

A Descriptive study of Ethical issues in use of social media for influencing Consumer

Dr. Bhanu Pratap Singh
Reader
Institute of Management Studies, DAVV

Abstract:

Deceiving customers to achieve financial gain is ethically wrong. On the other hand, establishing trust through honest interactions is an ethical gain, and is more likely to lead you to financial gain as well. When the consumers are getting the facility of relatively unrestricted communication on social media, they are vulnerable to various scams and deceptions. The increasing exposure to social media put the consumer's data readily available to access through various apps which has become the reason of attention for various Social Networking Ethics. While discussing the social media ethics, behavioral targeting becomes the matter of consideration. Social Media Networking provides various avenues for the participants in the creation and sharing of multimedia information. Twitter, YouTube, LinkedIn, Facebook are some SNSs that let the consumers share their data. But these SNSs and various apps invite consent of consumers also for access of user's data as well. Various advertisement agencies took benefits for promotional advertisement through their link.

The paper is intended to provide a detailed examination of relevant ethical issues in the use of social media for influencing consumer behavior.

Keywords: Ethics, consumer, security, malicious software

Introduction:

Ethical issues become a matter of concern not only with respect to the privacy settings and confidentiality of data by these applications and platforms, but also in relation to the use of the 'big data' that is produced via social media for decision making and influence, trend analysis and consequently for predictive modeling

A range of high-profile research ethics scandals, such as Cambridge Analytica, OkCupid, and the Facebook Emotional Contagion study, remind us of the ethical issues at stake.

As marketing is done through social media marketers must not forget that social media for most of the customers is a platform of social experiences not for exposure to marketing activity. For marketing activity market place and market space is used, market place is a physical location while market space is a virtual location. Due to location distribution constraints virtual space is very easily accessible and can target many customers at single point of contact and also customers can be segmented on the basis of level of involvement. Brian Solis, of Future Works, defines social media as "any tool or services that uses the Internet to facilitate conversations." Increased usage of Smartphones, tablet computers multifold the use of social media everywhere and anywhere.

Consumer behavior can be defined as the decision process and physical activity individuals engage in when evaluating, using and disposing of goods and services. A consumer undergoes need recognition, search for alternatives, information processing, evaluation of alternatives, selection of alternatives and disposition of choices made. Consumers while using social media may explore for terminal values

also termed as end-states of existence or chase for Instrumental values (modes of conduct). Through social media these values like want of comfortable life, sense of accomplishment, world of peace, world of beauty, sense of security, inner harmony, courageous, responsible, intellectual or imaginativeness is explored and practiced to influenced

Concept of Social Media:

Social media is an online platform offered to people for contact, communicate and information sharing (through voice, pictures, video, reel or real time streaming sharing)

Social media because of its very nature is fast and easily reachable to end users. Internet not only facilitate search of information but also makes evaluation of alternatives in hundreds of ways. Social media helped in segmenting customers in various ways depending upon conventional methods like demography, geography, psychographical and behavioral.

Various social media tools available are blogs, microblogs, media sharing sites like Youtube, Flickr, Facebook, Picasa, photobucket, crowd-sourced communities such as Reddit, Digg. Social media and Mobile technology uses SMS, MMS, Mobile Web sites (MOBI and WAP sites), Bluetooth marketing Smartphone apps includes software to turns phone into scanners for various types of barcodes-including QR codes.

Social media sites offer quick access to the friends, relatives and trusted people through web and also permits the customer to view and access to the posts and comments in an easier way. This technique helps the consumer to know about the product information shared and posted by others in social media. Webscraping (also known as screen scraping, web data extraction, web harvesting). It is a technique that uses specialized software to extract large amounts of data from websites. End-to-end encryption a system of communication where only the communicating users can read the messages. In principle, it prevents potential eavesdroppers – including telecom providers, Internet providers and even the provider of the communication service – from being able to access the cryptographic keys needed to decrypt the conversation

Literature Review:

From CNNIC Online shopping report (2014), several factors of social media trigger the consumer purchasing motivation and social media purchasing has developed into a new consumption pattern online. In a systematic review of the social media literature, Kapoor et al. (2018) find that social media has been widely adopted as a marketing medium. In the private sector, social media is often used as a communication tool to promote and sell products and services; in the public sector, social media is often used to share information and encourage user engagement (Royle and Laing, 2014; Gruzd et al., 2018). Research has analyzed the effectiveness of social media marketing (Dwivedi et al., 2015; Kapoor et al., 2018; Lee and Hong, 2016) and behavioral attitudes towards viral marketing (Citton, 2017; Eppler and Mengis, 2004) and advertising (Alalwan, 2018; Lee and Hong, 2016; Shareef et al., 2019). Factors such as interactivity (Jiang et al., 2010), perceived relevance (Jung, 2017), perceived usefulness (Chang et al., 2015), and organizational reputation (Boateng and Okoe, 2015) have been found to impact consumers' attitudes towards social media marketing. Social media is celebrated as giving people the opportunity to express themselves and their ideas via user-generated content (Van Dijk, 2009), yet many people express privacy concerns with the use of their social media data by third parties (Acquits and Gross, 2006; Marwick and Hargittai, 2018).

Rational of Study

With the advent of technology and AI, privacy of information is no more a controllable part. Many consumers while searching for their purchases often are directed towards unwanted decisions. Sometimes unwanted marketing practice is also being pushed towards consumers like popping of advertisement, misrepresentations, unrestricted exposure of period of the content shown etc. A very similar situation occurs when the company share registered e-mail or contact number of users to social media apps to match are being targeted of spamming. Now a days controversy is also received for end to end encrypted security. In this situation concern of ethical behavior becomes imperative, so, the paper is aimed at studying various ethical issues of social media practices.

OBJECTIVES OF THE STUDY

The objective of the study is to know about ethical dimensions to be considered while using social media for influencing consumer behavior.

METHODOLOGY

Present study is based on secondary data sources for which observation and literature references were considered.

Discussion

Following are the threats posed before use of social media that can affect consumers Invasion of privacy. Privacy is at stake in various methods as follows

Social tracking

Data collection and analysis also known as data scraping: The companies who track the data and shared information of peoples are called as Harvesters. These harvesters are basically researchers who are engaged in extracting the details of online users and put forth the argument that people are knowingly sharing personal details on social media and thus, it's free for everyone's use. Data harvesters don't ask for the owner's consent. And this raises an ethical as well as online privacy concern.

Information leaks

It's a noted mistake while granting permission by "Allowing" any application during its downloading process to grant access to pictures, contact numbers, location etc. Once a consumer click "Allow" tab, applications are leaking this access permission to advertisers to access profile data. However, no assurance is given that data is not being transferred to any third party. Thus, privacy and safety are at risk

Phishing

In the form of an email, a text message, or a phone call, a phishing attack presents itself as a message. These messages trick people into sharing sensitive data, including passwords, banking information, or credit card details. In a phishing attack on Instagram a hacker creates a fake Instagram login page and re-direct a user to the real Instagram login page for authentication. The link takes you to a website which requests confidential details or causes your computer or mobile device to be infected with malware. The credential is stolen once user ID and password shared on phony page. The same trick is adopted on other social media like Facebook, twitter, linkedin where redirecting for login process is repeatedly induced to follow.

Malicious software

Malware are any software which is designed to damage or harm computer system's resources of consumers or leak its confidential information through unauthorized access either remotely or locally. Cybercriminals use sophisticated malware to leak or compromise confidential information from a compromised system. This harmful software normally enters into the system of users unknowingly and the user may remain unaware when and how they entered. The analysis of these Malware can be mainly performed through static analysis, dynamic analysis, memory analysis, code analysis, , and hybrid analysis techniques

Bot attacks

Bots originated as a useful feature for carrying out repetitive and time-consuming operations but they are being exploited for malicious intent. The attacker may choose to write its own code or simply extend or customize an existing bot. With the advancement and sophistication of botnets and with skilled and organized botmasters, a powerful threat as that from network worms, intrusion, viruses, Trojan horses, and other familiar cyber threats persists to the internet security and privacy.

Spamming

Spam refers to unsolicited messages sent in the form of bulk messages, phone numbers, malicious tiny URLs, trending hashtags, images with hidden URLs, porn videos, healthcare advice, ransomware, stock market spams, forged commercials, fake reviews, fake news, and political astroturfing, etc. by spammers to make good earnings

Artificial Intelligence

With the increasing use of AI-powered technologies, there is a concern about the potential erosion of privacy. AI systems can collect and analyze vast amounts of personal data, leading to potential privacy breaches and surveillance. If misused, AI can infringe upon individual privacy rights and lead to a surveillance state. AI can be exploited by malicious actors for various purposes, including cyber-attacks, misinformation campaigns, and social engineering. As AI becomes more advanced, it could potentially be used to create sophisticated hacking tools, deepfake videos, or autonomous weapons systems, posing significant security threats. ethical dilemmas arise when programming AI systems to make decisions that have moral implications, such as self-driving cars choosing whom to save in a potential accident.

Conclusion

Consumer plays an important role for benefit of any organization. Technological adoption has gained more pace in consumers life. The smart phone reached in every aspect of consumer whether social, financial, personal or organizational. So, any threat to security and privacy to consumer may also lead to threat to all these aspects. Rule regulation and law are subject of national political-legal scenario but more can be done if ethically this intrusion can be stopped, Afterall we all are human beings and have moral value to respect privacy and security of each other's.

Suggestions and Recommendations

1) Take Privacy Seriously:

One way of precaution is to control how much information you put about yourself. You can remove your details from database of 'People-search'. Time to time password changing is also helpful in preventing leakage of privacy. Recognize threats of financial issues or offers that seem too good to

be true. Establishing guidelines and regulations that prioritize transparency, fairness, and accountability can help mitigate potential risks and ensure that AI technologies are used in a way that benefits society as a whole.

2) **Aim at Transparency:**

Don't Distort or Overstate

Avoid Over-Promising and Under-Delivering

Don't Spam or Over-Promote

Don't Use Clickbait Headlines

Avoid Controversy for Publicity's Sake

Don't Engage in Fear-Mongering.

Consider how it will affect others

Don't be opportunistic

Be truthful in reporting

Avoid public bashing

Implication of Study

The study have its affect not only on creating awareness among consumer that how social media can be misused by invaders can threat their every aspect but also how it pose threat to organization and any nation.

References

1. Moreno MA. Fost NC. Christakis DA. Research ethics in the MySpace era. *Pediatrics*. 2008;121:157–161. [[PubMed](#)] [[Google Scholar](#)]
2. Chew C. Eysenbach G. Pandemics in the age of Twitter: content analysis of Tweets during the 2009 H1N1 outbreak. *PLoS One*. 2010;5:e14118
3. Heavilin N. Gerbert B. Page JE, et al. Public health surveillance of dental pain via Twitter. *Journal of Dental Research*. 2011;90:1047–1051
4. Prochaska JJ. Pechmann C. Kim R, et al. Twitter=quitter? An analysis of Twitter quit smoking social networks. *Tobacco Control*. 2012;21:447–449
5. Paek HJ. Hove T. Kim M, et al. Mechanisms of child abuse public service announcement effectiveness: roles of emotional response and perceived effectiveness. *Health Communications*. 2011;26:534–545
6. Baer W. Schwartz AC. Teaching professionalism in the digital age on the psychiatric consultation-liaison service. *Psychosomatics*. 2011;52:303–309
7. Bowen LN. Malaty IA. Rodriguez RL, et al. Did General Douglas MacArthur have Parkinson disease? A video and archival analysis. *Neurology*. 2011;76:1668–1672
8. Papacharissi Z. The virtual geographies of social networks: a comparative analysis of Facebook, LinkedIn and ASmallWorld. *New Media Society*. 2009;11:199–220
9. Lenhart A. Purcell K. Smith A, et al. Washington, DC: Pew Internet and American Life Project;

2010. Social Media and Young Adults.

10. Moreno MA. Parks MR. Zimmerman FJ, et al. Display of health risk behaviors on MySpace by adolescents: prevalence and associations. Archives of Pediatrics and Adolescent Medicine. 2009;163:35–41.

11) <https://www.linkedin.com/pulse/how-ai-threat-humanity-dr-hitesh-mohapatra>