Consumer Privacy in New Media: A Study of University Students in Turkey

Ozgur Koseoglu, Ph.D.

Faculty of Communication, Ege University, Turkey
ozgur.koseoglu@ege.edu.tr

Nahit Erdem Koker, Ph.D.

Faculty of Communication, Ege University, Turkey
nahit.koker@ege.edu.tr

Doi:10.5901/mjss.2015.v6n2p588

Abstract

With the advent of digitization, consumer privacy and personal data protection in new media have arisen as new consumer rights issues. As message effectiveness has emerged as an issue in marketing communications, so has targeting the right consumers with the most appropriate messages become a common goal for marketers. However, targeting may result in some unethical practices such as tracking consumers' web surfing patterns and using and selling their personal data without permission. As university students constitute one of the most active groups in new media, this study focuses on how they perceived consumer privacy, how deliberative they were during their online shopping activities and to what extent they were aware of the risk of providing personal data, particularly through social media, and its consequences. Analysis of transcripts from semi-structured in-depth interviews revealed themes of concern about online shopping and data protection, the effects of social media on perception of privacy, "check-in" on social media, experiences related to privacy breaches, and attitudes towards consumer privacy and marketing activities in new media. The findings and implications of the research are discussed, and suggestions for further study are presented at the end of the study.

Keywords: *Consumer Privacy, New Media, Marketing Communications*

1. Introduction

Van Dijk (2006) notes that, with little exaggeration, the 21st century can be called the age of networks that are gradually becoming the nervous systems of our society, and it is expected that this infrastructure will be capable of influencing our entire society and personal lives. One of the consequences of this influence emerges as an issue of consumer privacy which has received considerable attention lately. While digital networks enable governments, firms, data aggregators and other interested parties to collect, store and analyze data about consumers at unprecedented levels of detail and speed (Taylor and Wagman, 2014), personal information could easily become commodity, which makes consumer privacy more prone to all kinds of breaches. DeCew (1997) asserts that control over information about oneself is referred to by many commentators as the core of privacy. For instance, Westin (1967) defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (p. 7). However, few websites clearly inform their visitors that they are tracking and recording their data (Hoffman, Novak & Peralta, 1999). Yousafzai, Foxall and Pallister (2010) hold the view that consumers perceive little control over information privacy in the digital environment. This view is supported by some research conducted in the U.S. and the U.K, which show that the majority of consumers think that businesses are not transparent regarding how their personal information is being used (Annalect, 2013; Accenture, 2014). Therefore, it is reasonable to conclude that consumer privacy is being challenged by new media technologies that either force consumers to reveal their personal data or, particularly in the case of social networking sites, consumers are encouraged to volunteer such data. This situation makes consumer privacy an important issue to address. Although there are quite a few quantitative studies that examine data protection, security, and the concept of privacy in general, more qualitative research is needed to investigate and understand more deeply how consumer privacy is perceived, in particular by young adults. Hence, this study focuses on examining how university students think about consumer privacy, and what meanings they ascribe to their experiences related to privacy invasions and surveillance in new media.

2. Literature Review

2.1 Concept of Privacy

Privacy as an abstract notion has always been a contentious concept. Bennett (1992) remarked that "attempts to define the concept of 'privacy' have generally not met with any success" (p. 25). Indeed, any review of the literature on privacy will indicate that the concept of privacy is complicated and difficult to define (Waldo, Lin, and Millett, 2007). As Westin (2003) explains, debates about privacy never end because they are tied to changes in the norms of society. As society changes so does the perception of privacy. Therefore, it is possible to say that perception of privacy is influenced by political, societal, and cultural factors (Ahituv, Bach, Birnhack, Soffer & Luoto, 2014).

Privacy is also a multidimensional concept. Privacy International (2006) identifies four different types of privacy: bodily privacy, territorial privacy, privacy of communication and information privacy. Back in the 19th century, both territorial and bodily privacies were the most predominant aspects of privacy protection. However, over the last 200 years, the focus of privacy has altered to communication of privacy and information privacy, where the violations are undertaken at a distance (Langheinrich, 2010). Therefore, in everyday usage, the term privacy generally refers to any type of behavioral, financial, consumer, biographical, medical and biometric information available about a person. Privacy is also related to the ability to gather, control, protect and use information about individuals (Waldo, Lin, and Millett, 2007).

Legal origins of privacy can be traced back to the late 19th century (Ruiz, 1997), when the U.S. Judge Thomas M. Cooley (1888) defined privacy as "the right to be let alone" (p. 29). However, the concept of privacy was popularized by Samuel Warren and Louis Brandeis when they penned their oft-cited article "The Right to Privacy" in 1890. Warren and Brandeis (1890) worried that technological developments in photography and the print media were invading privacy. They said "instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life" (p. 195). In the late 19th century, newspapers were the most rapidly growing form of media. Sensational "yellow" journalism was on the rise and the columns of daily papers were filled with idle gossip which they thought was overstepping privacy boundaries. Moreover, with the introduction of small and affordable cameras into daily life, ordinary people could take candid photographs. Warren and Brandeis feared the intersection of this technological development in photography with the gossip-hungry press (Solove, 2004; Richards & Solove, 2007).

The concerns Warren and Brandeis expressed more than a century ago show that the effect of technology on privacy is an old question of debate. However, in the age of new media and big data in which privacy has been surrounded by digital cameras, location-based services, facial recognition technologies, real-time urban monitoring systems, smart phones, and social media with user profile pictures and personal data, the debate on invasion of privacy has reached an all-time high.

2.2 Invasion of Consumer Privacy in Digital Communication

In the digital era, dealing in personal information has grown into a profitable industry. Recent developments in communication and computer technologies facilitate the collection of data about individuals that is used to build profiles of their behavior, sexual and political preferences, driving record, social networking activity and even health status (Prowda, 1995). In electronic shopping, it is almost impossible to accomplish a transaction without exposing some personal data (Ackerman, Cranor & Reagle, 1999). Personal information registered to a website might be used later for marketing purposes or sold to third parties. It is possible to track web surfing habits of users and merge them with their personal information. Cookies are used to collect information about visitors. Moreover; disabling cookies may cause some websites not to function properly (Cranor, 2002). Christiansen (2011) points out that websites apply three main methods to data collection. The first method is to anonymize and then aggregate the personal data collected from the web users in order to use it internally or to sell it to third parties. This aggregated information can be used to organize the content on the website or sell advertisements. This type of information helps advertisers determine the overall characteristics of the website's users. As it is not identifiable information, this method is not as invasive as the other methods. The second method is to specify a certain range of traits for advertisers doing target marketing. However, personal data is still kept within the website. The third method is used to collect personal data for the purpose of selling it to anyone interested. As this data may include specific names or profiles of consumers, it is the most intrusive type of data collection from the consumer privacy point of view. Although there are some privacy protection software products and services that allow consumers to remove existing cookies, they are not generally effective against web bugs, which are small graphic images that can be embedded in a webpage or e-mail for collecting information about users. Moreover, most users either do not know about such privacy protection tools or question their effectiveness. Some consumers are not concerned enough

about privacy to use them (Turner & Dasgupta, 2003).

Human tracking technologies are another face of privacy invasion. The accuracy and capabilities of tracking technologies such as geographical positioning systems (GPS) have increased since the year 2000. Mobile devices have become an essential part of social life. In addition, it is expected that GPS will be included in many different devices in the near future (van Schaik & van Der Spek, 2008). Technologies in GPS, wireless-fidelity (Wi-Fi) and cellular identification, which are often embedded in mobile devices that are connected invisibly and remotely to networks, have produced location-based services (LBS) (Cheung, 2014) such as GPS assisted navigation, travel guides, mapping services, fleet monitoring, local information services, tagging and check-in applications. Although LBS provide significant benefits to individuals and society, they pose serious risks to consumer privacy in that such technologies have the potential to enable third parties to locate and track people. Consumers who are unaware of this potential hazard may unknowingly grant companies the opportunity to assemble a detailed profile of their daily activities by using LBS (ACLU, 2010; Andrés, Bordenabe, Chatzikokolakis, Palamidessi, 2013). Delivering marketing messages to consumers' mobile devices via location-based services when they are physically close to businesses, which is sometimes called geo-targeted marketing (Queensland Government, 2014), is an example of use of human tracking technologies.

In reference to human tracking technologies, Dobson and Fisher (2003) point to what they call a "new form of slavery" defined by location control; they use the term "geoslavery" for "the practice in which one entity, the master, coercively or surreptitiously monitors and exerts control over the physical location of another individual, the slave" (p. 47). In such environments, where consumers are surrounded by new media technologies, privacy concerns are raised by the invasive surveillance conducted by corporations.

2.3 Consumer Privacy

According to Goodwin (1991) consumer privacy can be viewed in the context of any interaction between consumer and marketer and includes two dimensions of control. The first dimension is control of any unwanted intrusion in the consumer's environment while the second is related to control of information about the consumer. She defines consumer privacy as "the consumer's ability to control (a) presence of other people in the environment during a market transaction or consumption behavior and (b) dissemination of information related to or provided during such transactions or behaviors to those who were not present" (p. 152).

Westin (2003) asserts that, depending upon their changing personal needs, desires and will, people pursue an intrapsychic balance between their need for privacy and their needs for disclosure and communication, thus rendering privacy a complex issue and a matter of personal choice. Streitz (2011) also concludes that perception of privacy is context-dependent. For instance, some consumers seem to be willing to trade their privacy for the benefits that come from companies or service providers (Lauth, Berendt, Pfleging, Schmidt, 2012; Ahituv, Bach, Birnhack, Soffer, Luoto, 2014). The nature of information that consumers reveal is also important in perception of privacy. For instance, highly sensitive data such as telephone number, income, and health information trigger concerns over privacy. Although perceived company policy is an effective factor to lessen privacy concerns, it is not adequate when highly sensitive data are in question (Lwin, Wirtz, William, 2007). Phelps, Nowak, Ferrell (as cited in Phelps, D'Souza, Nowak, 2001) identified four general factors determining concerns of consumer privacy: (1) the type of personal information requested, (2) the amount of information control offered, (3) the potential consequences and benefits offered in the exchange, and (4) consumer characteristics. The complex nature of privacy brings up the question of whether or not it is possible to generalize about the attitudes towards privacy and personal information.

Westin conducted over 30 privacy surveys between the late 1970s and early 2000s. He classified the public into three segmentations in terms of general privacy concerns as follows: (1) Privacy fundamentalists, (2) Privacy unconcerned, and (3) Privacy pragmatists. Privacy fundamentalists are very sensitive about their privacy and therefore always skeptical about corporations' data collection practices. They are generally resistant to any further erosion of their privacy. At the other extreme, are those who are unconcerned about their privacy and are comfortable with corporations collecting their personal information and using them. They are mostly ready to waive their privacy rights voluntarily in order to gain some benefits from the corporations. The third and the largest group is privacy pragmatists who are not as sensitive as privacy fundamentalists about their privacy but still cautious. Privacy pragmatists believe that their trust should be earned – that is to say, they need to be assured by the government or corporations that personal information they share will not be misused. Privacy pragmatists always tend to weigh the risks and benefits of data sharing (Kumaraguru & Cranor 2005; Taylor, 2003). In 1998, 6, Lasky and Fletcher conducted a focus group study using the selection criteria of Westin's segmentation for the purpose of designing a survey. However, the recruiters stated that the sectorial distinction was not clear to many people. Moreover, during the sessions, the unconcerned group turned out to

be more fatalistic than unconcerned. Based particularly on their own focus group findings and the results of a large survey that they handled in the U.K., 6 et al. (1998) divided population into four groups by adding another category to Westin's three groups: privacy fatalists "who believe that there is little that they or anyone else can do to ensure proper use of personal information" (p. 2).

A qualitative research study conducted by the Australian Communications and Media Authority (ACMA, 2009) revealed that a similar fatalistic /resigned attitude was common across all focus groups. The findings showed that accepting the notion that invasion of privacy was inescapable may partly explain the lack of actions in protection of personal information among the participants.

In light of the researches referred to above, the purpose of this phenomenological study is to understand consumer privacy in new media for the participants. The main research question of the study is "How do the university students perceive consumer privacy in new media?" This main research question is divided into five sub-questions:

- How do new media affect the participants' perceptions of privacy in general?
- What are the main concerns of the participants about online shopping and protection of personal data?
- What are the feelings and attitudes of the participants towards online consumer privacy?
- What are the feelings and thoughts of the participants towards marketing activities in new media?
- What are the lived experiences of the participants regarding consumer privacy breaches in new media?

3. Methodology

3.1 Research Design

A qualitative research is appropriate if a researcher wants to understand the perspectives of participants and explore the meanings they give to phenomena (Green & Thorogood, 2004). In this study, the qualitative phenomenological design was used to understand how university students experience the phenomenon of consumer privacy in digital world and what meanings they ascribe to their experiences. Capturing and communicating meanings in empathetic and lucid ways are the goals of the phenomenological design (Berglund, 2007). The phenomenological design facilitates analyzing the perceptions of the participants and enables the interpretation of personal perspectives, which often generates insights into themes that may not be revealed with quantitative research (Fetters & Tilson, 2012).

3.2 Sample

Although a quantitative inquiry focuses on producing a statistically representative sample for generalization, a qualitative inquiry aims to select information-rich cases for study in depth. As Patton (1990) defined, "information-rich cases are those from which one can learn a great deal about issues of central importance to the purpose of the research" (p. 169). Therefore, a purposeful sample of 7 male and 7 female university students participated in the study. The students were recruited from the Ege University Faculty of Communication, which is located in Izmir, Turkey. Their ages ranged from 19 to 22, with an average of 20.07. Inclusion criteria were (a) regularly shopping online, and (b) using actively social media. Pseudonyms were used to protect the confidentiality of the participants in the study.

3.3 Procedure

The inquirers conducted in-depth, semi-structured interviews with the students who met the inclusion criteria. All interviews took place in April 2013 at the university campus. Each interview lasted between 45 and 60 minutes and proceeded until no new themes emerged. Demographic information was obtained through a questionnaire at the beginning of the interview. After obtaining informed consent, the participant was asked open-ended questions to obtain experiences, perceptions, and feelings about consumer privacy in new media. All interviews were held, transcribed and analyzed in Turkish. The inquirers tried to create an atmosphere of trust to obtain data from the participants in an honest manner.

3.4 Data Analysis

After verbatim transcription, a content analysis was conducted on the data. Content analysis refers to "any qualitative data reduction and sense-making effort that takes a volume of qualitative material and attempts to identify core

consistencies and meanings" (Patton 2002, p. 453). Following the steps recommend by Tesch (1990) and Creswell (2007), the transcripts were read several times to explore the general sense of the data. Then the process of coding the transcripts began. Firstly, the text segments in the data were identified and labeled with codes. The codes were examined for overlap and redundancy and finally the list of codes was reduced to six themes.

3.5 Trustworthiness

Several strategies were used to enhance the trustworthiness of the study and the quality of the findings. Purposeful sampling enabled the inquirers to deliberately select appropriate informants and collect rich information about consumer privacy (Patton, 1990). Member checking was achieved by providing the preliminary analyses to the participants and asking them to judge the accuracy of the findings and the interpretations of their feelings. With the exception of a few minor suggestions, which were implemented in the final document, the participants agreed that the findings were meaningful and consistent to their experience (Creswell, 2007). Thick description strategy, "the complete, literal description of the incident or entity being investigated" (Merriam, 2009, p. 43), is evident in the detailed information about the experiences and the verbatim quotes of the participants. Additionally, peer debriefing was conducted with a colleague who accompanied all stages and assisted the inquirers in verifying the data analysis and interpretation of the experience to "provide external check of the research process" (Creswell, 2007, p. 208).

4. Findings

4.1 Concerns about Online Shopping and Protection of Personal Data

The interviews with the participants generated a list of concerns about online shopping and protection of personal data. The probability of being a victim of identity theft, which includes criminal appropriation of someone's name, credit card information, identification number, home address and telephone numbers over the Internet, was the most mentioned concern among participants. Some of them revealed that they were scared to use their first credit card and delayed their first online shopping because of what they heard or read about identity theft. Ezgi (F, 20) explained it this way: *"People around me used to say, 'It is dangerous to shop on the Internet, you may get hacked and ripped off by crooks'.* Merve (F, 20) emphasized the fear of losing money: *"I was scared of getting hacked by identity thieves. I was scared they would assume my identity and spend my money".*

Other concerns were about getting a different product from the one that was ordered on the website, being overcharged on the credit card, or getting a fake or damaged product and not being able to return it to the retailer. However, almost all participants agreed that now they were less concerned about online shopping compared to their first experience because, with one exception, none of them has faced a major problem with shopping on the Internet. For example, Merve (F, 20) said, *"In my first online shopping experience, I was worried because I was required to give my credit card information. As I had some trust issues with the website, I asked my friend's advice. She told me that it was a reliable online store. Then I did my first online shopping. Now I do it with no hesitation."*

Most participants emphasized the importance of trust in online transactions. They said that the reputation of the vendor was vital to feel trust towards the website. As Alper (M, 22) put it, *"At first, I was scared to shop online because you have to give your personal data, but after a few tries, I got used to it. If you shop only on sites that you trust, you don't need to hesitate to place an order or you don't have to worry about whether you will get what you paid for."* Some participants mentioned that the design of the website was also significant for developing trust.

4.2 Effects of Social Media on Perception of Privacy

Most participants accepted that social media were an effective communication platform that helps them to keep in touch with friends and acquaintances, but they also stated that these media were breaching privacy. They associated social media with self-disclosure, self-exposure, self-indulgence, caring about nobody, swearing rashly and inconsiderately, bending rules, breaking taboos, blurring borders, showing off, and being unaware of negative consequences of users' actions. This issue was illustrated in the response of Yasemin (F, 21): "*I don't think people care about privacy that much anymore. We share almost everything on social media. We peep into other people's lives. Actually the borders of privacy are being redefined so it is hard to know whether we are inside or outside the borders. I just don't know."*

Two participants pointed out that some people they know in real life act differently on social media. Kemal (M, 21) and Merve (F, 20) made the following comments on this issue:

"Some introvert people around me are more relaxed on social media. Maybe it is easy to behave that way because you don't see each other face to face; you are not in the same physical place."

"Some people annoy me when they contradict themselves. They are defending conservative values in real life but later you see their daring pictures on social media; they are expressing themselves differently on the Internet."

On the other hand, almost all participants abstained from making a direct self-criticism about their attitudes on privacy matters in new media.

4.3 Check-in on Social Media

Most participants showed a particular interest in check-in as either a privacy breach or a consumer experience. Check-in on social media means to announce that you are at particular location via a social network by using a smartphone or any GPS capable mobile device. Consumers generally check-in at restaurants, cafés, hotels and other gathering spots. Location-based social media platforms, like Foursquare, in which consumers use check-in also, enable them to make comments on the business locations and their services.

4.3.1 Check-in as a Privacy Issue

Some of the participants indicated that telling everybody where you were via a social network was simply a privacy breach. Melis (F, 21) was very clear on this issue: *"Why should I expose myself that way? It is nobody's business where I am or what I am doing. This is my personal life.*" Aksu (F, 20) criticized people checking in at home. She believed that this could lead to severe invasion of privacy and some security problems: "*Some people check-in at home. That is to say 'Hey strangers, I live at this address.' I would never do that. As I told you, there is no privacy anymore."*

Some participants believed that the users who check in actually try to show off and make their friends jealous by checking in only at prestigious locations. According to these participants, this is a way of creating a false social status on social media. This was exemplified by Alper (M, 22): "*Nobody checks-in in a mom and pop grocery store, people check-in in Bodrum[1], at a popular café or at a beach. People check in to say, 'Hey look, I am a cool person and I can pay 20 TL for a cup of coffee at Starbucks."*

These participants also agreed that, in some cases, check-in is a way of sending an indirect invitation to a potential date.

4.3.2 Check-in as a Consumer Experience

Some participants, who had a positive attitude towards check-in, considered it as an interesting consumer experience. According to these participants, check-in was a way of sharing their experience with other customers, recommending others or discouraging them from trying something of poor quality, taking the opportunity for criticizing the services provided by the businesses and enjoying discounts. This positive attitude was expressed by Selin (F, 22): "*I like earning points and virtual badges on Foursquare, it has also other features as well. For instance, if it is my first time in a venue, I read the tips left by other customers. I sometimes make notations for myself to remember something about the venue for my next visit. If I order a meal in a restaurant, they give me a free dessert or drink for checking in. It is always great to get something free."*

4.4 Feelings and Attitudes towards Consumer Privacy in New Media

The feelings and attitudes of the participants towards consumer privacy in new media can be observed in four categories which can be stated as follows: 1. Resignation, 2. Indifference, 3. Preservation, 4. Opportunism.

4.4.1 Resignation /Fatalism

Although the participants falling into this category were uncomfortable with the invasion of digital privacy, they reported to continue using the Internet actively. According to these participants, there was not much to stop privacy breaches from

[1] *Bodrum is one of the most popular tourist destination in Turkey*

happening and hence they should be accepted as a part of modern life. They believed that if one wants to enjoy the opportunities the Internet provides such as shopping or banking online, there may be a price to pay. They conceived that the risks were inevitable and they despaired of things ever getting better in terms of consumer privacy. These participants also showed pessimism regarding consumer rights in near future. Yasemin (F, 21) and Metin (M, 19) made the following comments on this issue:

> *"– I think there is no escape from this. Even if I am very careful on the Internet, my electronic footprints are being tracked in real life when I do shopping with my credit or ATM card in a store. It is unavoidable. I don't know which of us can fully stop it. I think no one. Of course I don't like giving my personal data over the Internet but there is no other way, so we have to continue to keep up with this new world."*

> *"– This has become a part of modern life. Even email services want your mobile phone number to give you an account. Do they really need this info? No. But you can't have an email address unless you give your number."*

4.4.2 Indifference

The participants in this category regarded privacy breach as a matter of indifference. They were not worried about being tracked online as they have nothing to hide. They often declared that they don't do anything bad on the Internet. Hence, they generally don't mind companies collecting their personal data. This was explained by Ezgi (F, 20): "*All I do is shopping but nothing else. Why should I be worried about collection of data about me? If the company sells my personal data to other companies or banks, they get low marks from me but does it stop me from shopping online? I don't think so."*

Volkan (19) accentuated that the data shared on social media was part of the deal between social media sites and consumers: *"– I don't understand the people feeling uncomfortable with the social networking sites using or selling the data the users shared on the social media. You read and accepted the user agreement before clicking the sign up. Then you can't say 'my personal data is being shared with third party companies'. That is the part of the deal."*

Selin (F, 22) said, '*Not just me, but everybody else is sharing their personal data. The companies know my address or my mobile phone number, so what about it? They know addresses of millions of consumers."*

In fact, these students voluntarily give their personal data because they believe the data collected on their habits and preferences will be used by the companies to make their life easier. These students also believe that the risks are being exaggerated.

4.4.3 Preservation and Concern

The participants in this category think that the invasion of consumer privacy in new media is an emerging issue that has to be taken seriously. These students believe that the risks are high, so it is necessary to take some precautions. To reduce privacy breach risks, they avoid giving their mobile phone numbers, and ID card information when possible. They don't complete optional information fields on websites. They provide only bare minimum information and use fake e-mail addresses for the memberships. They only buy from reliable websites and rarely or never check in. In short, they are very meticulous about everything they do on the Internet. Their goal is to remain anonymous as much as possible in the digital world. It is correct to conclude that these participants have a strong sense of preservation of their privacy. For example, Mert (M, 20) saw it as a moral issue: *"I don't like the idea that companies can track me when I am online. It is not right to monitor consumers. It is ethically wrong. I don't like anyone knowing where I am and what I am doing."* Aksu (F, 20) found behavioral targeting frightening: *"We are exposed to more targeted ads than ever on social networks. This may be profitable for the companies using this service but I don't think it is right. It's sinister."* Alper (M, 22) emphasized the importance of remaining anonymous: *"I don't think check-in and other location-based services make our life easier. They are designed to identify us personally".*

4.4.4 Opportunism

The participants in this category generally believed that the Internet increased the competition among vendors and created major opportunities to bring benefits to the consumers. These participants were generally willing to exchange their personal data for getting better services from the companies. They associated this exchange with discounts, special offers, free gifts, dumping, opportunities, time- and money-saving benefits and tips for making life easier. In addition, they generally defended the idea that if the companies track consumers' online behavior and their viewing habits to create new

sources of revenue and profit for themselves, and if there is no way to stop this monitoring, then it is the consumers' right to demand their share from this wealth. Volkan (M, 19) and Selin (F, 22) made the following comments on this issue:

> *"–What do I think of my personal data being shared with third parties? Well, I don't think it is morally right but if they offered a special discount in turn, I would take it."*

> *"I do check in irrespective of whether they give me a discount or not, so why wouldn't I benefit from it, if they offered me something good?"*

4.5 Attitudes towards Marketing Activities in New Media

The participants' attitudes towards marketing activities on new media can be divided into two subcategories as follows: 1) Positive Attitude: Feeling Special and Privileged, 2) Negative Attitude: Skeptical.

4.5.1 Positive Attitude: Feeling Special and Privileged

The students with positive attitude towards marketing activities on new media said in general that they benefit from the relationships they have with the companies. For these students, these relationships mean enjoying customized products and services, receiving personalized messages, and benefiting from special offers, discounts and free gifts, all of which they regard as being noticed and cared about by the companies. This care makes them feel special and privileged. The following quote from Metin (M, 19) exemplified the effect of personalization on the consumer:

> *"Yes, I have a supermarket membership card. I gave my home address, telephone number, e-mail and some other details about myself to get that card. You earn points by shopping with it. They send me some personalized messages addressing me by my name, and they inform me about their discounts. I like this. I feel special."*

Ezgi (F, 20) talked about how ads on the social network made her life easier*: "The targeted ads on Facebook don't annoy me. On the contrary, they make my life easier because they advertise the products and the services that I am already interested in. If they catch my eye, I click on them. It's that easy. The companies and Facebook have a contract on targeted ads. This is how Facebook makes money."*

4.5.2 Negative Attitude: Skeptical

The participants who were skeptical about marketing communications in new media believed that the relationship between consumers and companies is not mutually beneficial; in fact, the companies take advantage of consumers by monitoring their online behaviors without permission and use this knowledge against consumers to sell them more. The participants also thought that this data collection may lead to identity theft because the companies cannot guarantee the security of the data. Aksu (F, 20) explained her thoughts on personalization of the marketing messages on Facebook: *"Why do they put those targeted ads on Facebook? They do this to sell their products and services. I don't need that. I can do the search by myself. I can find the proper product or service by myself. I like exploring them by myself. I find targeted ads sinister. Actually, these ads don't draw my attention at all."*

4.6 Experiences Related to Privacy Breaches in New Media

When the participants were asked about whether they experienced a privacy breach in new media, some of them revealed that their Facebook, e-mail and MSN Messenger accounts were hacked. The prior concern among those participants was the fear of losing reputation within society due to hackers pretending to be them on social media. For example, Melis (F, 21) said, "*When my Facebook account got hacked, I was afraid of losing face because the hackers could tarnish my image on social media. My Facebook account is something representing me."*

Alper (M, 22) reported a similar concern: "*A few years ago, my e-mail password was stolen. I was freaked out that this guy may pretend to be me and send out to all my contacts slanderous remarks about me or make an indecent proposal to someone I know. I tried to reach my contacts and informed them that my email account had been hacked and asked them to ignore any messages coming from that mail address."*

Metin (M, 19) revealed his confused feelings over the hacking of his MSN Messenger account and mentioned his Internet addiction: "*My MSN Messenger account was hacked once. The hacker posing as me asked my father to send*

him some money. I was so furious when I first realized what was going on but I didn't know what to do. And for the first time I thought how easy things may get out of control on the Internet. I thought to stop using it. But that was impossible. We are all addicted to the Internet"

Kemal (M, 21) was the only person who had his credit card information stolen while shopping online. He didn't realize it until he got the credit card statement. He stated, "*That was a long time ago. My credit card was hacked and 290 TL were spent. Thank God, it had a limit of 400 TL. When I received my credit card statement, I got angry and felt like a fool. The first thing I did was to format my computer. I don't use antivirus software anymore because I believe antivirus developers create these viruses."*

In addition, almost all participants complained about receiving unsolicited and unrelated text messages on their mobile phones, which they regarded as an invasion of privacy. They found these commercial messages annoying and intrusive because they perceive their mobile phones to be for personal communication. In general, the participants who experienced a privacy breach explained that they felt helpless and furious because of what happened to them.

Interestingly, none of the participants reported any privacy breaches related to online tracking via cookies, storage of browsing habits of consumers and the sale of personal data to third parties. When asked, some of the participants said that they didn't regard these practices as privacy breaches unless they affected them directly or personally, which meant losing money or prestige. Some participants reported that these practices were not the first things that came to mind when thinking about privacy breaches in new media. These participants said they didn't know about such practices or were not aware of being exposed to them.

5. Discussion

This study provides some insights into the perceptions of consumer privacy among university students in Turkey. Several themes regarding consumer privacy were revealed in in-depth, semi-structured interviews with the students.

Most students believed that the Internet and particularly social media were changing the perception of general privacy in a negative way. They particularly criticized their friends and acquaintances on Facebook for sharing private information. This finding is consistent with the study of Cavalli et al. (2011) who found a negative perception of Facebook related to over-exposure of personal matters among Italian students. Another finding was that unsolicited and unrelated text messages on mobile phones and direct marketing calls were regarded as an invasion of privacy. Tsang, Ho, Liang (2004) reached a similar result that "consumers have generally negative attitudes towards mobile advertising unless they have specially consented to it" (p. 65). Therefore, mobile marketing should be permission based and content should be relevant, useful and entertaining (Al-alak, Alnawas, 2010). Most students stated that the more experienced they became about online shopping, the less concerned they were about identity theft or any potential problems related to online shopping. Similar results can be found in Hernandes' (2009) research which examined the main motives, risks and trust attributes of experienced online shoppers. The students in this study also pointed out that trust was positively related to purchase intention, which seems to be consistent with research by Milne & Boza (1999) and Choi, Sohn & Lee (2010). In addition, the students revealed that the design quality of the website is a significant factor for developing trust towards vendors. This finding is supported by some previous research (Safari, 2012; Chang & Chen, 2008).

Another important finding was identification of four distinct attitudes towards privacy: resignation, indifference, opportunism and preservation. An attitude of resignation was detected and reported as fatalism by 6, Lasky and Fletcher (1998) and ACMA (2009) in their previous research. In addition, the students from the category of preservation and indifference have characteristics similar to the privacy fundamentalists and privacy unconcerned groups in Westin (2003). However, there are differences between the students in the opportunism category and the privacy pragmatists. The privacy pragmatists are sensitive about privacy issues, and they need to understand the reasons why and how corporations use their data; they are in a struggle as they weigh the risks and benefits of data sharing, whereas the students in the opportunism category don't seem to make such effort; they are aware that corporations take advantage of data collection, and hence think that they should receive more benefits in return for the data they provide to companies. Therefore, it is possible to say that students falling into the categories of resignation, indifference and opportunism have similar attitudes or behavioral preferences in terms of data sharing although they differ slightly in their discourse about privacy issues. These students use the Internet actively and are less careful to reduce the risks of privacy breaches. Indeed, most of the students can be classified in more than one category. In other words, there are no absolute boundaries between those three groups. For example, a participant showing indifference to consumer privacy is likely to be an opportunist or vice versa. However, the students in the category of preservation differ from the rest by the fact that they share bare minimum personal data and take some serious precautions to preserve their privacy. While the students from the other three categories generally have positive attitudes towards companies' marketing activities in new media,

the students with preservation attitude regard those activities as sinister and insidious.

Since this study is based on a small homogeneous sample, the findings should not be generalized to all situations. Further research is needed to confirm and understand how university students perceive consumer privacy in new media and how their attitudes differ among themselves and from other groups in society.

References

6, P.; Lasky, K., & Fletcher, A. (1998). The Future of Privacy, Vol. 2: Public Trust and the Use of Private Information. London: Demos

Accenture (2014). Eighty Percent of Consumers Believe Total Data Privacy No Longer Exists, Accenture Survey Finds, Retrieved from http://newsroom.accenture.com/news/eighty-percent-of-consumers-believe-total-data-privacy-no-longer-exists-accenture-survey-finds.htm

Ackerman, M. S., Cranor, L. F., & Reagle, J. (November 1999). "Privacy in e-commerce: Examining User Scenarios and Privacy Preferences." In Proceedings of the 1st ACM Conference on Electronic Commerce, 1-8

ACMA (2009). Attitudes towards Use of Personal Information Online: A qualitative Report, Commonwealth of Australia, Australian Communication and Media Authority: Melbourne

Ahituv, N., Bach, N., Birnhack, M., Soffer, T., & Luoto, L. (2014). "New Challenges to Privacy Due to Emerging Technologies and Different Privacy Perceptions of Younger Generations: The EU PRACTIS project". Proceedings of Informing Science & IT Education Conference (InSITE) 2014, 1-23

Al-alak, B.A., & Alnawas, I. A. M. (2010). "Mobile Marketing: Examining the Impact of Trust, Privacy Concern and Consumers' Attitudes on Intention to Purchase". International Journal of Business and Management 5 (3) 28-41

Allen, A. L. (2000). "Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm". Faculty Scholarship. Paper 790. Retrieved from http://scholarship.law.upenn.edu/faculty_scholarship/790

American Civil Liberties Union (November 2010). Location-Based Services: Time for a Privacy Check-In, An ACLU of Northern California publication. Retrieved from www.aclunc.org/tech, 1-23

Andrés, M. E; Bordenabe, N. E.; Chatzikokolakis, K. & Palamidessi, C. (2013, November). "Geo-Indistinguishability: Differential Privacy for Location-Based Systems". In Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. New York: ACM, 901-914

Annalect (2013). "Consumer Online Privacy". Retrieved from http://www.annalect.com/how-well-do-you-understand-consumer-online-privacy/

Bennett, C. J. (1992). Regulating Privacy: Data Protection and Public Policy in Europe and the United States, New York: Cornell University Press

Berglund, H. (2007). "Researching Entrepreneurship as Lived Experience". In Handbook of Qualitative Research Methods in Entrepreneurship, ed. Neergaard, H. & Ulhøi, J. Cheltenham, UK & Northampton MA, USA: Edward Elgar, 75-93

Cavalli, N.; Costa, E. I.; Ferri, P.; Mangiatordi, A.; Micheli, M.; Pozzali, A.; Scenini, F. & Serenelli, F. (May 2011). "Facebook Influence on University Students' Media Habits: Qualitative Results from a Field Research". In International Conference MIT7 Media in Transition-Unstable Platforms: The Promise and Peril of Transition

Chang, H. H. & Chen, S. W (2008). "The Impact Of Online Store Environment Cues on Purchase İntention: Trust and Perceived Risk as a Mediator" . Online Information Review 32(6) 818–841

Cheung, A. S. Y. (2014). "Location Privacy: The Challenges of Mobile Service Devices". Computer Law & Security Review 30: 1-5

Choi, J.; Sohn, C. & Lee, H. J. (2010). "The Impact of Multi-dimensional Trust for Customer Satisfaction". Management Science and Financial Engineering, 16(2) 81-97

Christiansen, L. (2011). Personal Privacy and Internet Marketing: An Impossible Conflict or a Marriage Made in Heaven?". Business Horizons 54 (6) 509-514

Cooley, T. M. (1888). A Treatise on the Law of Torts, 2nd ed. Chicago: Callaghan & Co.

Cranor, L. F. (2002). Web Privacy with P3P. Sebastopol CA, USA: O'Reilly & Associates

Creswell, J. (2007). Qualitative Inquiry and Research Design: Choosing among Five Traditions, 2nd ed. Thousand Oaks, CA: Sage

DeCew, J. W. (1997). In Pursuit of Privacy: Law, Ethics, and the Rise of Technology. Ithaca: Cornell University Press

Dobson, J. E., & Fisher, P. F. (2003). "Geoslavery".Technology and Society Magazine, IEEE 22 (1) 47-52

Fetters, L. & Tilson, J. (2012). Evidence Based Physical Therapy. Philadelphia: F. A. Davis Company

Goodwin, C. (1991). "Privacy: Recognition of a Consumer Right". Journal of Public Policy & Marketing 10(1) 149-166.

Green, J. & Thorogood, N. (2004). Qualitative Methods for Health Research, London: Sage Publications

Hernandes, J. M. (2009). "Motives, Risks and Trust in Online Shopping: A study among Experienced Internet Users-Shoppers". Unpublished Master's Thesis, Dublin Business School (DBS), Dublin, Ireland

Hoffman, D. L.; Novak, T. P. & Peralta, M. (1999). "Building Consumer Trust Online". Communications of the ACM, 42(4) 80-85

Kumaraguru, P. & Cranor, L. F. (December 2005). "Privacy Indexes: A Survey of Westin's Studies", Institute for Software Research International, Carnegie Mellon University. CMU-ISRI-5-138. Retrieved from http://www.cs.cmu.edu/~ponguru/CMU-ISRI-05-138.pdf

Langheinrich, M. (2010). "Privacy in Ubiquitous Computing". In Ubiquitous Computing Fundamentals, ed. John Krumm. Boca Raton, FL: Chapman & Hall / CRC Press, 95-159

Lauth, C.; Berendt, B.; Pfleging, B. & Schmidt, A. (2012). "Ubiquitous Computing". In Handbook of Technical Communication, ed.

Alexander Mehler, Laurent Romary, Berlin/Boston: Walter de Gruyter, 735-770
Lwin M.; Wirtz J. & William, J. D. (2007). "Consumer Online Privacy Concerns and Responses: A Power–Responsibility Equilibrium Perspective". Journal of Academy of Marketing Science 35, 572–585
Merriam, S. B. (2009). Qualitative Research: A Guide to Design and Implementation. Hoboken NJ: John Wiley &Sons, Inc.
Milne, G. R., & Boza, M. E. (1999). "Trust and Concern in Consumers' Perceptions of Marketing Information Management Practices". Journal of Interactive Marketing 13(1) 5-24
Patton, M. (1990). Qualitative Evaluation and Research Methods. Beverly Hills, CA: Sage.
Patton M. Q. (2002). Qualitative Research and Evaluation Methods, 3rd ed., London: Sage Publications
Phelps, J. E.; D'Souza, G. & Nowak, G. J. (2001). "Antecedents and Consequences of Consumer Privacy Concerns: An Empirical Investigation". Journal of Interactive Marketing 15(4) 2-17
Privacy International (2006). Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments
Prowda, J. B. (1995). "Privacy and Security of Data". Fordham Law Review 64(3) 738-769
Queensland Government (2014). How Location-Based Marketing Works. Retrieved from http://www.business.qld.gov.au/business/running/marketing/online-marketing/using-location-based-marketing-to-promote-your-business/how-location-based-marketing-works
Richards, N. M. & Solove, D. J. (2007). Privacy's Other Path: Recovering the Law of Confidentiality, 123-182 Retrieved from http://ssrn.com/abstract=969495
Ruiz, B. R. (1997). Privacy in Telecommunications: A European and an American Approach. The Netherlands: Kluwer Law International
Safari A. (2012). "Customers' International Online Trust - Insights from Focus Group Interviews". Journal of Theoretical and Applied Electronic Commerce Research 7(2) 59-72
Schaik, J. van & Spek, S. van Der (2008). "Urbanism on Track- Expert Meeting on the Application of GPS-based and Other Tracking-based Research in Urban Design and Planning.". The Architecture Annual. Rotterdam: 010 Publishers, 40-43
Solove, D. J. (2004). The Digital Person: Technology and Privacy in the Information Age. New York and London: New York University Press
Streitz, N. A. (2011) "Smart Cities, Ambient Intelligence and Universal Access". In Universal Access in Proceeding of Human–Computer Interaction: Context Diversity, ed. Constantine Stephanidis. Springer-Verlag: Berlin & Heidelberg, 425-432
Taylor, C. & Wagman, L. (2014). "Consumer Privacy in Oligopolistic Markets: Winners, Losers, and Welfare". International Journal of Industrial Organization 34, 80–84
Taylor, H. (2003). "Most People Are 'Privacy Pragmatists' Who, While Concerned about Privacy, Will Sometimes Trade It Off for Other Benefits, the Harris Poll" (17) Retrieved from http://www.harrisinteractive.com/vault/Harris-Interactive-Poll-Research-Most-People-Are-Privacy-Pragmatists-Who-While-Conc-2003-03.pdf
Tesch, R. (1990). Qualitative Research: Analysis Types and Software Tools. Bedford: Routhledge, LSL Press Ltd.
Tsang, M. M.; Ho, S. C. & Liang, T. P. (2004). "Consumer Attitudes toward Mobile Advertising: An Empirical Study". International Journal of Electronic Commerce 8(3) 65-78
Turner, E. C. & Dasgupta, S. (2003). "Privacy on the Web: An Examination of User Concerns, Technology, and Implications for Business Organizations and Individuals". Information Systems Management. 20(1) 9-18
Van Dijk, J. A. G. M. (2006). The Network Society: Social Aspects of New Media, 2nd ed. London: SAGE Publications
Waldo, J.; Lin, H. S. & Millett, L. I. (2007). Engaging Privacy and Information Technology in a Digital Age. Washington: The National Academies Press
Warren, S. D. & Brandeis, L. D. (1890). "The Right to Privacy". Harvard Law Review 4(5) 193-220
Westin, F. A. (2003). "Social and Political Dimensions of Privacy". Journal of Social Issues 59(2) 431-453
Westin, A. F. (1967). Privacy and Freedom. New York: Atheneum
Yousafzai, S. Y.; Foxall, G. R. & Pallister, J. G. (2010). "Explaining Internet Banking Behavior: Theory of Reasoned Action, Theory of Planned Behavior, or Technology Acceptance Model?" Journal of Applied Social Psychology 40(5) 1172–1202