

A Research on Protection of Consumer Privacy in E-Commerce

Serpil KARLIDAĞ

Başkent University
Vocational School of Social Sciences
06530 Etimesgut/Ankara, Turkey
skarli@baskent.edu.tr

Selda BULUT

Gazi University
Faculty of Communications
06490 Emek /Ankara, Turkey
seldabulut@gmail.com

Extensive Summary

Introduction

E-commerce has emerged as one of the vital components of today's business due to the recent developments in Information Technologies (IT). E-commerce, which has various types, is the act of buying and selling goods and services over the Internet. As *business to business* (B2B) e-commerce involves companies doing business with each other, *business to consumer* (B2C) e-commerce consists of business selling to the public through shopping cart software. *Business to business* has launched in 1981 and *business to consumer* has launched in 1984 respectively (Marangoz, Yeşildağ ve Saltık Arıkan, 2012; Diker ve Varol, 2013). Thence an infrastructure for online shopping has been built since 1980's. Nowadays, online shopping has steadily been increasing. In fact, for the first 51 days of the November-December 2014 holiday season \$48.3 billion has been spent online, which is marking a 15-percent increase, compared with last year (Comscore, 2014). According to recent research carried on Forbes magazine lower prices are the main motivating factor to purchase books, consumer electronics, entertainment, health and beauty products, toys, sports, hobby related merchandise, clothing and furniture as the better selection has become the leading impetus to buy food and beverages. Furthermore free shipping has had a strong impact on buying commodity goods as cleaning and paper products (Forbes, 2013).

Despite of all developments, consumers are concerned about their protection of privacy and safety. The research conducted for Economist showed that "consumers don't know how their data is used and think regulation and data protection are weak" (Economist, 2013). Since consumers are concerned about problems like identity theft and fraud they are more focused on the safety of making purchases.

From the perspective of business, it's an understandable reason why they collect personal information. When the businesses get more information about the customers they personalize their communications with them and can create competitive advantages within their industries. Moreover, these businesses promote effective customer engagement, loyalty and segmentation. As users move through their internet their

information are also collected by cookies. Then companies gather data without attaching the users' name and show them advertisements more likely to click.

Two separate field surveys conducted by Malhotra et al (2004) indicated that control and awareness of personal data helped consumers to get rid of their concerns. Thence providing clearer information about the company's privacy policy on e-shopping website can reduce information asymmetry between consumer and vendor and also can decrease the transaction costs associated with learning privacy statements. In fact, privacy information affects e-shopping decision (Tsai Egleman, Cranor and Acquisty, 2011).

In post-Fordist economies, intangible goods like information add more value than the manufacturing of material components. Companies can significantly benefit from the ability to learn so much information about their customers. As we live in "consumer data driven and consumer data-focused commercial revolution", consumers also create their own personal information (Acquisti, 2010, p.8). In this study, the contents of privacy statements on e-shopping websites were analyzed. The main question in this study is how companies protect personal information and to post privacy statements on their websites as they increase revenues through consumer data.

Method

Recent developments in information and communication technologies have changed both the business world and daily life of societies like education, health, culture and entertainment. Besides their positive effects they can include unexpected difficulties. Thus new set of rules have been proposed to protect privacy and give consumers/users back control over their personal data. In this study, a purposive sample of Turkey's top 50 websites was analyzed. These websites were selected from McKinsey's report of 2013 and Turkishtime Economy Magazine and Trendbase's research of 2014.

The goal of content analysis is to make valid and objective inferences about the collected data on the basis of explicit rules. Content analysis has also been used to determine the hidden meanings while examining manifest or readily apparent meanings (Gökçe, 2006, pp. 20-22). With this approach, contents across many texts can be objectively compared by the researchers and analysis tables can be created according to the result (Neuman, 2006, p. 466). In this context, the top earning 50 web sites were analyzed in two stages. At first EU Data Protection Directive and Turkish Act numbered 6563, which contains provisions compatible with the EU Electronic Commerce Directive No 2000/31 were evaluated in order to create criteria. Privacy policy texts were selected as the unit of analysis. Categories have been established prior to the analysis based upon protection of personal privacy. Categories have provided for a clean analysis of content and aligning the research problem as Berelson pointed out (1952, p. 147). While categories were being constructed, it was paid attention to exclude from each other. In fact, different categories were formulated in respect to privacy statements. Coding in content analysis is important to reduce the number of different materials. Thus coding units should be defined appropriately and different people should code the same texts in the same way. In this study, while coding was applied to data, two coders developed the coding scheme so closely and commented the hidden meanings in the same way. Thus, in this study the agreement between coders was provided and reliability of level was found acceptable.

In the second stage, the selected e-shopping websites have been analyzed according to created criteria like the following:

- 1) In the study it is looked into the conformity of the contents of privacy policies with the existing law on privacy protection in Turkey and also looked into the availability and findability of privacy policies on websites.
- 2) Tables have been organized according to findings.
- 3) Replicable and valid inferences from texts have been made. Based on inferences, the researchers moved from the texts to the research questions. In fact, these inferences have helped discover the meanings and relationships which can not be usually noticed.

Findings and Analysis

Privacy contracts/policies/rules/principles are available under the websites. However they are sometimes available in or with the using rules. They are rarely placed on the page which the membership contract is made (e.g. Teknosa, Media Markt). 41 out of 50 Turkey's leading e-shopping websites have privacy contracts and 34 of them are on the main page where can be seen by the visitors.

Consumers' personal information, who are visiting the web pages of e-shopping sites are collected in different forms. Mainly, personal information like first name, last name, e-mail address (user ID), password, country etc. is collected during membership registration. In the privacy or membership contracts, business explain why and which information they collect and how they handle customer's personal information. In this study, 42 out of 50 analyzed websites explain how they collect and use personal information.

Technology is the other way of collecting personal data. A cookie is a small text file which gathers information through web pages. There are types of cookies. Some of them only store information and do not personally identify the user but the others identify information about the user. Malicious cookies can be used to store and track the user's activity online. However some businesses don't tell visitors how their websites use cookies. In the study only 11 websites explained their use of cookies. The rest of the websites either say nothing about cookies or pronounce the word "cookie" though they mention that they are storing personal information and tracking user's online habits.

To become a member or benefit from the promotions and campaigns, users give their personal information voluntarily and after that they are supposed to give their consent for them to share their information with others. Although businesses state that they do not rent, sell or share consumer's personal information with third parties they have exceptions. For instance, they do not see their business partners as third parties. They also say they can disclose personal information to the legal authorities as part of a lawful investigation. However they keep all their information either material or immaterial very strictly. They say they have intellectual property of all the texts, videos, images, visual or audial materials, database etc., on their webpages and nobody can use them without permission.

In the study, 10 websites state that they cannot provide absolute guarantee of the security of personal information whilst they will take all reasonable measures like technological and operational security systems to protect customer's information. Since they assume they have no responsibility for the content, privacy policies or practices of

third parties, they strongly advise customers to check the privacy policies of these sites before they click or visit their shopping websites.

Results of the content analysis of 50 web sites have shown that though businesses are committed to protecting customers' personal information they cannot guarantee the privacy and security of any information. Thus consumers should be more careful with their privacy and take the necessary measures before online shopping.