Chapter 5
Privacy Concerns and Customers' Information-Sharing Intentions: The Role of Culture

Monica Grosso
Emlyon Business School, France

Sandro Castaldo
Bocconi University, Italy

ABSTRACT

Today companies are more and more interested in collecting personal information from customers in order to deliver goods and services effectively and to improve their Marketing database and CRM efficacy. However, the ease with which data can be acquired and disseminated, also thanks to the digital technologies, has led to many potential customers demonstrating growing concerns and ethical issues about disclosing personal information. On this topic it is difficult to make too many generalizations, since the cultural differences and the different country regulations seem to weigh significantly.

INTRODUCTION

Today companies are more and more interested in collecting personal information from customers in order to deliver goods and services effectively and to improve their Marketing database and CRM efficacy. Thanks to the new devices and technologies (smartphones, Rfid, online tracking, social media, etc.) it is now possible to collect, aggregate and analyze huge amount of information quickly, easily and at a very low cost, compared to the past traditional, slow and expensive methods of data collection used in marketing studies. Furthermore, technology evolution allows space and time separation and simplifies a lot the internationalization of a business at lower cost than before.

DOI: 10.4018/978-1-5225-7113-1.ch005

At the same time, Big Data involves new types of risk to privacy, many of which are only now beginning to be fully understood by customers, lawyer and managers. To completely realize all the new tech's opportunities requires overcoming the main barrier to new technology adoption: the perceived risk of sharing personal information due to the lack of controls to safeguard it. The increasing interaction opportunities and low cost data exchanges that new technologies allow, indeed reduce control over the use of exchanged data: anonymous and unknown parties may access and consequently use this data. Consequently, the ease with which data can be acquired and disseminated and the peculiarities of high-tech settings have led to growing concerns regarding whether and how consumers can safeguard their privacy (Milne, 2000; Phelps, Nowak and Ferrell, 2000).

Information privacy can be defined as the "individual's ability to control when, how, and to what extent his or her personal information is communicated to others" (Son and Kim, 2008). A person has privacy to the extent that others have limited access to information about her/him, limited access to the intimacies of her/his life, or limited access to her/his thoughts or body (Persson and Hansson, 2003). Information privacy concerns refer "to the individual's subjective views of fairness within the context of information privacy" (Malhotra, Kim and Agarwal, 2004). Information privacy concerns stem from the fear of losing control over one's personal data, which refers to the possible intentional or unintentional mismanagement of personal data submitted online. There is a wide range of possible privacy infringements: the company collecting data might use it for purposes that the customer did not explicitly authorize, for instance, by selling this information to third parties unknown to the customer; hackers can steal or tamper with personal data; and databases might contain errors that can affect the user negatively.

Potential loss of privacy has been largely studied as a deterrent to consumer disclosure (Culnan, 2000; Milne, 2000; Milne, and Boza, 1999; Phelps, Nowak, and Ferrell, 2000) and it represents a specific type of socially risky disclosure consequence (White, 2004). Consumers' concern for privacy broadly refers to who has access to their personal information, and what is done with it (Jarvenpaa, Tractinsky, and Vitale, 2000). Consumers, for instance, may wonder whether the information is likely to be accessed by or even sold to parties external to the commercial relationship dyad, and whether it is going to be used for phone or mail intrusion or even fraud. When consumers feel they don't have full control over disclosure of personal information (such as demographics, lifestyle, financial data, and shopping or purchase habits), they are vulnerable to a potential loss of privacy and may behave to protect their threatened privacy. Customers' "protecting behaviors" seem to be aimed at reducing the information they share with firms (Sheehan, and Hoy, 2000; Raman, and Pashupati, 2005). According to a survey by the Pew Research Center 's Internet and American Life Project, as many as 57 percent of users have uninstalled or refused to install applications on their mobile devices for fear of disclosing private information. This reaction threatens the marketing and sales opportunities disclosed by technology evolution and companies should work to reduce such kind of customers' reactions. Several studies explored the nature of the privacy concerns, many of them specifically for the online environment, with the objective of getting a better understanding of the factors that can affect privacy concerns and how these in turn could affect the users' behavior and the future of the Internet and online channels. The research is mainly focused in understanding the privacy concerns as the main antecedent of customer intention (e.g. willingness to share information) and behavior (e.g. WOM or shopping). The aim of this chapter is to contribute to this relevant issue providing a deeper understanding of the privacy concern and its relationship with the customers' willingness to disclose personal information to companies. In particular the chapter presents the results of a study that is considering several conditioning elements that may intervene as we think