RESEARCH PAPER | Management | Volume : 4 | Issue : 3 | Mar 2014 | ISSN - 2249-555X

Consumers' Privacy & Ethical Issues Towards Mobile Marketing in India

KEYWORDS: privacy, ethical issues, mobile marketing, mobile technology

Devender Kumar
Research Scholar, Dept. of Marketing & Supply Chain Management (M&SCM), School of Business & Management Studies [SBMS], Central University of Himachal Pradesh [CUHP], TAB Shahpur, Dharamshala, H. P.

Himanshu Rajput
Research Scholar, Dept. of Marketing & Supply Chain Management (M&SCM), School of Business & Management Studies [SBMS], Central University of Himachal Pradesh [CUHP], TAB Shahpur, Dharamshala, H. P.

ABSTRACT *In today's business environment, technology has become the predominant indicator of growth and competitiveness. In recent time, every business has welcomed wireless and mobile technology into their boardroom to offer their customers the freedom to pay bills, planning payments while stuck in traffic jams, to receive updates on the various marketing efforts while present at any place to provide more personal and intimate relationships. Mobile marketing is a quickly changing industry, Privacy & ethical issues can be difficult to pin down different technological capabilities or get a clear understanding of how different technologies work together. The present study plans to 'plug' gap of research in the privacy & ethical issues of mobile marketing among the consumers.*

Introduction
Mobile marketing is a quickly changing industry, still very inconsistent and, in many instances, opaque, complicated, and variable. It can be difficult to pin down different technological capabilities or get a clear under- standing of how different technologies work together.

Mobile marketing will evolve just like traditional online marketing did—over time. It will see small surges as technology improves or key demographics' change, but overall, we can expect the growth and acceptance of mobile marketing to follow a normal or slightly accelerated acceptance curve, similar to the growth of traditional Internet marketing.

Mobile marketing describes any attempt to appeal to potential customers with some sort of marketing message. Mobile marketing encompasses such a wide variety of activities, including

- Mobile advertising, in which brands pay to display visual ads embedded within the content of another website
- SMS and MMS
- Location-based mobile marketing
- Mobile applications
- Mobile search marketing
- Offline marketing in TV, radio and print
- Online marketing on websites, in searches, and with email

Direct marketing relies on the availability of our target market to receive and understand our marketing message directly, so mobile marketing falls neatly into this category of marketing. When compared to other types of direct marketing, the mobile phone offers a greatly expanded opportunity for our target market to receive our direct marketing messages. It has drastically changed our perception of availability, and this has changed how we market our products and services

Direct marketing with mobile devices offers a lot of advantages over other types of direct marketing. It is particularly useful because it has these characteristics:

· Cost effective	· Immediate
· Scalable	· Measurable
· Personal	· Effective
· Interactive	· Actionable
· Targeted	· Repeatable
· Shareable	· Fun
· Portable	· Immediate

Mobile marketing also has the power to convert traditional marketing efforts into direct-response campaigns.

Privacy and the Internet
The use of the Internet can affect the privacy rights a person has in his or her identity or personal data. Internet use and transactions generate a large amount of personal information which provides insights into your personality and interests.

- Ease of access to and the appropriation of email addresses have led to the practice of sending vast amounts of unsolicited e-mails (spam).
- Identification through email and website transactions and the ability to locate people's physical addresses easily through national and international directories have raised new privacy concerns.

Privacy issues relating to personal data arise from
- insecure electronic transmissions,
- data trails and logs of email messages,
- online transactions and the
- Tracking of web pages visited.

Mobile marketers are generally forced to abide by laws and standards for both email- and computer-based marketing, as well as phone-based telemarketing restrictions.

Laws that control marketing and messaging on the traditional Internet also apply to the mobile phone.

Mobile Spamming
The term is used to describe untargeted digital marketing communication (untargeted email marketing). Spam is also used to describe marketing communication that is deceptive or obtrusive. Although email spam can be accessed on mobile phones, mobile spam generally describes unsolicited text, picture messages, or location-based marketing.

Volume : 4 | Issue : 3 | Mar 2014 | ISSN - 2249-555X

Internationally, mobile spam is quite a large problem. In 2008:
- 40% of the SMS messages received in India were spam.
- 50% of the SMS messages received in China were spam.
- 70% of the SMS messages received in Japan were spam.

Mobile Malware and Viruses
Mobile viruses and malware also threaten the efficacy of mobile marketing because they put doubt in the minds of consumers, making them question whether to trust your company or the content you are sending. However, in the mobile world, it is much more difficult to write a virus that will affect a large portion of phones because so many different operating systems are available.

Different virus-related terms :
- Malware—An umbrella term for any malicious software, including viruses, Trojans, worms, and spyware.
- Virus—Code that inserts itself into another program and replicates when the host software runs.
- Trojan—Otherwise known as a Trojan horse, this is a program that purports to be something the user would want to download, but actually harbors malicious code or viruses. In the mobile world, Trojans are usually masked as wallpapers, ringtones, or applications.
- Worm—Worms are self-replicating viruses that automatically spread themselves across a network, usually taking advantage of a user's contacts or address book on an infected device. Worms can also spread via Bluetooth or WiFi.
- Spyware—Spyware is software that runs in the background of an operating system to collect and send private information about a mobile user's behavior to an unauthorized party. Information including private call logs, text messages, and picture messages can be distributed to a third party.

As viruses on traditional computers, mobile viruses can overwrite or delete system files, install corrupted applications, block antivirus soft- ware, block memory, or provide remote access to a user's phone. Mobile viruses are unique, in that they can be spread via a broader range of technology, including SMS, MMS, Bluetooth, WiFi, downloadable applications, and email. They can stop handsets from working properly or at all.

Research Objectives:
This study plans to 'plug' gap of research in the acceptance of mobile marketing among the consumers.

The primary objective of this study is to:
- Explore the adoption of mobile marketing services by consumers considering privacy.
- To suggest measures to ensure the better mobile marketing practices in terms of privacy and security.

Literature Review:
According to Froehlich (1994), Smith (1994) and Shaver et al. (1985), the main ethical problems in this regard (with specific reference to online searching) are as follows: can personal details, obtained from the reference interview, be used for purposes other than for that which it was specifically gathered, is it ethically correct to re-use a search strategy formulated for one user for anther user?, is it appropriate to discuss the nature of a specific query with other people?

The merging of databases which contains personal information. This is also known as data banking (Frocht & Thomas, 1994, p. 24). By this is meant the integration of personal information from a variety of databases into one central database. The problem here does not in the first place arise from the integration of the information as such. The main problems include the fact that the individual is not aware of personal information being integrated into a central database, that the individual does not know the purpose/s for which the integration is effected, or by whom or for whose benefit the new database is constructed and whether the information is accurate.

Closely related to the merging of files is the increasing use of buying cards ("frequent-shopper cards") by retail stores. Inside such a card a computer chip is buried that records every item purchased along with a variety of personal information of the buyer (Branscomb, 1995, p. 19). This information obtained from the card enables marketing companies to do targeted marketing to specific individuals because the buying habits as well as other personal information of people are known.

Another threat to privacy is the raise of so called hackers and crackers which break into computer systems (Benjamin, 1991, p. 7). This coincides with the shift in ethical values and the emergence of the cyberpunk culture with the motto of "information wants to be free".

Analysis & Interpretation
Consumer behavior is strongly influenced by perception of risk; consumers are usually uncertain about the consequences of a decision or an action [Bauer 2005]. Furthermore, it has been revealed that consumers try to minimize risk rather than maximize utility. A consumer's subjective risk perception can thus strongly determine his behavior [Mitchell 1999]. This is especially true for the adoption of innovations, as consumers lack experience with the new product and find themselves in a situation of high risk. Consumers therefore try to reduce the risk

associated with a certain behavioral decision. During an adoption decision this can result in the refusal of an innovation.

The risk associated with mobile marketing is mainly perceived as one of data security. New media services users tend to have concerns about data manipulation, unauthorized data access, and unwanted tracking of usage patterns. Another security issue concerns consumers' privacy. By using the mobile medium it is possible for marketers to reach consumers anytime and anywhere. This characteristic provides the basis for high-potential, personalized mobile marketing on one hand, but also accounts for consumer's fear of privacy violations on the other.

Digital identity is the ground necessary to guarantee that the Internet infrastructure is strong enough to meet basic expectations such as security and privacy. Anywhere anytime mobile computing is becoming true. In this ambient intelligent world, the choice of the identity management mechanisms will have a large impact on social, cultural, business and political aspects: privacy is a human need and the all of society would suffer from the demise of privacy; people have hectic life and cannot spend their whole time administering their digital identities. Significant growth in mobile media consumption has prompted a call to better understand the socio-cultural and policy dimensions of consumer choices.

Particulars	Wireless	Wireline	Total Wireless + Wireline
Total Subscribers (Millions)	867.02	29.99	897.02
Urban Subscribers (Millions)	521.18	23.37	544.55
Rural Subscribers (Millions)	345.85	6.62	352.47
Overall Teledensity*	70.71	2.45	73.16

- Mobile Number Portability requests increased from 89.70 million subscribers at the end of March

Volume : 4 | Issue : 3 | Mar 2014 | ISSN - 2249-555X

2013 to 91.73 million at the end of April 2013. In the month of April 2013 alone, 2.03 million requests have been made for MNP.
- Active wireless subscribers on the date of Peak VLR in April 2013 are 724.52 million, 83.56% of the total subscribers.
- Broadband subscription reached 15.09 million in April 2013 from 15.05 million in March 2013.

Source: www.trai.gov.in

The growth of mobile business requires the ability to provide context-aware services when and where needed, the development of trust relationships between trading partners, and an ever-expanding capability to reconfigure value chains.

Identity fraud as a term and concept in its formative stages was often presumed to be identity theft and vice versa. However, identity theft is caused by the identities (or tokens) of individuals or organizations being stolen is an enabling precursor to identity fraud.

Suggestive Measures :
- The market for devices like mobile phones, multifunctional watches, and personal digital assistants is growing rapidly. Most of these mobile user devices need security for their prospective electronic commerce applications.
- While new technology has simplified many business and personal transactions, it has also opened the door to high-tech crime. Such applications authorize transactions: mobile phone calls, access to an office or car, electronic payment in stores, retrieval of stored medical data, and access to information on portable computers. Digital signatures-the electronic equivalent of handwritten signatures are at the core of most of these applications.

There are three types of agent trustworthiness:
- Personal-agent trust: Here, the device must act according to the user's wishes while it is in the user's hands.
- Captured-agent trust: In this case, the user is protected even if the mobile user device is lost, stolen, or given away (inserted into a point-of-sale terminal or sent away for maintenance).
- Undercover-agent trust: In this case the mobile user devices will protect a third party from the device's legitimate user.
- Data may be used only for the specific purposes for which it was collected.
- Data must not be disclosed to other parties without the consent of the individual whom it is about.
- Individuals have a right of access to the information held about them.
- Personal information may be kept for no longer than is necessary and must be kept up-to-date.
- Personal information may not be sent outside the geographical boundaries unless the individual whom it is about has consented or adequate protection is in place.
- All entities that process personal information must register with the Information Commissioner's Office.
- Entities holding personal information are required to have adequate security measures in place. Those include technical measures (such as firewalls) and organizational measures (such as staff training).
- Subjects have the right to have factually incorrect information corrected.

Conclusion

The personal nature of mobile marketing is generally a great benefit, but it can also cause major problems for marketers who are not respectful of their customers' privacy. In the world of mobile marketing, trust is at a premium. To increase the adoption of mobile marketing, marketers need to be aware about the privacy concerns of customers. They need to take some measures so that the customer privacy is not compromised. Along with privacy, security is also an important aspect that marketers need to handle. They are required to promote secure mobile transactions practices and need to increase awareness among the consumers toward safe mobile transactions. Most of all mobile marketers are required to promote positive perception towards mobile marketing among mobile users.

Given the fast pace of diffusion of smart phones in India, mobile marketing has got a big potential for marketers that no organization can afford in today's cut throat competition.

REFERENCE

• Archana Sharma, Dr. Vineet kansal - Mobile Banking as Technology Adoption and Challenges: A Case of M-Banking in India - published at: "International Journal of Scientific and Research Publications, Volume 2, Issue 2, February 2012 Edition." | • Bauer, H. H., Barnes, S. J., Reichardt, T., & Neumann, M. M. (2005). Driving consumer acceptance of mobile marketing: A theoretical framework and empirical study. Journal of electronic commerce research, 6(3), 181-192. | • Barkhuus, L., & Dey, A. K. (2003, July). Location-Based Services for Mobile Telephony: a Study of Users' Privacy Concerns. In INTERACT (Vol. 3, pp. 702-712). | • Britz, J. J. (1996). Technology as a threat to privacy: ethical challenges and guidelines for the information professionals. Microcomputers for Information Management, 13(3), 175-194. | • De Kervenoael, R., Palmer, M., & Hallsworth, A. (2013). From the outside in: Consumer anti-choice and policy implications in the mobile gaming market.Telecommunications Policy, 37(6), 439-449. | • Hiller, J., Belanger, F., Hsiao, M., & Park, J. M. (2008). POCKET protection.American Business Law Journal, 45(3), 417-453. | • Jamieson, R., Wee Land, L. P., Winchester, D., Stephens, G., Steel, A., Maurushat, A., & Sarre, R. (2012). Addressing identity crime in crime management information systems: Definitions, classification, and empirics.Computer Law & Security Review, 28(4), 381-395. | • Lugosi, P. (2009). The production of hospitable space: Commercial propositions and consumer co-creation in a bar operation. Space and Culture, 12(4), 396-411. | • Mitchell, V. W. (1999). Consumer perceived risk: conceptualisations and models. European Journal of marketing, 33(1/2), 163-195. | • Ngai, E. W., & Gunasekaran, A. (2007). A review for mobile commerce research and applications. Decision Support Systems, 43(1), 3-15. | • Pfitzmann, A., Waidner, M., Pfitzmann, B., & Schunter, M. (1997). Trusting mobile user devices and security modules. Computer, 30(2), 61-68. | • Roussos, G., Peterson, D., & Patel, U. (2003). Mobile identity management: An enacted view. International Journal of Electronic Commerce, 8(1), 81-100. | • Sharma, A., & Kansal, D. V. Econspeak: A Journal of Advances in. | • Westin, A. F. (2003). Social and political dimensions of privacy. Journal of social issues, 59(2), 431-453. |