacing pagers and personal digital assistants (PDAs), as mobile phones merge into a single unit with interactive large-screen format that is more subservient to advertising (Dagon et al., 2004).

Greater data collection

Content sent to a mobile device is most valuable to consumers when it is personalised. Therefore, businesses may seek to collect large amounts of highly personal information. As with surfing the wired Internet, users' browsing patterns on the wireless Web may be monitored and traced to individuals (Geradts & Sommer 2006). Since a mobile device is normally owned by a single person, the way the device is used, the kind of data downloaded and the phone numbers called can reasonably be assumed to represent the interests and activities of an individual.

The greater the knowledge about personal information, the greater the capability to generate detailed personal profiles linked to the individual. It is obvious that online shops need some data for doing business with a customer. This so-called primary use of data, where the objective is clear, is a natural prerequisite for doing so (WP15.1, 2005). However, businesses may use personal data beyond the original purpose in order to offer personalised services. Hereby, the use of data is made for individual transactions, and the personal profiles that are stored, processed and accumulated by other data are used to predict customer preferences. This gives companies the opportunity to literally place a brand in a consumer's hand.

The determination of location of mobile devices is a natural prerequisite for their functionality in mobile networks. Network providers need to be able to track their customers' devices in order to enable call handoffs, regional roaming, and customer billing (Gow, 2005). The new era of tracking technologies, however, offers much higher resolution in tracking the physical location of mobile users allowing for commercial business practices. These technologies enable monitoring of the precise location of the mobile user whenever the device is turned on. At this point, it is advisable to mention that location data itself cannot be regarded as personal data per se but its use and disclosure in conjunction with other information about the user could produce personal profiles for commercial purposes (Gow, 2005).

By means of the collected data, service providers can make a use of static (demographic and psychographic data) and dynamic (collection and processing of movements over time) profiles. The portability of mobile devices and the ubiquity of their applications, coupled with the possibility to locate the user and to reveal the information to others, could produce a data profile where the everyday activities and movements of the users are tracked and recorded (Gratton, 2002). Each time a user response to an m-advertising his profile may be updated with the specific content related to his actions. Moreover, once a profile has been established, the consumer may be defined, analysed, etc. at any time. Thus, m-advertising requires extensive profiling, and managing a user profile is an ongoing process. Basically, the key task of building a customer profile is customer identification. The more knowledge the advertiser has about a mobile user the greater the capability to establish a detailed personal profile.

Privacy Issues

M-advertising campaigns must address a number of public policy concerns, such as privacy and confidentiality, before their full potential can be realised. Irrespective of how well advertising messages are designed and how many additional possibilities they provide, if mobile users do not have confidence that they will protect their privacy, this will hinder their widespread deployment (Kalakota & Robinson, 2001).

This section will only discuss privacy concerns raised by m-advertising.

Privacy concerns

Information stored in databases may, on the one hand, enable advertisers to send helpful information to mobile users, but on the other hand, will also enable companies to build a very detailed record of a mobile user's past preferences, current activities, and future plans (Gratton, 2002). Personalised services could satisfy both customers and businesses. However, an m-advertisement delivered to a mobile user supposedly at the right place in order to make the message relevant, could be very intrusive if the message is unanticipated by the user. Privacy is thus a complex concept. An acceptable use of private information in one situation may be an unacceptable invasion of privacy in another. Consumers differ in their tolerance for unsolicited commercial communication: consumers rather tolerate communications pertaining to products and services in which they are interested as opposed to products and services in which they have little interest (Petty Ross, 2003). Unanticipated advertising messages, commonly referred to 'mobile spam', are considered to be a form of privacy violation (Gratton, 2002).

Once a data profile has been established, the consumer is defined as available for the market (i.e. advertising) even when his "real" self is absent (Zwick & Dholakia, 2004). These practices may lead to an

over-collecting of personal data without the proper implementation of personal data privacy, such as providing a set of standards governing the collection as well as the use of personal data and addressing issues of privacy and accuracy. Mobile users are providing passive and constant access to personal data through the use of mobile devices. They may be unaware of who has access to this data, how persistent the data is, or how data mining techniques are deployed to integrate data across a range of systems. Once personal data is used without the knowledge or consent of the consumer, privacy clearly is compromised. Furthermore, it is important to consider that in the case of mobile telephones, the perception of intrusion and invasion in the private sphere is greater than in the case of other means of communication.

From a consumer's perspective, services such as personalised advertising come at a price, as they give away some power by disclosing some personal data. The risk of losing individual freedom is increasing. Consumers may react to this problem by restricting the information they make available about themselves, by declining to disclose requested data, or simply by providing false information (O'Connor, 2005). Consequently, privacy fears may not only be limiting the growth of m-advertising, but may also be affecting the validity and completeness of customer databases and profiles, leading to inaccurate targeting, wasted effort, etc.

Addressing privacy concerns

Irrespective of how beneficial the above-mentioned technologies may be, without adequate privacy protection they have the potential to create an environment of profiles, blacklists, and constant surveillance of people that may affect their behaviour. Basically the emergence of new business practices calls for a regulatory framework that is tailored to the specific challenges and unique requirements of m-commerce (Merry, 2004).

However, due to the dynamics of the Information Age and the novelty of the existing regulations, there remain open issues, such as the level and type of consent required prior to the processing of personal data and the sending of advertising messages. Moreover, because of the complexity of the regulations, businesses may not comply with the rules. There is a need for appropriate technology to protect personal data in the digital world in order to provide users with a clear, integrated opportunity to manage and control their personal information. The concept of privacy has been defined in terms of control over the disclosure of personal information in order to ensure an effective right for privacy. Westin (1967), for example, defines privacy as "*the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"* (p.7).

Permission-based advertising may, on the one hand, establish the legal ground for the control of personal data. However, it is one of the most fundamental challenges that mobile communication services present to current legal frameworks and initiatives. Consent can be interpreted as the terms and conditions by which personal information may be collected and processed to produce personal profiles for commercial purposes. These terms and conditions have significant implications for personal privacy and the future development of mobile data services (Gow, 2005). In order to obtain consent, businesses must make the terms and conditions of the use and disclosure of the personal data available to the consumer. The consumer, in contrast, must understand the facts and implications of an action to be able to make informed choices about such practices. Moreover, mobile users should have the possibility to revoke their consent for both, the processing of personal data and the receiving of further communication.

Regulation

Nevertheless, as will be analysed in this section, the conditions of consent are much more difficult to establish. This is because the protection of privacy must be achieved in combination with a number of efforts. Legislation is certainly the basis for privacy protection; however, social norms, business practices, and technical means can also contribute to this goal (Camponovo & Cerutti, 2004). Therefore, a combination of a legal framework, privacy enhancing technologies and consumer education may be important components of protecting consumer privacy.

General principles

On EU level the development of communication technology is seen to be a vital element in stimulating future economic growth, and to promote further integration (European Commission, 2007). Therefore, the European Commission (EC) tries to establish a common framework of rules and practices which is in line

with the purpose of EU law, namely to encourage competition, to improve the functioning of the Internal Market, and to guarantee basic consumer interests (e.g.: Directive 2000/31/EC, art. 1(3)).

These legal frameworks are implemented in the form of fair information practices which is, according to O'Connor (2005), a principle that attempts to *"balance the privacy interests of individuals with the legitimate need of business to derive value from customer data"* (p. 352). Within the EU, the legal framework sets the condition for the processing of personal data and offers individuals the right to maintain control over their data. The data protection principles are relatively well-established and documented in two main directives: The EU Data Protection Directive (95/46/EC) protecting individual informational privacy and the Privacy and Electronic Communications Directive (2002/58/EC) regulates privacy and data protection issues as a result of new online marketing practices by requiring permission-based advertising.

The core principle of the directives, which shall guide the development of privacy policies, is to guarantee the mobile user to be able to make an informed choice. The user should be informed about the applied information practices and have the opportunity to choose whether or not to disclose personal data and to receive m-adverting. From this follows there are two types of consent required: First is the need to consider the consent of the mobile user to being tracked for the purpose of receiving m-advertising. Second, consent may be given prior to receiving advertising messages on a 'push' basis. The latter procedure aims to avoid the spam issue.

Requirements according to the processing of personal data

Marketers must comply with a number of information requirements prior the processing of personal data. This is seen to be a necessary condition to guarantee the data protection rights to the persons concerned. The data protection Directive (95/46/EC) defines in Article 2(h) the 'consent of the receiver' as *"any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".* From this it follows that that meaningful consent can only be obtained if the user is aware of the whole situation. Thus, before a company starts using personal data of a mobile user an effective disclosure must be provided.

In order to ensure transparency, the advertiser must provide his name and address, the purpose of the processing, the recipients of the data, and all other information required to ensure that the processing is fair (Directive 95/46/EC, art. 10 and 11). The law also requires that the mobile user gets information about the right to access, rectify and delete all personal information during the m-advertising campaign (Directive 95/46/EC, recital 41)). It is also important that the user has knowledge of the logic behind the data collection (Directive 95/46/EC, art. 12). This will avoid decisions resulting from personal profiles, without the user knowing the underlying valuation standard.

By giving his consent, the mobile user restricts the competence to collect, process, and use his personal data for a certain purpose. A misuse is therefore regarded as an unlawful act. From this it follows that the user must be able to choose the type of data collected about him. This excludes the possibility of encouraging the user to opt-in into a blanket provision for the use of his/her personal data. It is essential to ensure that consent is given freely and voluntarily. This implies that the service provider has provided the customer with a clear, conspicuous, and complete disclosure and that no more data than is necessary should be collected for the underlying purpose.

Requirements before the sending of m-advertising

Since m-advertising may become an extremely intrusive practice, EU legislation restricts m-advertising to some extent, as it only allows permission-based advertising, meaning that *"direct marketing may only be allowed in respect of subscribers who have given their prior consent"* (Directive 2002/58/EC, art. 13(1)). Given the personal nature of a mobile device, only permission-based advertising is regarded as an appropriate approach for m-advertising. This approach is called *'opt-in'* and requires that a customer explicitly agrees to be provided with services before the provider is allowed to send them. In case the user gives his consent he must at any time, easily and at no charge, have the option to oppose (opt-out) of the receipt of further messages (Directive 2002/58/EC, art. 13(2)). s

Next to obtaining that personal data is processed, a mobile user must also be informed of the purpose of the advertising campaign (Directive 2002/58/EC, recital 32). This will ensure that the mobile user is able to choose freely whether or not to participate in an m-advertising campaign that is based on the use of personal data. Here, consent also implies the type, location and frequency of received m-advertising to which a mobile

user may agree. Moreover, the mobile user must be provided with a right of informational self-determination not only prior to the service start but also during the advertising campaign (Directive 95/46/EC, recital 41). This will ensure that he will be actively involved in the process and be able to make a free decision on which m-advertising he will receive and from whom, as well as over which period of time.

Moreover, the Privacy and Electronic Communications Directive (2002/58/EC) has a very soft approach to opt-in, allowing for several types of exemption that makes it possible for marketers to send commercial communications without having to ask for permission first. In the case of a pre-existing commercial relationship the opt-out system applies, but this opportunity is limited to similar products and services (Directive 2002/58/EC, art. 13(2)). In this case, the service provider must furthermore prove that the consumer has not initially refused commercial contact and that the consumer has obtained clear and appropriate information to object - free of charge and in an easy manner – to the receiving of future e-mails (opt-out). Only the company involved in this relationship is subject to this right. It cannot be conferred upon third parties (Directive 2002/58/EC, recital 41).

According to the Privacy and Electronic Communications Directive (2002/58/EC), it is left to the EU Member States to decide how to protect the legitimate interests of legal persons with regard to unsolicited commercial communication for direct marketing purposes (Directive 2002/58/EC, art. 13(5))). However, it must be provided that these people have been given the opportunity to object, free of charge and in an easy manner, at any point of time. Any legal person, not wishing to receive unsolicited commercial communications, must at least have the possibility to register themselves in opt-out registers which must be consulted regularly and respected by the advertiser (Directive 2002/58/EC, recital 45).

Evaluation and design proposals

A critical aspect of permission-based m-advertising lies in the issue of 'meaningful consent' (Cavoukian & Gurski, 2002): *"In order for consent to be meaningful, however, it must be informed. This is becoming increasingly difficult as technology outstrips the guidelines that govern it"* (p. 3). To ensure informed consent businesses must make the details of their data protection measures publicly available. In the mobile world, however, this will be difficult to realise due to the limited screen size of mobile devices. Obviously, given the constraints associated with the size of the display on most wireless devices, it is impractical to publish pages of privacy policies on a mobile screen. Moreover, mobile devices allow for mobility and the user may be en-route and not fully aware of the content and due to the low speed of data transmission, mobile users often have no incentive to read the privacy policy of the service provider. This will hamper the understanding of the policy content. Therefore, the disclosure requirement must fit the circumstances.

The opt-in approach was chosen to avoid users being overwhelmed with messages since the current technology enables advertisers to send electronic commercial communications easily and inexpensively. Due to the personal nature of mobile devices, too many advertising messages may be perceived as a nuisance. However, the modality in which consent must be collected is not clear formulated in the law. Even though EU law unambiguously requires the opt-in system, it is still unclear what 'opt-in', or for that matter 'opt-out', actually means in practice. Existing definitions are not definite enough to inform the advertiser whether giving, for example, the mobile user the opportunity to un-tick a ready-ticked opt-in box is in fact opt-in. In the past people went to phones to communicate, nowadays it has become a common practice that phones follow people. Access to online information and easy data entry extend the ability for dynamic and real-time decision-making. To ensure that a mobile user is not giving his consent accidentally or hastily the permission process should be different in m-commerce situations. Confirmed opt-in[1] is an approach which verifies a user's permission in order to ensure that consent is appropriately obtained. Although confirmed opt-in may be considered as the highest level of subscriber permission, in the mobile sector it should be the baseline. From this follows that a simple keypress or ready-ticked opt-in box can by no means be regarded as sufficient to obtain consent for the purpose of receiving m-advertising. In case of 'pull' advertising, the opt-in approach is not regarded as necessary since the mobile user receives requested information. It would be annoying to the consumer to have to agree to each advertisement that is delivered with requested content.

Several parties may be involved in an m-advertising campaign: Network operators, advertisers, and other service and content providers may be involved but not visible to consumers. The question is whether the disclosure is to come from all parties and whether the mobile user must give permission to each of them. If

[1] 'Confirmed opt-in' (also called double opt-in) is the process by which each new subscriber is sent an "authentication" message requesting that he or she confirm the intention to receive communications from a company or organization.

this was the case, coordination among them will be required, which may further confuse the mobile user. Meanwhile, the relevant laws do not consider the type of relationship that the mobile user may have with the involved parties.

A possible solution to this problem could be the following: disclosure could be included at the time when a consumer signs a service contract with the network carrier. The advantages are that disclosure can be made in writing and that the mobile user will receive a uniform disclosure. The latter implies that the user does not have to be informed about each single event since he is aware of the processing practices of the service provider. The carrier would then take the role of a central service provider and be in charge of providing the mobile user with an informed disclosure while at the same time being able to obtain meaningful consent. This will also avoid the problem of the mobile user having to agree to each 'push' advertisement sent to him – which may be annoying if this event occurs on a regular and/or frequent basis. This argument is strengthened by the fact that the carrier is providing the network service and therefore already owning a relationship with the mobile user (Gratton, 2002).

In the case that the disclosure was not combined with the mobile phone subscription the privacy policy could be delivered by conventional means if the advertiser knows the address of the receiver or if he has already been in contact with the consumer. However, the mobile user may want to make use of the advantages of a fast transaction so that this procedure will not be appropriate in m-commerce. The same applies to the sending of the policy by e-mail which will also delay the transaction process. Therefore, the voice functionality could come into play. Although PDAs are certainly widespread, no handheld device has become as dominating as the mobile phone. Since the latter is a voice-centric device it may be advisable to consider adding the voice functionality to the advertising message in order to provide the mobile user with an effective disclosure. The mobile user could receive an SMS including a toll-free number which will establish a connection to a live person or to a recording in order to provide privacy disclosures. Yet another and simpler way would be to apply the 'call-through' technology. This allows the user to click on a text-based hyperlink that will automatically connect the user to an audio privacy disclosure. However, using the voice functionality is only meaningful if a concise and understandable statement is given. An audio disclosure should therefore be used in connection with a written version of the stated policy on the date the consumer uses the service in order to guarantee accurate protection since a voice-based policy would not be a permanent mechanism.

As mentioned in the previous section, the Privacy and Electronic Communications Directive (2002/58/EC) has a very soft approach to opt-in, as it includes the exception of a pre-existing commercial relationship which is limited to similar products and services. The directive raises the question as to the definition of what an existing relationship is and what is considered to be a similar product or service. Since it is not defined in the directive, how can a marketer know when an existing relationship ceases or when it exists? Moreover, since there is no common definition on European level, does the term 'existing relationship' have different meaning in different EU Member States? When does the marketer know whether his product or service is similar enough to send his customer an opt-out-based campaign? And finally, how shall/can the advertiser decide when a customer is a natural or a legal person?

In order to be a legitimate marketer there are several paths a marketer can take when doing m-advertising. One solution would be to become an expert in how to avoid violating the exemptions. However, this will not be the best attempt in terms of achieving effective mobile communication as it will remain too complicated. Another choice would be to go 'full opt-in', meaning not to differentiate between B2B and B2C communication. Thereby, advertisers do not run the risk of breaking the law since they avoid the situation of accidentally sending m-advertising to a business contact that may have the status of a natural person. Consequently, permission-based m-advertising will then be guaranteed for both legal and natural persons. Moreover, advertisers do not have to think about what defines an existing relationship or what is a similar product or service. However, the full-opt-in approach will not reduce the volume of collection events, since it includes the notion that each event will require the acknowledgment of the user.

The service provider must at any time ensure that the user will have the choice as to which information is used in order to determine for himself when, where, and how often to receive m-advertisements. Therefore, the following consideration may find remedy: the service provider could install a personal data account for the mobile user. Thereby, the mobile user gets the possibility of recognising as well as correcting and deleting his personal data at any point of time. A prerequisite for this is, however, that access is granted by means of a secure system limited to the personal data of a certain user. The data retrieval must be performed by means of a reliable authentication process to ensure that third parties are not able to access and change data of another person. The use of digital signatures may be an appropriate tool. In order to

prevent fraudulent use corrective action should not be accepted immediately, and the advertiser must have the possibility to prove the data before acceptance. In order to control the types and volume of m-advertising mobile devices should be equipped with a control mechanism which will be activated by the mobile user. Unsolicited messages stifle user acceptance particularly as mobile phones cannot automatically distinguish between spam and desired communication. Profiling options are already used on mobile devices, i.e. users can design their own profiles or use pre-existing ones (e.g. silent, meeting, outdoors) (Leppäniemi & Krajaluoto, 2005). The user can then input his present status that indicating whether he is willing or not to receive adverts.

Conclusion

M-advertising will be highly personalised, thus requiring a certain amount of information about the receiver of the message. The mobile user can be reached quickly based on his physical location at a given time. While m-advertising may provide the ability to offer valuable services to consumers, it may become an intrusive practise if it invades the personal sphere of the receiver without his previous consent.

For the moment, the scope of m-advertising is limited by technology. However, technology in the mobile world is progressing at an extremely fast pace. Although data protection rules are relatively well established within the EU, the dynamics of the Information Age lead to a gap between the law and business practices within the digital world. The application of mobile communication technologies tends to collect personal information beyond necessity, thereby creating a risk to individuals' privacy. Thus, there remain open issues, such as the level and type of consent required before the collecting of personal data as well as the sending of unsolicited m-advertising.

In this article it was analysed that informed consent is not a simple matter, but in fact opposes most fundamental challenges that m-advertising present to the current legal frameworks. In order to provide meaningful consent prior to receiving m-advertising, mobile users need to obtain an appropriate and effective disclosure regarding the processing of personal data through mobile technologies. Consumers should be given some form of control over their personal data and they should be able to control the types and volume of m-advertising messages. The success of m-advertising is dependent on the development and execution of legislative and industrial initiatives. Consequently, in the mobile world, privacy is not simply a question of legislative compliance, but also one of solid business practices and technical solutions in order to avoid unsolicited m-advertising.

References:

European Commission (2007, March 2007): Information Society Policies. *Information Society*. Retrieved 21.03.2007, from http://ec.europa.eu/information_society/policy/index_en.htm.

Ask, J., M. Gartenberg, C. Matiesanu and N. Scevak (2006): *US Mobile Marketing Forecast, 2006 to 2011*. (Vision Report): JupiterResearch.

Camponovo, G. and D. Cerutti (2004, July 12th-July 13th): *The Spam Issue In Mobile Business A Comparative Regulatory Overview.* Paper presented at the Third International Conference on Mobile Business, New York.

Cavoukian, A. and M. Gurski (2002): *Privacy in a Wireless World*. Paper presented at the Business Briefing: Wireless Technology 2002. Retrieved 21.03.2007, from http://www.ipc.on.ca/.

Commission, E. (2007, March): Information Society Policies. *Information Society.* Retrieved 21.03.2007, from http://ec.europa.eu/information_society/policy/index_en.htm

Dagon, D., T. Martin and T. Starner (2004): Mobile Phones as Computing Devices: The Viruses are Coming! *IEEE Pervasive Computing 3*(4), 11-15.

Directive 95/46/EC (of 24 October 1995) on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Directive 2000/31/EC (of 8 June 2000) on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

Directive 2002/58/EC (of 12 July 2002) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

Geradts, Z. and P. Sommer (2006): *Forensic Implications of Identity Management*. FIDIS Consortium.

Gow, G. A. (2005): Pinpointing Consent: Wireless Location Privacy and Mobile Phones. In K. Nyíri (Ed.), *A Sense of Place*. Vienna: Passagen Verlag.

Gratton, E. (2002): M-Commerce: The Notion of Consumer Consent in Receiving Location Based Advertising. *Canadian Journal of Law and Technology, 1*(3), 59-77.

Kalakota, R. and M. Robinson (2001): *M-Business: The Race to Mobility*. New York: McGraw-Hill Professional.

Kurkovsky, S. and K. Harihar (2006): Using Ubiquitous Computing in Interactive Mobile Marketing. *Personal and Ubiquitous Computing Journal, 10*(4), 227-240.

Lahlou, S., M. Langheinrich and C. Roecker (2005): Privacy and Trust Issues with Invisible Computers. *Communications of the ACM, 48*(3), 59-60.

Leppäniemi, M., H. Karjaluoto and J. Salo (2004): The success factors of mobile advertising value chain. *E-Business Review, IV*, 93-97.

Leppäniemi, M. and H. Krajaluoto (2005): Factors influencing consumers' willingness to accept mobile advertising: a conceptual model. *International Journal of Mobile Communications, 3*(3), 197-213.

Merry, P. (2004): *Mobile transactions in Europe: the challenge of implementation and ramifications of EU directives.* London: ARC Group.

MMA (2006): *Mobile Advertising Guidelines*. Mobile Marketing Association.

O'Connor, P. (2005): Comparative Analysis of International Approaches to the Protection of Online Privacy. In S. Krishnamurthy (Ed.), *Contemporary Research in E-Marketing* (Vol. 2, pp. 347 - 364). Hershey PA, USA: Idea Group Publishing.

Petty Ross, D. (2003): Wireless advertising messaging: Legal analysis and public policy issues. *Journal of Public Policy & Marketing, 22*(1), 71-82.

SkyGo (2003): *Ideas & strategies for implementing mobile marketing*. (White Paper): SkyGo, Inc.

Westin, A. F. (1967): *Privacy and freedom*. New York: Ateneum.

WP15.1 (2005): *Privacy and Identity Management for Europe*. (White Paper): PRIME - Privacy and Identity Management for Europe.

Zwick, D. and N. Dholakia (2004): Whose Identity Is It Anyway? Consumer Representation in the Age of Database Marketing. *Journal of Macromarketing, 24*(1), 31-44.