PressAcademia Procedia - (PAP), ISSN: 2459-0762

PressAcademia Procedia

2nd World Conference on Technology, Innovation and Entrepreneurship
May 12- 14, 2017, Istanbul, Turkey. Edited by Sefer Şener

CONSUMER PRIVACY IN THE ERA OF BIG DATA: A SURVEY OF SMARTPHONE USERS' CONCERNS

DOI: 10.17261/Pressacademia.2017.509
PAP-WCTIE-V.4-2017(1)-V.4-p.1-10

Tevfik Sukru Yaprakli[1] Musa Unalan[2]
[1]Ataturk University. sukruyaprakli@atauni.edu.tr
[2]Ataturk University. musa.unalan@atauni.edu.tr

ABSTRACT

Smartphones increase rapidly and become high-speed mobile data networks progressively appearing everywhere in the recent years. Also, there is a large and ever increasing number of mobile phone applications on the market. In this case, consumer privacy become critically important because sellers might access a large volume of personal information. This paper attempts to identify the consumer privacy and concerns in the context of big data and to explore how consumers' demographic differences may affect their concerns for information privacy. The smartphone owners' demographic differences and their concerns over privacy are analyzed, based on a survey of 392 smartphone users in Erzurum. It has been found that consumers' demographic differences have varying degrees of impact on their concerns for information privacy in the context of big data.

Keywords: Big data, consumer privacy, privacy concerns, smartphone users.
JEL Codes: G10, G32

1. INTRODUCTION

Although the internet wasn't widely accessible all over the world with just 400 million internet users in 2000, the numbers have soared high up to 3.2 billion internet users globally by the end of 2015 (Union 2015). By 2018, according to eMarketer, nearly half of the world's population, or 3.6 billion people, will access the internet at least once each month (eMarketer 2014a). A mobile phone market which was 4.08 billion users globally in 2012 grew by 6.2% in 2013 to 4.33 billion users. The mobile market was supposed to grow by 5.1% to 4.55 billion users in 2014 and further by 4.7% to 4.77 billion users. The worldwide smartphone market grew 13.0% over year in 2015 Q2, with 341.5 million shipments, according to data from the International Data Corporation (IDC) Worldwide Quarterly Mobile Phone Tracker (IDC 2015). A total mobile phone users are likely to reach 5.13 billion users globally by 2017 (eMarketer 2014b). Among the mobile phone users, there were around 1.13 billion smartphone users in 2012 i.e. around 28% of global smartphone users. The number of smartphone users was further expected to increase by 22.5% to 1.75 billion users in 2014, which was around 39% of mobile users. Around 49% i.e. nearly half of the mobile phone users globally are likely to use smartphone by 2017. (eMarketer 2014b)

These data give what happens in this area. Using of the internet and mobile devices have spread across the world. Wade (2014) note that we can surf the web on a smartphone, read the newspaper on an e-reader and access e-mail virtually anywhere. It means that technology has become an integral part of our lives. Currently, there are varieties of information including personal data, social network data, and location data in mobile apps (Keith et al. 2014). Therefore, mobile apps have become the most appropriate device for collecting consumer information in one device. (Keith et al. 2014). However, these applications and services also introduce a range of new threats to users' privacy. While a user carries it, a mobile device can capture a complete record of the user's location, online activities, and social encounters, potentially including an audio-visual record (Aditya et al. 2014).

While there are benefits of having access to mobile apps, using applications in a bad way increase privacy concerns for mobile phone users. Thus, many academic researchers became interested with information privacy (Culnan and Armstrong

1999; Malhotra et al. 2004; Smith et al. 2011; Chen et al. 2015; Hirose et al. 2016). This shows that consumer privacy is an important issue. Because of no quantitative studies that examine privacy in the era of Big Data in Turkey, we investigate to how consumer privacy is perceived, in particular by smartphone users. The rest of paper is as follows:

- This paper provides a review of the prior literature to introduce the theoretical background of studying information privacy, privacy concerns in Big Data.
- This paper attempts to contribute by studying the privacy issues in the context of the smartphone within Erzurum, and more specifically, the relationships between consumers' demographic differences and their information privacy concerns.
- This is followed by a description of the research methodology and findings
- The smartphone owners' demographic differences and their concerns over privacy are analyzed, based on a survey of 392 phone users in Erzurum.
- The paper concludes with a discussion of the main results in relation to the existing literature, directions for future research.

2. CONSUMER PRIVACY IN THE ERA OF BIG DATA

Huaiqing Wang et al. (1998) define privacy as "the right to be let alone," which is interested in solitude, secrecy, and autonomy. It is also related to the ability to gather, control, protect and use information about individuals (Waldo et al. 2007). You can also express privacy that refers to any kind of behavioral, financial, consumer, biographical, medical and biometric information available about a person (Koseoglu and Koker 2015). When we look to how we define to privacy in an era of big data with mobile devices, Shilton (2009) defines privacy as "the ability to understand, choose, and control what personal information you share, with whom, and for how long" (p. 50).

On the other hand, the definition of consumer privacy from Goodwin (1991) is "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). Youn (2009) defines consumer privacy as "consumers' ability to control when, how, and to what extent their personal information is to be transmitted to others" (p. 391).

Smartphones have achieved significant penetration. They have a range of additional capabilities, including image/audio/video recording, GPS location, compass, accelerometer, near-range radio (NFC and Bluetooth) (Aditya et al. 2014). Besides this, the smartphones also include advanced computing and communication facilities, such as location-tracking or position-aware applications, which can be used by mobile phone companies, relatives, and friends, or third parties, to identify the specific location of a mobile phone user (Leek and Christodoulides 2009). Smartphones also include multiple functions which can be listed as web browsers, emails, photo albums, games, calendars, and contact lists, and also through apps they can collect much information about consumers such as identity, upcoming schedule, time spent on different apps, contact lists, real-time location, etc. (Xu et al. 2012). For this reason, the personal information of consumers starts to become a commodity.

Taylor and Wagman (2014) emphasized that governments, firms, data aggregators and other interested parties collect, store and analyze data about consumers for easily obtained information. They can collect the personal information about users via mobile devices especially smartphones because they think that personal data is the new great opportunity of the internet (Spiekermann et al. 2015). For example, The Wall Street Journal revealed that, when the 101 popular smartphone apps examined, 56 apps transmitted the phone's unique identifiers to other companies without users' awareness and 47 apps transmitted the phone's location to outsiders. (Thurm and Kane 2010). It was further found that both Apple IOS and Google Android mobile operating systems regularly record and transmit location data without the consent of device owners (Angwin and Valentino-Devries 2011). This shows that sometimes we cannot regulate the applications to control our privacy information (Wade 2014). The information automatically collected by applications and distributed other channels (Xu et al. 2012).

However, there is a lack of understanding of what consumers think about the data collection and using their personal information that is getting from applications as a result of their mobile phone use. People want to use mobile applications for a variety of different functions (Gomez-Martin 2011). For example, they want to use any applications for their interests such as games, tutorials on various lifestyle topics, social networking, and banking etc. (Gomez-Martin 2011). Even though there are series of threats and problems, consumers have to use mobile phones for many advantages. It does not mean that consumers do not care this issue. On the contrary, mobile phone users are concerned about their privacy when their personal information is shared others without any permission or consent (Phelps et al. 2000). Consequently, their behaviors are affected by these concerns (Pan and Zinkhan 2006). For instance, a recent study shows that Ovum's Consumer Insights of 11,000 respondents from 11 countries confirms that consumers are concerned about privacy issues in the era of Big Data. Sixty-eight percent of these respondents indicate that they prefer a "do-not-track" (DNT) feature if available (Network

World Asia, 2013). In order to reduce the problem, these privacy concerns should be solved (Gurau and Ranchhod 2009). Because consumer users do not want to leak their personal information such as their name, address, location, login credentials, contacts, emails, photos, and other files (Wetherall et al. 2011).

Most of the existing studies are addressing the issue of privacy with big data (Yu et al. 2015; H. Wang et al. 2015; Quinn 2015; Liu 2015; Combe 2015; Kshetri 2014; Hahn 2014; Gaff et al. 2014; Cate 2014; Bardi et al. 2014; Karabey 2012) and consumer privacy with mobile environment, mobile devices (Zhang et al. 2013; Okazaki et al. 2009; Praher and Praher 2008; Holtmanns 2002; Buck et al. 2014)

All the happenings show that ''we live in an era of an explosion of data'' (Landau 2015). In light of the many studies and which is referred to above, the purpose of this study is to understand consumer privacy in the era of big data. The main research question of the study is "How do the smartphone users perceive consumer privacy in the era of Big Data?"

3. RESEARCH METHODOLOGY

The purpose of the research model is to how to test consumers' demographic differences such as gender, income, age and education level may affect their privacy concerns on mobile devices.

The questionnaire was applied to 392 randomly selected mobile phone users during November-December 2015, in a location of Turkey which name is Erzurum. All respondents included in this study indicated that they were smartphone users. The questions were designed to collect information about the demographic profile of respondents which can be listed as age, gender, education level and income and the level of respondents' about privacy concerns and personal information.

Privacy concerns were measured by items developed from Boyles et al. (2012). The collected data have been analyzed using the SPSS 20 software package. In line with the exploratory approach adopted in this study, the statistical methods used to analyze the data were frequency, cross-tabulations, and the Chi-square test.

4. RESULTS

A total of 392 participants were included in the sample. The participants were recruited from the Erzurum. The gender distribution was 206 (52.6%) males and 186 (47.4%) females. Their ages ranged from 17 to 50 and over. A majority of respondents (53.8%) are within the age range of 17 to 24. In terms of education level, about 11.5% are high school, about 13.3% are college, about 53.3% are undergraduate, and the remaining 21.9% are postgraduate participants. Out of 392 respondents who reported monthly income level, about 52.8% are less than 1000 Turkish Lira.

4.1. Gender Analysis

Through analyzing investigations results from the questionnaires, the following features of privacy concerns and personal information in different genders are observed.

The degree of privacy concerns and personal information from females is obviously lower than males in the data collection by mobile users. Among the 7 variables, only ''phone has been lost or stolen'' and ''back up phone contents'' are proved to be true, and there is a difference between them, which is shown in Table 3.

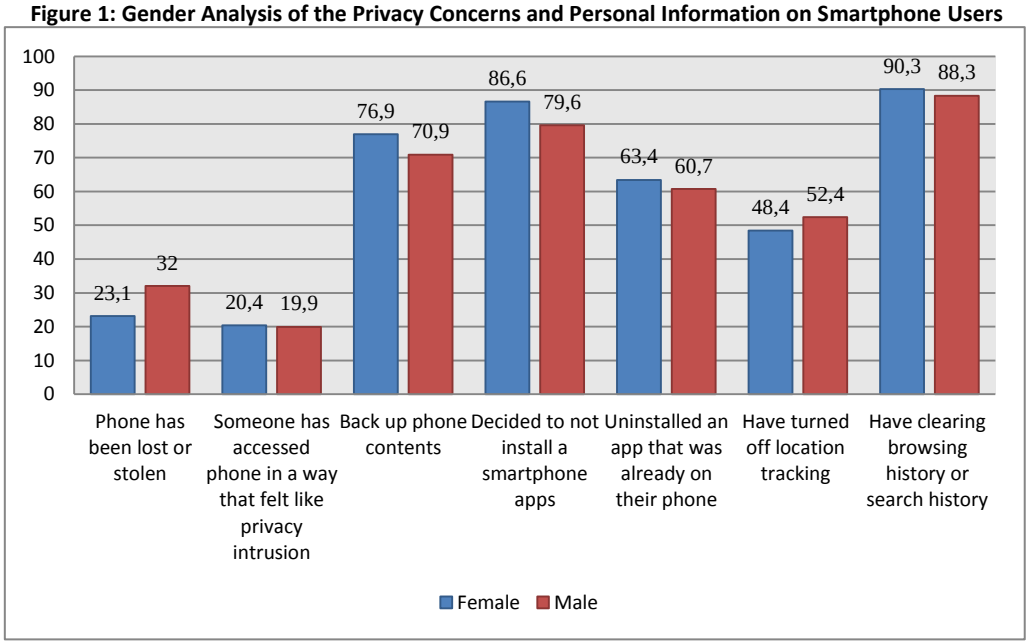
Table 3: Gender Analysis of Privacy Concerns and Personal Information

Questions	p-Value	Female	Male
1. Phone has been lost or stolen	<0.05	39.4%	60.6%
2. Someone has accessed phone in a way that felt like privacy intrusion	0.897	48.1%	51.9%
3. Back up phone contents	<0.05	49.5%	50.5%
4. Decided to not install a smartphone app	0.068	49.5%	50.5%
5. Uninstalled an app that was already on their phone	0.574	48.6%	51.4%
6. Have turned off location tracking	0.424	45.5%	55.5%
7. Have clearing browsing history or search history	0.528	48.0%	52.0%

Note: Chi-square test was used. If p-value < 0.05, there was a statistically significant difference between the female and the male.

In general, when we look at Figure 1, the proportion of the females about privacy concerns is higher than males. It is shown in the data that 76.9% of the respondents who back up phone contents are females, and females account for 86.6% of the respondents who decided to not install smartphone applications. Besides, the proportion of males who have turned off location tracking is higher than females. It is learned from the questionnaires that females worried about privacy concerns than males.

Figure 1: Gender Analysis of the Privacy Concerns and Personal Information on Smartphone Users



4.2. Age Analysis

Based on the investigation results from the questionnaires, features of privacy concerns and personal information of respondents from different age groups can be summarized as follows:

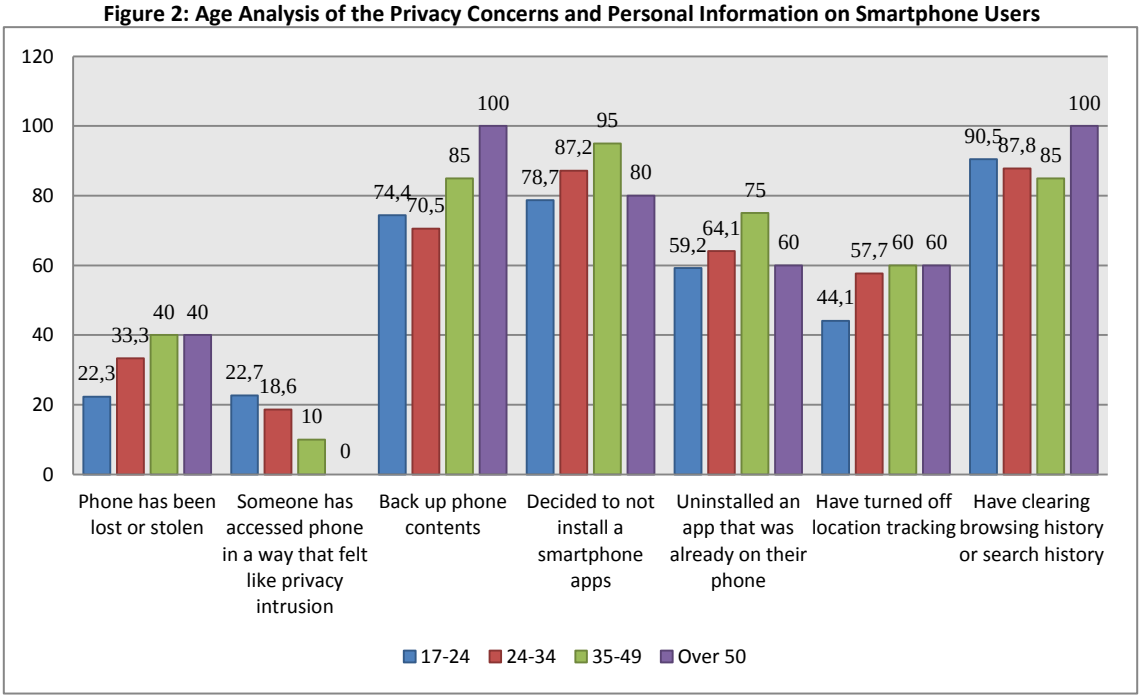
Respondents between 35 and 50 years old are more suspicious of the data collected by organizations (Table 4). The reason obtained through the questionnaires is that people of this age group have accumulated a certain amount of savings and thus pay much attention to privacy protection, whereas people who are between 17 and 24 years old do not care much about this because they do not have any savings and have nothing to lose.

Table 4: Privacy Concerns and Personal Information Analysis of Respondents from Different Age Groups

Questions	p-Value	17-24	25-34	35-49	Over 50
1. Phone has been lost or stolen	0.059	43.1%	47.7%	7.3%	1.8%
2. Someone has accessed phone in a way that felt like privacy intrusion	0.300	60.8%	36.7%	2.5%	0.0%
3. Back up phone contents	<0.05	54.3%	38.1%	5.9%	1.7%
4. Decided to not install a smartphone app	0.080	51.1%	41.8%	5.8%	1.2%
5. Uninstalled an app that was already on their phone	0.490	51.4%	41.2%	6.2%	1.2%
6. Have turned off location tracking	0.055	47.0%	45.5%	6.1%	1.5%
7. Have clearing browsing history or search history	0.643	54.6%	39.1%	4.9%	1.4%

Chi-square test was used. If p-value < 0.05, there was a statistically significant difference among those groups. Looking at the results for Figure (2) below we see the percentage of respondents for each age group asked about the extent to which they agree with the following statements about their privacy. We observe that except second statement the other all statements which refer to a high degree of privacy concern, as age increases the proportion of mobile users with the high degree of privacy concerns increases.

Figure 2: Age Analysis of the Privacy Concerns and Personal Information on Smartphone Users



4.3. Education Background Analysis

Through analysis of investigation results from the questionnaires, features of the attitudes toward privacy protection from respondents with different education backgrounds are summarized as follows:

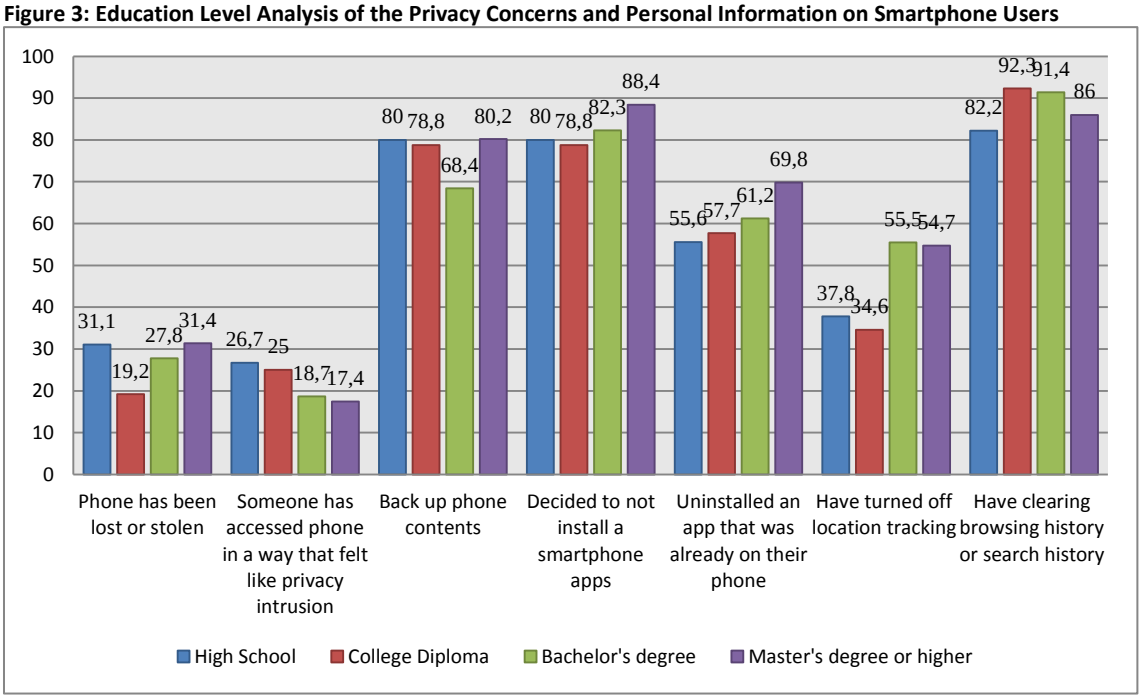
The level of privacy concerns drops with the increase in respondents' educational degree (Table 5). It is observed through data analysis that compared with respondents with an education background of high school, those with a Master's degree or higher are more inclined to think that have turned off location tracking may result in a leakage of personal information ($p < 0.05$).

Table 5: Privacy Concerns and Personal Information Analysis of Respondents with Different Educational Backgrounds

Questions	p-Value	High School	College diploma	Bachelor's degree	MD PhD
1. Phone has been lost or stolen	0.440	12.8%	9.2%	53.2%	24.8%
2.Someone has accessed phone in a way that felt like privacy intrsusion	0.453	15.2%	16.5%	49.4%	19%
3. Back up phone contents	0.085	12.4%	14.2%	49.5%	23.9%
4. Decided to not install a smartphone app	0.433	11.1%	12.6%	52.9%	23.4%
5. Uninstalled an app that was already on their phone	0.327	10.3%	12.3%	52.7%	24.7%
6. Have turned off location tracking	<0.05	8.6%	9.1%	58.6%	23.7%
7. Have clearing browsing history or search history	0.191	10.6%	13.7%	54.6%	21.1%

Chi-square test was used. If p value < 0.05, there was a statistically significant difference among those groups. Respondents with a higher education level are more conscious of privacy protection (Fig. 3). It is observed from the data that more respondents with a Master's degree or higher education background actively take privacy protection measures than respondents from other education backgrounds.

Figure 3: Education Level Analysis of the Privacy Concerns and Personal Information on Smartphone Users



4.4. Income Level Analysis

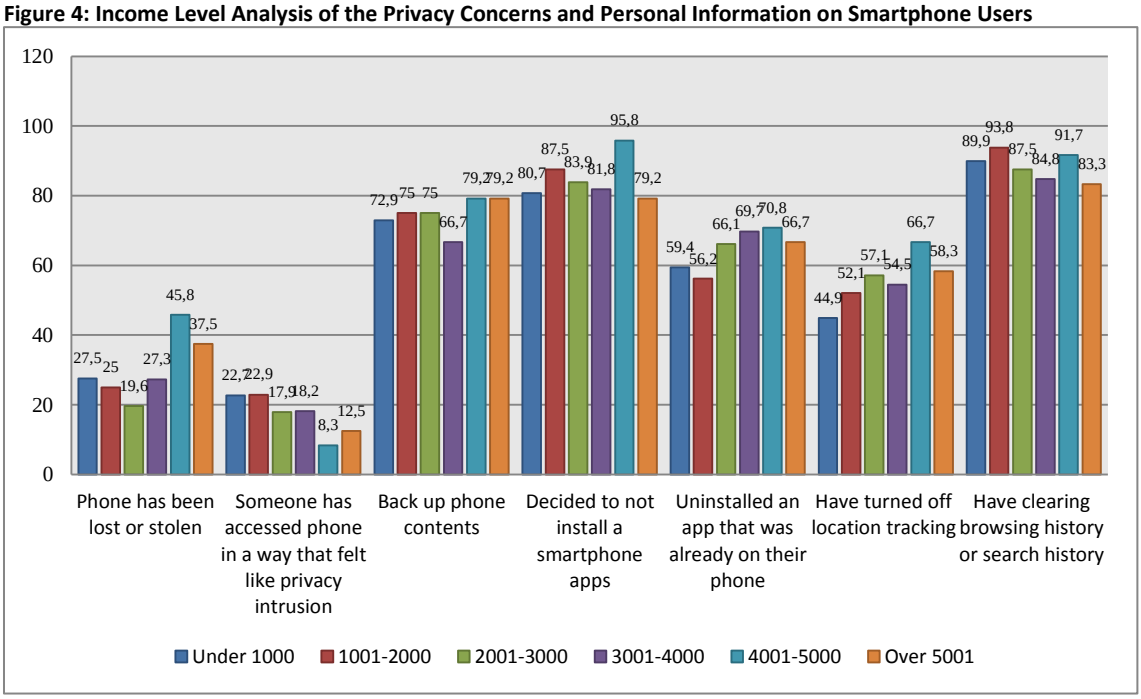
The next relationship of interest is privacy and personal information versus income distribution. Table 6 shows the relationship. It can be seen that for those with the highest degree of concern there isn't any specific trend except for respondents with income 4001-5000 Turkish Lira a group that seems to have a higher percentage of users with concern than the other income groups.

Table 6: Privacy Concerns and Personal Information Analysis of Respondents with Different Income Level

Questions	p-Value	Under 1000	1001-2000	2001-3000	3001-4000	4001-5000	Over 5001
1. Phone has been lost or stolen	0.216	52.3%	11.0%	10.1%	8.3%	10.1%	8.3%
2. Someone has accessed phone in a way that felt like privacy intrusion	0.509	59.5%	13.9%	12.7%	7.6%	2.5%	3.8%
3. Back up phone contents	0.732	52.2%	12.4%	14.5%	7.6%	6.6%	6.6%
4. Decided to not install a smartphone app	0.470	51.4%	12.9%	15.5%	8.3%	7.1%	5.8%
5. Uninstalled an app that was already on their phone	0.624	50.6%	11.1%	15.2%	9.5%	7.0%	6.6%
6. Have turned off location tracking	0.226	47.0%	12.6%	16.2%	9.1%	8.1%	7.1%
7. Have clearing browsing history or search history	0.705	53.1%	12.9%	14.0%	8.0%	6.3%	5.7%

Chi-square test was used. If p-value < 0.05, there was a statistically significant difference among those groups. Looking at the results for Figure (4) below we see the percentage of respondents for each income group. We observe that from (3) statement to (7) statement there is trend while the income level increases. It means that statements which refer to a high degree of privacy concern, as income level increases the proportion of mobile users with the high degree of privacy concerns increase.

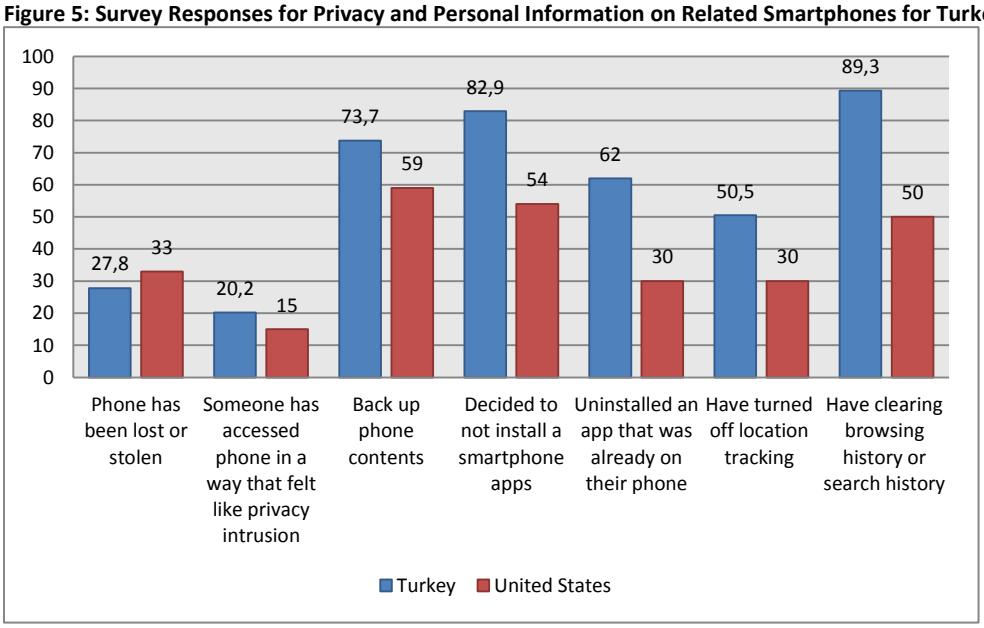
Figure 4: Income Level Analysis of the Privacy Concerns and Personal Information on Smartphone Users



5. CONCLUSION AND PRACTICAL IMPLICATIONS

This paper attempts to study the consumers' concerns with personal information in Big Data. In our study, we investigated the behaviors of consumers about smartphone apps in Erzurum. In our research, we selected to study common individual consumers' demographic differences, such as gender, age, education level and income and how they affect their concerns for information privacy in the context of Big Data. Based on data collected and the statistical analyses performed, we found that nearly one-fourth of smartphone owners have lost their smartphone or had it stolen, one-fifth of smartphone owners says that another person has accessed their phone's contents in a way that made them feel that their privacy had been invaded, seven in ten of smartphone owners back up the photos, contacts, and other files on their phone so they have a copy in case their phone is ever broken or lost, eight in ten of smartphone owners have decided to not install a smartphone app when they discovered how much personal information they would need to share in order to use it, more than half of smartphone owners have uninstalled an app that was already on their smartphone because they learned it was collecting personal information that they didn't wish to share, one-half of smartphone owners have turned off the location-tracking feature on their smartphone because they were concerned that other individuals or companies could access that information, nearly nine in ten of smartphone owners have cleared the browsing history or search history on their phone.

Figure 5: Survey Responses for Privacy and Personal Information on Related Smartphones for Turkey and United States



As in Figure 5, we can see that compared to the U.S. (Boyles et al. 2012), Turkey users have a higher proportion of users who have a high degree of privacy concerns and personal information. Thus, Turkey users appear actually to have more concerns about privacy and security issues than U.S. users. We can say that one of the reasons of privacy differences between these two countries is culture. The internet can change the consumer behaviors. However, some dynamics of societies is critical for how to think, react, and behave. For example, the religion of people, the degree of civil liberties and political rights are very important in every nation. It is predictable that people who live in developed countries behave more confidentially contrast to developing or undeveloped countries. From this point of view, it might be a difference for Turkey and United States. Turkish people is loyal to family. Therefore, they care much more what they do in their social and internet life. Also, families expect some behaviors from theirs. They do no ignore the pressure of family and society rules. In a word, the social and cultural factors determine the behaviors on online.

The findings of this article can provide beneficial information for company owners and managers, members of parliament and government officials, and lastly consumers. The company owners and managers should indicate that what the meaning of their applications for customers and how customers use these apps with safely. Also, if the customers learn their personal information collect by companies without any allow rules, what the managers of company feel about it. Therefore, they have to think how they gain trust of their mobile apps users or others in the internet environment. The first thing that what they should do is determine their privacy statements about each apps. They emphasize more details about using mobile apps in order to level of assurance for customers. The findings also indicate the perceptions of smartphone users about privacy issues. Therefore, consumers should easily control their personal information in apps. In this point, mobile application developers try to design a mechanism that works for a range of specific privacy settings. The marketers try to understand consumer perceptions and attitudes in order privacy perspective. Therefore, they can fix the best mobile apps for their strategy. On the other hand, the members of parliament and government officials must develop a legislation for protecting of people privacy. It is the area of responsibility of deputy. They should do some plans for increasing mobile customers' awareness. Consumers should know their rights about the subject of privacy issues. That's why, state officials should educate consumers about how people protect their privacy contrast to organizations.

The mobile consumers should learn important of privacy. They have to protect their personal information because of many malicious companies. As such these companies do not care personal rights. They might sell mobile users information for their profit. While consumers use some mobile apps, they should be careful about company privacy statement. In the era of big data, the cost of personal information and security should be very important for every customers. Therefore, if they increase their level of awareness about mobile privacy, they will be more comfortable in this area.

Our study contributes to existing literature on the relationship between demographic differences and consumer privacy concerns in Big Data. It has been suggested individual consumers' demographic differences (gender, age, education level, income) are correlated to their concerns for information privacy in the context of Big Data which can affect their behaviors. Future studies can be such as privacy experiences, privacy awareness, personality differences, and culture climate, and test how may affect consumers' privacy concerns (Zhang et al. 2013).

REFERENCES

Aditya, P., Bhattacharjee, B., Druschel, P., Erdélyi, V., & Lentz, M. Brave new world: privacy risks for mobile users. In Proceedings of the ACM MobiCom workshop on Security and privacy in mobile environments, 2014 (pp. 7-12): ACM

Angwin, J., & Valentino-Devries, J. (2011). Apple, google collect user data. Wall Street Journal, 22.

Bardi, M., Zhou, X. W., Li, S., & Lin, F. H. (2014). Big Data security and privacy: A review. China Communications, 11(2), 135-145.

Boyles, J. L., Smith, A., & Madden, M. (2012). Privacy and data management on mobile devices. Pew Internet & American Life Project, 4.

Buck, D.-K. C., Horbel, C., Kessler, T., & Christian, C. (2014). Mobile consumer apps: Big data brother is watching you. Marketing Review St. Gallen, 31(1), 26-35.

Cate, F. H. (2014). Privacy, Big Data, and the Public Good. Science, 346(6211), 818-818, doi:10.1126/science.1261092.

Chen, J., Ping, J. W., Xu, Y. C., & Tan, B. C. (2015). Information Privacy Concern About Peer Disclosure in Online Social Networks. IEEE Transactions on Engineering Management, 62(3), 311-324.

Combe, C. (2015). Privacy, Big Data, and the Public Good: Frameworks for Engagement. Local Government Studies, 41(1), 181-182, doi:10.1080/03003930.2014.981403.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. Organization science, 10(1), 104-115.

eMarketer (2014a). Internet to Hit 3 Billion Users in 2015. http://www.emarketer.com/Article.aspx?R=1011602. Accessed November 9 2015.

eMarketer (2014b). Smartphone Users Worldwide Will Total 1.75 Billion in 2014. eMarketer.

Gaff, B. M., Sussman, H. E., & Geetter, J. (2014). Privacy and Big Data. Computer, 47(6), 7-9.

Gomez-Martin, L. E. (2011). Smartphone usage and the need for consumer privacy laws. Pitt. J. Tech. L. & Pol'y, 12, i.

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

Gurau, C., & Ranchhod, A. (2009). Consumer privacy issues in mobile commerce: a comparative study of British, French and Romanian consumers. Journal of Consumer Marketing, 26(7), 496-507.

Hahn, J. (2014). Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family. Library Journal, 139(10), 124-124.

Hirose, M., Mineo, K., & Tabe, K. THE INFLUENCE OF PRIVACY INFORMATION IN MOBILE APPS. In 2016 Global Marketing Conference at Hong Kong, 2016 (pp. 1337-1341)

Holtmanns, S. (2002). Privacy in a mobile environment. 13th International Workshop on Database and Expert Systems Applications, Proceedings, 493-497.

IDC, I. (2015). Worldwide Quarterly Mobile Phone Tracker.

Karabey, B. (2012). Big Data and Privacy Issues. E-Science and Information Management, 317, 3-3.

Keith, M. J., Babb, J. S., & Lowry, P. B. A Longitudinal Study of Information Privacy on Mobile Devices. In System Sciences (HICSS), 2014 47th Hawaii International Conference on, 2014 (pp. 3149-3158): IEEE

Koseoglu, O., & Koker, N. E. (2015). Consumer Privacy in New Media: A Study of University Students in Turkey. Mediterranean Journal of Social Sciences, 6(2), 588.

Kshetri, N. (2014). Big data's impact on privacy, security and consumer welfare. Telecommunications Policy, 38(11), 1134-1145, doi:10.1016/j.telpol.2014.10.002.

Landau, S. (2015). Control use of data to protect privacy. Science, 347(6221), 504-506.

Leek, S., & Christodoulides, G. (2009). Next-generation mobile marketing: how young consumers react to bluetooth-enabled advertising.

Liu, Y. (2015). Privacy Protection Method in the Era of Cloud Computing and Big Data. International Conference on Engineering Technology and Application (Iceta 2015), 22, doi:ARTN 01041

10.1051/matecconf/20152201041.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information systems research, 15(4), 336-355.

Okazaki, S., Li, H. R., & Hirose, M. (2009). CONSUMER PRIVACY CONCERNS AND PREFERENCE FOR DEGREE OF REGULATORY CONTROL A Study of Mobile Advertising in Japan. Journal of Advertising, 38(4), 63-77, doi:10.2753/Joa0091-3367380405.

Pan, Y., & Zinkhan, G. M. (2006). Exploring the impact of online privacy disclosures on consumer trust. Journal of Retailing, 82(4), 331-338, doi:10.1016/j.jretai.2006.08.006.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. Journal of Public Policy & Marketing, 19(1), 27-41, doi:DOI 10.1509/jppm.19.1.27.16941.

Praher, C. P., & Praher, J. F. (2008). Security and Privacy in an Enterprise Search Infrastructure for Mobile Devices. Idimt-2008: Managing the Unmanageable, 25, 431-444.

Quinn, A. C. (2015). Privacy in the age of big data: Recognizing threats, defending your rights, and protecting your family. Government Information Quarterly, 32(3), 362-362, doi:10.1016/j.giq.2015.04.004.

Shilton, K. (2009). Four billion little brothers?: Privacy, mobile phones, and ubiquitous data collection. Communications of the Acm, 52(11), 48-53.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. MIS quarterly, 35(4), 989-1016.

Spiekermann, S., Acquisti, A., Bohme, R., & Hui, K. L. (2015). The challenges of personal data markets and privacy. Electronic Markets, 25(2), 161-167, doi:10.1007/s12525-015-0191-0.

Taylor, C., & Wagman, L. (2014). Consumer privacy in oligopolistic markets: Winners, losers, and welfare. International Journal of Industrial Organization, 34, 80-84.

Thurm, S., & Kane, Y. (2010). Your apps are watching you: A WSJ investigation finds that iPhone and android apps are breaching the privacy of smartphone users. The Wall Street Journal.

Union, I. T. (2015). The World in 2015: International Telecommunication Union.

Wade, A. (2014). Children's Online Privacy Protection Act: Can Website Regulations Be Applied to Mobile Phone Apps, The. Fed. Cts. L. Rev., 8, 197.

Waldo, J., Lin, H., & Millett, L. I. (2007). Engaging privacy and information technology in a digital age: National Academies Press Washington, DC, USA.

Wang, H., Jiang, X. H., & Kambourakis, G. (2015). Special issue on Security, Privacy and Trust in network-based Big Data. Information Sciences, 318, 48-50, doi:10.1016/j.ins.2015.05.040.

Wang, H., Lee, M. K., & Wang, C. (1998). Consumer privacy concerns about Internet marketing. Communications of the Acm, 41(3), 63-70.

Wetherall, D., Choffnes, D., Greenstein, B., Han, S., Hornyack, P., Jung, J., et al. Privacy revelations for web and mobile apps. In Proc 13th USENIX Conference on Hot Topics in Operating Systems, 2011 (pp. 21)

Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy.

Youn, S. (2009). Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. Journal of Consumer Affairs, 43(3), 389-418.

Yu, Y., Mu, Y., & Ateniese, G. (2015). Recent Advances in Security and Privacy in Big Data J.UCS Special Issue. Journal of Universal Computer Science, 21(3), 365-368.

Zhang, R. D., Chen, J. Q., & Lee, C. J. (2013). Mobile Commerce and Consumer Privacy Concerns. Journal of Computer Information Systems, 53(4), 31-38.