INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN ECONOMICS & MANAGEMENT SCIENCES

OPEN ACCESS JOURNAL

Vol 5, Issue 2, (2016) E-ISSN: 2226-3624

The Importance of Trust and Privacy in Social Media

Anamaria - Catalina Radu, Mihai Cristian Orzan, Andra Ileana Dobrescu, Octavian Arsene

Bucharest University of Economic Studies, Faculty of Marketing, Bucharest, Romania

Email: anamaria_radu15@yahoo.com, mihai.orzan@ase.ro, andra.

To Link this Article: http://dx.doi.org/10.6007/IJAREMS/v5-i2/2212 DOI:10.6007/IJAREMS/v5-i2/2212

Published Online: 09 January 2016

Abstract

The emergence of the Internet and the development of new technologies brought both many benefits and disadvantages for the user. Obtaining information in a very short time, the opportunity to do online shopping without having to go to the shop and the possibility of contacting people at distance are some of the benefits that can be obtained by the online users. The trust must be seen in the digital environment as consumer`s belief that the products/services supplier will bring all the transactional contributions and that the data provided for this purpose will be safe. Along the time, the concept of privacy has been studied by many specialists. It has been analysed both in accordance with the individuals` perceived risk in the online environment and with their confidence in the service providers. This paper analyses the way in which trust and privacy have the capacity to influence users in social media. This paper analyses the way in which trust and privacy have the capacity to influence the customers in social media.

Keywords: Online Marketing, Web Technologies, Web Tools, Trust, Privacy

Users trust in the online environment

The increase in the number of Internet users has led many companies to switch activity and create their online platforms that offer them the possibility to sell products in this environment. The advantages for suppliers and consumers have determined many companies to quit the traditional distribution of products and to use all the opportunities of digital environment.

Carrying out certain activities on the Internet have been very often overshadowed by people`s mistrust in the virtual environment. Intangibility of online services and failure to manage all the activities preceding a transaction has made many people become sceptical regarding online transactions.

Because of this, there are people who despite their willingness to acquire various products online, do not do so because of fear of losing material goods or services in the transactions carried out. This mistrust is generated mostly by the fact that between the parts involved in online transactions there is no physical contact, which reinforces the idea of possibility to fraud the transactions (Cheshire et al., 2010).

Mayer defines the mistrust as being "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the user, irrespective of the ability to monitor or control that other party".

McLeod (2008) saw mistrust as being a set of convictions, attitudes and dispositions that we have regarding others whom we hope to be reliable. Trust is a lengthy process which requires involvement from both users and retailers. This is a feeling that requires a permanent contact between the involved parts, being the result of consumer`s perception and attitude towards actions in the external environment.

Corritore et al. (2003) mentioned that online user`s level of trust in the online environment mostly depends on the individual`s ability to overcome the cognitive barriers. Thus, the fear, perceived risks, the cost and the complexity in use are just some of the elements to be taken into account when deciding purchasing online a specific good.

Wang and Emurian (2005) underlined that trust in digital environment comprises a series of characteristics, similar to those in offline environment. However, there are elements of differentiation, as for example: the relation between the parts that carry the transaction (the impossibility of knowing the services provider), vulnerability (transaction complexity and marketer`s anonymity may lead to the occurrence of some certain unpredictable actions), actions concerning the product (trust in online environment may generate both online products sales on the website, by providing credit data and other digital environment specific actions) and subjectivism (trust in the online environment is different from one person to another, presenting specific features according to the characteristics that define each person).

Gefen (2000) shows in a study that building trust in the online environment depends very much on individual`s personality and its propensity to trust or distrust certain actions that occur in life. Thus, if a person is willing to trust new aspects that he encounters, it will also present a higher level of trust in the online environment. The degree of trust also depends a lot on the individual`s lifestyle and culture. There are cultures that encourage innovation, change and cultures reluctant to changes occurring in the external environment. With regard to lifestyle, the more dynamic, open-minded, communicative a person is, the more willing it will be to try new things, giving greater confidence to such actions.

Users' activity on the Internet is strictly related to their browsing experience (Dutton & Shepherd, 2003). Thus, the more often a user performs certain transactions online, the greater its confidence will be in the actions that he performs. The user experience may generate besides a higher level of trust, a higher strictness of the user. In this way, the consumer can become more attentive to the data it provides, learning from every online experience.

Consumer`s confidence in the activities carried out online is influenced by a range of factors such as: (Abbasi et al., 2011): the quality of the information provided, data security, personal data protection, protection of existing information on the cards, website reliability, guaranteeing the merchandise and offers found on the websites, the existence of other buyers or websites that recommend the purchasing of the products from the website in question, quick access to information and the existence of a simple search algorithm, offers history, a good communication with the consumer on the website and the history of the marketed goods. All these characteristics can be divided into several categories which the services provider must always consider. These are: the trust in the online goods, the positive effects of certain items on trust, the trust in sellers and online shops, the experience in buying certain products online.

From the aforementioned we can see the importance of website quality, as it is meant to provide the consumer all the information he needs. The website offers the information about: the products (the history, how the distribution is made, etc.), their quality, transaction safety or personal data protection. It represents the mediator between the consumers and the online services providers

The analysis made by Luo (2002) established the mechanisms that aim to strengthen the user's trust in the activities they carry out in the online environment. Trust mechanisms are: characteristic- based, pross-based, institutional- based, person/firm specific and intermediary mechanisms.

For the characteristic based mechanism, the reliable source is made up of family, community, and members of the reference group. At this level, relatives or ethical similitude are considered essential in generating trust. Process-based refers to the trust highly related to previous acquisitions, repeated purchases or future changes planned by the respondent. Unlike the previous mentioned mechanism, is the source of confidence generated by reputation, by the type of brands marketed and offered gifts. This is very much based on how previous acquisitions have been carried out. Institution-based trust is different from the previous, with an official commercial structure as for example the institutions and third parties who have the ability to guarantee and certify the transactions. This one is very important for the consumers in the virtual environment, being the one that generates trust to the targeted public and reduces the people`s lack of trust when they have to provide personal data. It helps evaluating the suppliers, confirming their identity and helping consumers in developing future transactions.

Trust shows the lowest rate of use in the field of banking transactions, where individuals often fear the possibility of identity theft and the possibility of defrauding transactions. The fear of losing financial resources many times prevent people from using Internet banking advantages (convenience, lower cost, quick response to orders, etc.) and make traditional transactions instead.

Suh and Han (2002) proved that the use of Internet banking is influenced by users' perception regarding the development of this process. Thus, if a user perceives this activity as being easy and useful, the level of trust will increase, which determines a certain attitude in employing it, and its further use. Therefore, trust is related to using a certain online application, this one being the determinant point for the activities performed by individuals.

Kim, Ferrin and Rao (2008) have shown that consumers` trust is not the final point that must be targeted by companies. This must be seen as a part of a whole made up of: the perceived risk, trust and benefits, and that it is able to directly influence consumer`s purchase intention. By analysing all the above, the Internet service provider should know what are the most important aspects that can generate consumer`s trust and that can increase the number of benefits.

Urban, Amyx and Lorenzon (2009), noted that trust must be analysed in terms of three dimensions that define it, namely: integrity/confidence, ability/competence, and benevolence. People`s trust in online activities is influenced by the way the website is organised and how it generates confidence among target audience.

Moreover, the experiences acquired from different websites and user`s skills have an important impact on purchasing decision in virtual environment. As we have seen before, trust is a mediator between the supplier's ability to generate trust (through its own elements: website, application data security, etc.) and individual`s actions (acquisition, fidelity, loyalty). In order for a particular company to succeed on the market, to achieve significant sales and

profits, it must have the ability to generate trust in the customers, having benefits on both short and long term. (Urban et al., 2009).

Gefen (2000) has shown that trust is an element that highly depends on user`s familiarity with the site. The better a consumer knows the website, the applications, the security system, etc.. the more confident he will be. Furthermore, a higher trust level may generate interest among the consumers, an interest that can turn into a particular purchasing behaviour.

Chiu et al. (2012) have shown that in addition to user`s familiarity with the activities in the online environment there are a number of factors that have the ability to influence the level of trust experienced by these users. The degree of confidence felt by Internet users depends very much on their satisfaction felt from previously carried out acquisitions. In this way, the more satisfied the consumer is with the products / services he previously purchased online, the more trusting he will be, which will lead to repeating the purchasing process.

On the other hand, Hong and Cho (2011) have shown that trust in intermediaries and sellers can generate a more rapid purchase, which subsequently lead to fidelity and customers loyalty. All this derives from the idea that a consumer needs to permanently identify the trading partners in order to trust them and to conduct further shopping.

Corbitta et al. (2003) emphasize that consumer`s confidence in the online environment is influenced by a number of factors that can influence individuals` purchasing and consumption decision. Thus, as we saw above, the user`s experience in the virtual environment, perceived risk, trust in the used techniques , the perception of quality of the website, market orientation and the degree of consumers participation in online transactions are only some of the aspects designed to determine whether or not a consumer trusts a particular transaction. All these elements that define individual's online behaviour have the power to influence its decisions and determine him to buy and use products purchased from the virtual environment.

Moreover these factors are of particular importance for the companies or users that sell various items in the digital environment. Improving certain indicators that are directly related to suppliers`activity (website quality, trades quality, technology used, the security system of the data) can lead to improved profits that arise from transactions. Besides this, the increase of the level of trust or of the number of transactions carried out highly depends on individual`s activity, but also on how various activities are performed in the digital environment.

Trust depends very much on the competence, responsibility and reliability of the providing company (Jones and Leonard, 2008). Moreover, a consumer succeeds in trusting some of the online companies only if he perceives the respective company as being honest and unable to perform various frauds in the transactions. Trust is seen as the result of passing over uncertainty. This is what certifies and allows the user to overcome cognitive barriers.

Jones and Leonard (2008) noted that the trust level is different, depending on the supplier of the marketed products / services. Thus, on C2C (chats, forums or websites marketing various products) trust level is much lower because we are not dealing with a company that can certify and guarantee its products / services. The perceived risks of such transactions are much higher, which causes consumers to be reluctant and to analyse in detail the actions they carry out in the online environment.

Bryce and Facer (2014) examined the relation between perceived risk, trust and providing personal data in the online environment interactions on young people. It was noted that individuals are aware of the risks that may occur by disclosing your identity online, but

they believe that sometimes the benefits obtained outweigh these types of risks. They believe that disclosure of personal information help them in further developing relations which are essential for socializing.

In the research conducted over time, Kima, Xub and Guptac (2012) have shown that the purchase decision online depends not only on the the degree of confidence felt by the user but also on how price level is perceived. Thus, it was observed that the trust in the online environment presents a far greater importance than the price level. Analysing both in terms of the current customers and prospects, it was noted that the perception of a certain level of trust to potential consumers has a much greater influence on the decision to purchase, compared to actual consumers.

The perception of a certain level of price is more important among customers than among the prospective clients. This reveals the fact that, the higher the consumer`s online experience is, the more confidence he manages to gain and to get to know the charged prices. This allows the individual not to be sceptical in the conducted transactions and to become more aware of the existing price level.

Trust was always seen as an obstacle that determines the user to be reluctant when shopping online. In order to increase the level of trust felt by consumers, the trust brands appeared, particularly aiming to increase the number of users who use digital services.

Rudiger (2013) defined trust mark on the Internet as ``*Internet trust marks are word and/or figurative marks issued by an independent institution, which online retailers can display on their websites as a sign of recognition, giving customers and potential customers in a compact form the assurance that the online retailer concerned fulfils certain criteria/(quality) requirements (i.e., codes of conduct, criteria catalogues, standards, guidelines, etc.) specified by the issuer with respect to his business practices, particularly with regard to information privacy, IT security and consumer protection*``.

Based on this definition we can see that trust marks in the digital environment are those that certifies and accredits the online sale of a product. These come to help traders reinforce the idea of quality product for the target audience.

Aiken and Boush (2006) studied the importance of trust marks for the consumer, trying to describe the impact that they have on trust and on the process of confidentiality. The attitude towards such powerful brand puts its mark on individual`s behaviour, the customer adopting a specific behaviour depending on its perception of the trust marks.

Privacy in online environment

These aspects mentioned above are continuously evaluated according to the risks taken by the respondents in terms of data confidentiality. The tension between the desire to obtain information quickly and providing personal data has lately become more pronounced, specialists trying to find the best solutions to solve this problem. More and more users have started to become sceptical regarding the provision of data on the Internet, evaluating carefully every detail of the website. (Kleve & De Mulder, 2008)

Users` privacy is the most important part of the Internet users, the perception of certain risks about it having an adverse effect on individuals` purchasing behaviour.

The notion of privacy has been defined by Warren and Brandeis (quoted in Paine et al. 2007) as people's right to be left alone. Awad and Krishnan (2006) define this process in terms of the individual's ability to control the personal information that can be made public. Actually, intimacy refers to all personal information that usually a person does not wish to

make public. This is individual`s private space, which includes personal data, behavioural data and identification data.

Since the emergence of Internet, people have raised the issue of studying how to protect their privacy from possible existing frauds in this environment. Many avoided purchasing products or entering on various social sites for fear of identity theft. Cases et al. define Internet privacy concerns as: "concerns about possible loss of privacy as a result of a voluntary or surreptitious information disclosure on a web site".

Privacy issues encountered in the digital environment occur mostly due to the peculiarities of this environment. Dinev and Hart (2006) mentioned that the emergence of information security issues in the online environment is largely due to use of information technology, people's desire to socialize and buy products in a very short time and at low costs. All these aspects mentioned above mostly involve providing certain personal information, which may create suspicion for the target audience.

The issues related to data confidentiality on the Internet were analysed by many specialists who tried to find profitable solutions to reduce these issues and increase users' confidence in the virtual environment.

Fabian (cited in Weber, 2010) emphasize that in order to improve aspects regarding respondents' privacy and to reduce the perceived risk at this level, a number of technologies have been developed. Among the most important are: virtual private networks (VPN) (networks that allow access only to those who are part of the group. It is characterized by a high degree of confidentiality), DNS (guarantees authenticity, integrity and data origin), Onion routing (encrypts the data and combine Internet traffic from different sources), transport layer security (improves data security and privacy). All these technologies have been developed in order to improve the activity carried out on the Internet and make individuals feel confident while carrying out activities in this environment.

Users provide information (sometimes without being aware) on a continuous basis regarding their behaviour and preferences; information that can be further easily used by unauthorized persons (Zviran, 2008).

Christiansen (2011) shows that in terms of personal data collection in the online environment, there are companies that gather all this information categorise it and then sell it to advertisers who need all this data to promote their products among the target audience. Moreover, information provided on various websites is used by companies, to meet user's profile and send him selective data, given its demographic characteristics and lifestyle.

After analysing individuals' privacy in terms of security issues that may arise in the digital environment, Earp and Baumer (2003) emphasized the differences between Internet users according to their required data. Therefore, personal data must be that information strictly related to the individual, which usually is not made public. By analysing from this perspective, someone`s telephone number or address are not strictly related to privacy, while bank account details or the intimate life are considered to be more personal.

Because of this, many people are more willing to provide general information about itself (phone number, address, e-mail) when they create an account, purchase products or register on various forums. Providing personal information is closely related to the characteristics that define a particular person. So, the greater the fear that a person feels to provide personal data is, the more reluctant it will be to do so.

Data collection has a very important role in terms of information security problems perceived by respondents in the digital environment. The more information a user is required, the more sceptical it will become regarding the correctness and safety of the website in

question. Fearing misuse of personal information, many individuals avoid using those websites which ask a series of personal information.

In terms of data collection, there can be found the following categories of companies (Christiansen, 2001): companies that collect data about users in databases, and instead of selling the personal information, they provide to third party companies only certain aggregate information (such information are useful for advertisers to identify general characteristics of the website users); companies that collect personal data, but do not provide it, offering the third party companies the opportunity to know some of the target audience features that are users of the website (agencies pay a certain sum of money to send their messages to targeted people), companies that collect data for selling this information (companies collect information in databases in order to sell them to third party companies).

Paine et al. (2007) showed in a study that 56% of those who have an account on one of the social networks are concerned about the privacy issues. This percentage is quite low compared to previous years, when the percentage reached somewhere around 70-80%. This reveals that, over time people began to gain confidence in the websites they are accessing, and to pay more attention to websites' privacy policies.

Fogel and Nehmad (2009) have shown that women are more concerned about data privacy issues than men. Thus, men are more open to provide personal information such as phone number or e-mail, compared to women who are more sceptical when they are requested such information.

Regarding the attitude depending on age, there are situations in which young people are more open in terms of providing contact information considering that by this means they can make new friends with whom they can communicate in the virtual communities. However, older people are very often considered more vulnerable in terms of security in the online environment (Chakraborty et al., 2013).

Jensen, Potts and Jensen (2005) have shown that users' trust in the web pages they visit and the existence of privacy policies (even though many times they are not read) are meant to influence the perception of the transaction security on that site. The most important privacy issues identified in the online environment are directly related to the possibility of identity theft, bank accounts copying or personal information collection without user`s consent.

Akhter (2012) tried to analyse the concept of privacy compared to a number of variables that have the ability to influence the purchasing and consumption decision in the online environment. It was noted that issues related to privacy have a much greater impact on the purchase decisions compared to attributes such as time spent or variety in use. Privacy issues are analysed and perceived in different ways, depending on the individual's education level and his income. So, the higher the user`s level of education is, the more attention he will pay to information security in the online environment. Regarding respondents` income, persons who have a relatively high income shows a much higher propensity to carefully analyse the security issues in the online environment.

References

Abbasi, P., Bigham, B. S., Sarenchen, S. (2011). Good's history and trust in electronic commerce. Procedia Computer Science. 3, 827–832.

Aiken, K. D., Boush, D. M. (2006). Trustmarks, objective-source ratings, and implied investments in advertising: Investigating online trust and the context-specific nature of internet signals. Journal of the Academy of Marketing Science. 34 (3), 308-323.

Akhter, S. H. (2012). Who spends more online? The influence of time, usage variety, and privacy concern on online spending. Journal of Retailing and Consumer Services. 19 (1), 109–115.

Awad, N. F., Krishnan, M. S. (2006). The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. MIS Quarterly. 30 (1), 13–28.

Bryce, J., Fraser, J. (2014). The role of disclosure of personal information in the evaluation of risk and trust in young peoples' online interactions. Computers in Human Behavior. 30, 299–306.

Cases, A. S., Fournier, C., Dubois, P.-L., Tanner, J. F. Jr. (2010). Web Site spill over to email campaigns: The role of privacy, trust and shoppers attitudes. Journal of Business Research. 63, 993-999.

Chakraborty, R., Vishik, C., Rao, H.R. (2013). Privacy preserving actions of older adults on social media: Exploring the behavior of opting out of information sharing. Decision Support Systems. 55 (4), 948–956.

Cheshire, C., Antin, J., Cook, K.S., Churchill, E. (2010). General and familiar trust in websites. Knowledge. Technology and Policy. 23 (3), 311-331.

Chiu, C.M., Hsu, M.H., Lai, H., Chang, C.M. (2012). Re-examining the influence of trust on online repeat purchase intention: The moderating role of habit and its antecedents. Decision Support Systems. 53 (4), 835–845.

Christiansen, L. (2011). Personal privacy and Internet marketing: An impossible conflict or a marriage made in heaven?. Business Horizons. 54 (6), 509–514.

Corbitta, B. J., Thanasankita, T., Yi H. (2003). Trust and e-commerce: a study of consumer perceptions. Electronic Commerce Research and Applications. 2 (3), 203–215.

Corritore, C. L., Kracher, B., Wiedenbeck, S. (2003). Online trust: Concepts, evolving themes, a model. International Journal of Human-Computer Studies. 58, 737–758.

Dutton, W. H., Shepherd, A. (2003). Trust in the internet: the social dynamics of an experience technology. Oxford: Oxford Internet Institute.

Earp, J. B., Baumer, D. L. (2003). Innovative web use to learn about consumer behavior and online privacy. Commun ACM. 46 (4), 81-83.

Fogel, J., Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. Computers in Human Behavior. 25(1), 153–160.

Gefen, D. (2000). E-commerce: The roles of familiarity and trust. Omega. 28 (6), 725–737.

Hong, I.B., Cho, H. (2011). The impact of consumer trust on attitudinal loyalty and purchase intentions in B2C e-marketplaces: Intermediary trust vs. seller trust. International Journal of Information Management. 31 (5), 469–479.

Jensen, C., Potts, C., Jensen, C. (2005). Privacy practices of Internet users: Self-reports versus observed behavior. International Journal of Human-Computer Studies. 63 (1–2),203–227.

Jones, K., Leonard, L.N.K. (2008). Trust in consumer-to-consumer electronic commerce. Information & Management. 45 (2), 88–95.

Kim, D.J., Ferrin, D.L., Rao, H.R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. Decision Support Systems. 44 (2), 544–564.

Kima, H.W., Xub, Y., Guptac, S. (2012). Which is more important in Internet shopping, perceived price or trust?. Electronic Commerce Research and Applications. 11 (3), 241–252.

Kleve, P., De Mulder, R. (2008). Privacy protection and the right to information: In search of a new balance. Computer Law & Security Review. 24 (3), 223–232.

Luo, X. (2002). Trust production and privacy concerns on the Internet: A framework based on relationship marketing and social exchange theory. Industrial Marketing Management. 31 (2), 111–118.

Mayer, R. C., Davis, J. H. F. D., Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. The Academy of Management Review. 20 (3), 709-734.

Paine, C., Reips, U.D., Stieger, S., Joinson, A., Buchanan, T. (2007). Internet users' perceptions of 'privacy concerns' and 'privacy actions'. International Journal of Human-Computer Studies. 65 (6), 526–536.

Rudiger, K., Rodrıguez, M.J.G. (2013). Do we need innovative trust intermediaries in the digital economy?. Global Business Perspectives. 1, 329–340.

Suh, B., Han, I. (2002). Effect of trust on customer acceptance of Internet banking. Electronic Commerce Research and Applications. 1 (3–4), 247–263.

Urban, G.L., Amyx, C., Lorenzon, A. (2009). Online Trust: State of the Art, New Frontiers, and Research Potential, Online Trust: State of the Art, New Frontiers, and Research Potential. Journal of Interactive Marketing. 23(2), 179–190.

Wang, Y.D., Emurian, H.H. (2005). An overview of online trust: Concepts, elements, and implications. Computers in Human Behavior. 21(1), 105–125.

Zviran, M. (2008). User's perspectives on privacy in web-based applications. Journal of Computer Information Systems. 48 (4), 97–105.

Weber, R.H. (2010). Internet of Things – New security and privacy challenges. Computer Law & Security Review. 26(1), 23–30.