Agricultural Marketing and Commercialization Journal
7(2), 15-42, 2023, ISSN Print: 2676640X, ISSN online: 2676-7570

Permission marketing and Privacy Concerns: A case study of online service customers of companies in the agricultural sector of Rasht city

Zahra Mohammadzadeh Emamverdikhan[1], AliReza Farokhbakht Foumani[2]*, Rahmat Ali Saberi Haghaegh[3]

Received: 17 February 2023/ Revised: 25 March 2023/ Accepted: 29 April 2023/ Published: 31 December 2023

Abstract

Nowadays, due to the number of advertisements and the increased awareness of customers, it has become difficult to communicate with them. They often do not respond to marketing stimulants and even consider it a nuisance. However, this research has shown that it is still possible to reach the potentials of customers with relevant and specific messages. To address these concerns and to meet legal requirements, the concept of pre-authorization consumer provides an interesting option for future engagement. This concept, called permission marketing, refers to direct marketing activities that require consumer consent for a particular company to contact the consumer. These messages are personal and relevant, beneficial and reciprocal. Permission not only has a positive effect on consumer response to interactive marketing activities, but is also a legal requirement for companies using direct marketing media. The present research, in terms of the practical purpose and the descriptive-survey data collection method, is based on correlation and in terms of time was carried out cross-sectional. The research model was evaluated with a questionnaire of 34 questions (based on a Likert scale 5-point). The statistical sample was account for 384 online customers receiving the services from the Rasht's Agriculture Department. At the end, among the 10 hypotheses proposed, two hypotheses were rejected and 8 hypotheses were confirmed. Privacy concerns were explained by 88% and permission by 50% in the model.

Keywords: Agricultural Service Companies, Customers' Intention to Accept Permission Requests, Permission Marketing, Privacy Concerns, Risk.

Introduction

Information privacy is defined as the ability to control information about oneself and determine when and for what purpose others can access such information (Crossler & et al, 2019). Previous studies indicate that the transformation in privacy follows the

[1] Ph.D. candidate, Department of Business Management, Rasht Branch, Islamic Azad University, Rasht, Iran
[2] Department of Management, Bandar Anzali Branch, Islamic Azad University, Bandar Anzali, Iran.
alirezafarrokhbakhtfoumani@gmail.com
[3] Department of Management, Bandar Anzali Branch, Islamic Azad University, Bandar Anzali, Iran

advancement of information technology and with the evolution of markets and technologies, its dimensions can also be changed (Smith et al., 2011). Three contemporary eras of information privacy have been discussed in the literature (Westin, 2003): The first era (1961-1979) is characterized by the emergence of technologies for collecting, processing and monitoring data through the guidance of mainframe computers and communications. The protocols have raised concerns about individuals' privacy rights. The second period (1919-1980) saw no major changes in privacy as advances in computers and telecommunications were incremental. Personal computers were introduced, but their computing power and network access were limited. In the third period (2010-present), with the widespread expansion of Internet and wireless communication technologies, the creation of big data tools and data breach incidents, web tracking and fingerprints, location-based services and the adoption of electronic health records, privacy has become a social and political priority. Became the challenges of balancing the needs to ensure privacy rights and protect freedom of information are complex. However, technological advances in the past decade have significantly changed the concept of privacy and raised unprecedented issues regarding the role of third parties, the extent of user involvement in privacy settings, and the commercialization of user data (for example, the Facebook-Cambridge incident). Technology has also significantly increased the value of data and hence the organization's efforts to gather information. About 90% of the data available on the Internet today after 2016 and almost half of this data is generated by mobile devices and the Internet of Things (Marr, 2018). Empirical analyzes show that these devices are the main target of privacy and security violations because they lack basic security protocols (Pour & et al., 2019). A recent study estimated that "99.98% of Americans are correctly identified using 15 demographic characteristics in each dataset" (Rocher & et al., 2019). Also, the number of social network users has increased from 5% in 2005 to 72% in 2019 (Pew Research Center, 2019). The temporal and spatial boundaries of privacy are fading (Acquisti et al., 2015). Because stored public data can even reveal people's secret affairs (Malm, 2018) and physical privacy is no longer a single concept but a subset and a function of information privacy. It has been argued that the significant technological advances of the last decade have changed the concept and dimensions of privacy, which is partly due to the increased differentiation in the provision of services equipped with mobile phones. In addition, with the integration of the Internet with social and mobile technologies, we may have entered the fourth era of information privacy: most positivist empirical information system studies on privacy concerns approach this phenomenon through the macro model "Antecedents-Privacy Concerns-Outcomes" (APCO) (Dinev & et al., 2015) are reviewed (Smith et al., 2011; Warkentin et al., 2016). However, when people are constantly involved in social and communicate with others through mobile devices, they may be forced to revise previous structures. People participate in

online social networks to create social capital, improve their self-esteem and self-confidence, and satisfy their enjoyment needs (Heravi et al., 2018). However, the content shared in these operating systems can attract the attention of a wide range of people, third-party organizations, and government organizations (Aquasti et al., 2015). Therefore, when deciding whether to disclose information, users should consider possible misuse of private information by: 1) the organization that operates the online social network and its partners (known as institutional privacy concerns) and (2) other users or Individuals in the operating system (social privacy) should consider issues (Raynes-Goldie, 2010). In addition, in the context of mobile phone applications, the disclosure of user information is supplemented with data generated on the device (for example device ID, location, and contact list of the user) (Crossler et al., 2019). Such data is automatically shared with the developer when users accept the permission request (Dogruel et al., 2017). Additionally, most developers share user data with third parties for tracking and advertising purposes. Thus, it enables third-party companies to match data from different applications and services and draw conclusions about individual users (Vallina-Rodriguez et al., 2017). Unlike traditional websites or desktop applications, mobile applications can continuously monitor the activities of their users (Wottrich et al., 2019). Therefore, the dynamics of data sharing and disclosure have made privacy studies more complicated in the era of social mobile (Barth et al., 2017; Crossler et al., 2019; Wottrich et al., 2018). The structure of mobile users' information privacy concerns was first presented by Zhu et al. (2012), which is based on the scale of concern for information privacy and privacy concerns of Internet users. The information privacy concern scale measures "individuals' concern about organizational information privacy practices" with four subscales: collection, errors, inappropriate access, and unauthorized secondary use. The collection of personal information enables companies to use this information about people in permission marketing and make offers more accurately to interested people. Due to errors and inappropriate access, people are concerned that companies should take more measures to reduce errors and control access to personal information. Regarding the possible opportunistic behavior of companies, unauthorized secondary use refers to the sale or sharing of personal information without their permission (Smith et al., 1996).

Importance and necessity of conducting research

There have been many reviews and articles on the role of customer information privacy in e-commerce: social media (Jozani et al., 2020), wearables (Longley 2015; Lydnia et al., 2017), and the Internet of Things (Emami Nayini et al., 2019; Kim et al., 2019; Paul et al., 2020) which indicate that customer privacy and related concerns in establishing marketing communications and customer permission are of great importance. Therefore, it should be noted that the protection of personal data and

privacy of all users is important and the protection of their personal information is the main priority in reducing the risk of further damage to the threat or inappropriate use of biometric data (Gerrya, 2018). Today, you can reach potential customers with relevant and exclusive messages. However, consumers usually perceive such messages as an invasion of their privacy, which creates a challenge for companies (Krafft, 2017). To address these concerns and meet legal requirements, consumer pre-authorization provides an interesting option for future engagement. This concept, called permission marketing, refers to direct marketing activities that require the consent of consumers to contact a particular company. As predicted, these messages are personal and relevant, beneficial and mutual (Goodin, 1999). Permissions not only have a positive effect on consumer response to interactive marketing activities (Tsang et al., 2004) but are also a legal requirement for companies using direct marketing media. In the United States, this issue arose due to the global debate on data sharing and abuse (CJEU, 2015). Likewise, the latest European data protection law prevents the targeted dissemination of unique interactive marketing activities. Aimed at giving consumers more control over their personal information, the revised law expands the definition of personal data and creates a universal requirement for consent for any use of personal data. Experts predict that this law will have a devastating effect on the online advertising industry (O'Reilly, 2015) and destroy the potential for high profits, for example, mobile marketing offers (Fang et al., 2015). Permission marketing appears to be a promising solution to legal issues and privacy concerns and provides a convenient way to reach customers (Kumar et al., 2014).

Consumers are more likely to allow multiple companies out of a large number of sellers but are likely to choose only one. As a result, companies that have a significant number of satisfied customers are at a competitive advantage over their business rivals. These companies can not only use targeted media to interact with existing customers, but they may also be able to use the existing relationship for mutual activities. Without their customers' permission, in many countries companies are not allowed to actively target customers and are therefore reduced to passive order takers. Designing the licensing process with the goal of increasing customer satisfaction is a priority for many companies. Organizations are faced with the question of what factors are influential in this decision-making process. On the one hand, there is a growing potential for personalizing messages in online marketing. On the other hand, a higher degree of personalization may also increase privacy concerns (Tucker, 2014). In this regard, the current debate about the consequences of privacy is increasingly focused on the authorized use of data alongside the growing potential for the illegal misuse of data (Shah, 2015). Despite the growing importance of permission-based interactive communications and disruptive privacy concerns, limited research has been done to examine the drivers and barriers to granting permission from customers. Until now, researchers have focused primarily on responses to personalized marketing, privacy impacts, and opt-in and opt-out

decisions, but not on permission decisions. There are still no studies that test a conceptual model with a large number of determinants based on permission decision theory. This is necessary given the increasing use of big data in marketing to target customers with personalized messages (e.g., Wedel,Kanan, 2016; Verhoef et al., 2010), which may potentially damage customer relationships (Van Doorn, Hoekstra, 2013) to address this gap, the main purpose of this study is to examine a list of factors that motivate or discourage customers to grant permission for interactive marketing activities. Therefore, our main objective is to evaluate the influence of different factors on the customer's decision to grant permission for personal marketing activities by companies. This is important because recent market studies confirm that consumers are concerned about access to their data and want more information about how it will be used, and are looking for benefits in exchange for the release of personal information, which is linked to the granting of permission (Groopman, 2015). In addition, the Institute of Marketing Sciences has named "creating optimal social contracts with customers" as one of their 11-year research priorities from 2014 to 2016. (Marketing Science Institute, 2016). Permission-based marketing has its origins largely in the direct marketing literature of the 1990s. With the advent of online and digital marketing, direct marketing communications have been partially replaced by personalized online marketing on multiple devices such as mobile phones (Rost et al., 2009). Giving decisions where customers have to allow companies to collect and store data is related to privacy (Martin et al., 2017). When granting consent, customers agree that companies may contact them directly with personalized messages through various channels such as direct mail, email, or telephone. Importantly, existing research shows that giving permission improves the effectiveness of personal communication (Kumar et al., 2014). Our study also includes research related to personal communications, the formation of attitudes toward personalization (eg, evaluation of direct mail activities), as well as behavior regarding engagement in personal marketing communications. Beyond this, research has also been conducted in the field of authorization process design by studying specific opt-in or opt-out procedures. Previous research mainly considers decisions related to receiving personal communications as a trade-off between benefits and costs (Krishnamurthy, 2001). The use of profit and cost trade-off has been described in various theories and research streams, such as Homans' (1961) social exchange theory. This theory explains that people only decide to engage in an exchange situation if they expect the outcome to be completely positive. Social exchange theory is used to explain the basics of human interaction and has been repeatedly used in the field of information exchange (Culnan, Armstrong, 1999; Shuman et al., 2014). In the research literature, several advantages and costs have been considered. One of the dominant advantages of these studies is the level of personalization and, as a result, more communication for customers. This

has been confirmed by studies that show that personalized marketing campaigns have a higher response (Ansari & Mela, 2003). It also shows that incentives and types of content and especially entertainment can be important benefits. Cost factors have received less attention in the existing literature. However, existing research suggests that consumers anticipating higher costs for maintaining their consent (for example, by feeling pressured to regularly update personal information) are less likely to consent. Additionally, the anticipated loss of privacy is considered an important cost factor, as customers who allow companies to send them personal communications may be viewed as a nuisance (Van Doorn, Hoekstra, 2013). Considering the importance of privacy in general and for the present study in particular, we present an overview of privacy in the relevant literature. One study has extensively examined consumers' decisions to allow companies to collect and use their personal data (Martin et al., 2017). There has been extensive research on this decision in the marketing and information systems literature (Zu et al., 2011). Another interdisciplinary review is presented that focuses on the so-called privacy account and analyzes the risks and benefits of sharing personal information with others. Similar to the literature on personal communication, studies often use a benefit-cost perspective to make decisions. Unsurprisingly, the main costs here are the costs of loss of privacy. Therefore, most previous studies have reported a negative effect of privacy concerns on consumers' willingness to share personal information (Kim et al., 2008). Providing incomplete or inaccurate information, opting out, negative word-of-mouth, or actively complaining about additional negative consequences of apparent privacy concerns can be less likely to register online (Kim et al., 2008; Lwin et al., 2007). Providing more control to consumers can reduce privacy impacts (Tracker, 2014). Interestingly, factors such as company reputation, consumer trust, and data protection seals can build confidence and reduce the negative impact of privacy concerns (Xie et al., 2006). Therefore, this research also shows that according to some factors, the effect of privacy concerns can be reduced. On the other hand, previous researches show that when communication is perceived as irritating, disturbing, and annoying, consumers react less and if consumers think that these communications cause dissatisfaction or negative feelings, a negative response occurs. Such expectations can even lead to attempts to avoid any contact with the sender (Beak et al., 2012). Tsang, Hu, and Liang (2004) show that perceived harassment, which is defined as one aspect of stimulation, has a negative effect on consumers' attitudes toward mobile phone advertisements. In the context of online advertisements, perceived influence explains the consumer's negative response (Van Doorn, Hoekstra, 2013). From here, we conclude that these findings support the presence of the predicted negative influence on consumer-company relationships. Once consumers decide to register and consent to interactive marketing activities, they must provide personal information to the relevant company. Such information includes at least a contact address, but can also include more details

such as demographics or personal settings (Krishnamurthy, 2001).

Depending on consumers' perception of the value of their personal information, privacy concerns may arise. Often, consumers perceive the disclosure of private data as personal self-sacrifice (Krofft, 2017; Kim et al., 2008). Several researchers have found evidence of the negative impact of privacy concerns in various research fields, for example, mobile marketing programs and consumer loyalty (Zhao et al., 2012), as well as Tsai et al. (2016), found that consumers are even willing to pay a higher price to purchase products from websites that protect their privacy. Their research shows that consumers are aware of the monetary value of their data. In the context of interactive marketing, it was also found that privacy concerns have detrimental effects on the acceptance of information storage as well as on mail-order purchasing behavior (Phelps et al., 2001). Finally, Beak and Morimoto (2012) supported that privacy concerns lead to increased ad skepticism and ad avoidance. Based on these arguments and obvious findings, it can be seen that privacy concerns are an important variable in many decisions related to providing information. Interactions between privacy concerns and perceived benefits Consumers with strong privacy concerns have a generally negative attitude toward all forms of personalized communications (Martin et al., 2017). Customers have a strong fear that their data will be misused and usually do not trust the good intentions of companies. In view of these cases, we have accepted the direct and negative impact of privacy concerns on licensing decisions. Accordingly, we consider and integrate insights from discussions of theoretical approaches, literature on personal communications and privacy concerns, perception of intrusion, perceived benefits, potential costs, and degree of control over data presentation, to develop and substantiate our conceptual framework.

Methods and Methodology

This research is considered to be quantitative in terms of its practical purpose and in terms of its implementation strategy. At first, data, models, and theoretical literature in this field were collected. The appropriate and comprehensive model was selected and tested in the field by distributing a combined 34-question questionnaire (standard and researcher-made) based on a five-point Likert scale among the statistical population of 384 online customers receiving services from the agricultural sector of Rasht. The following model, which was obtained from the qualitative research of Mohammadzadeh & et al., (2022) was evaluated:

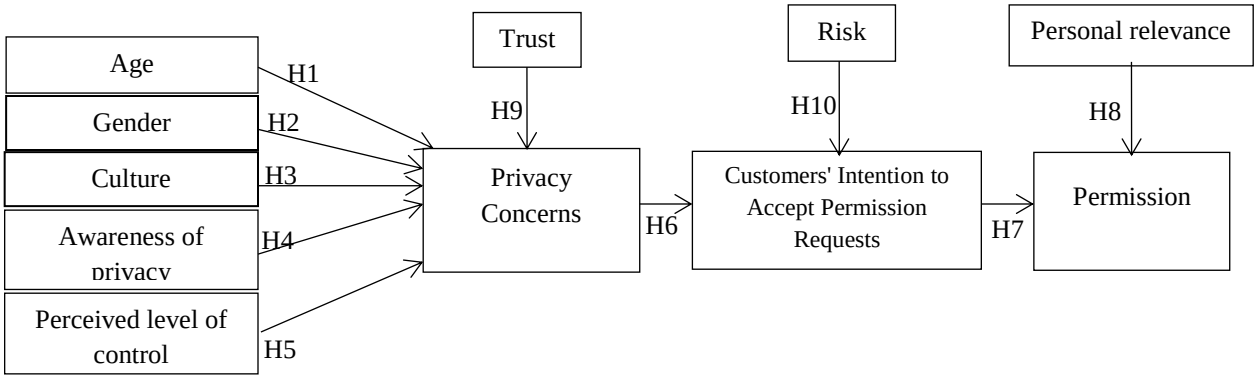

Figure 1. Conceptual model was obtained from (Mohammadzadeh & et al., 2022)

Results

Data analysis was done in two parts, descriptive and inferential statistics. In descriptive statistics, using descriptive statistics techniques such as frequency indices and percentages, tables and graphs, we analyzed the demographics of the statistical sample, and in the inferential statistics section, we investigated the research hypotheses using statistical tests. Inferential analysis was performed using tests such as correlation coefficient, confirmatory factor analysis, model fit test, measurement model and path analysis with the help of SmartPLS software.

Research demographic

The total number of respondents was 384, of which 3.9% were between 10 and 15 years old, 4.4% between 16 and 21 years old, 8.1% between 22 and 27 years old, 16.1% between 28 and 33 years old, 19.5% between 40 and 45 years old, 15.9 % between 34 and 39 years, 16.7% between 46 and 51 years, 8.6% between 52 and 57 years, 1% between 58 and 63 years, 3.1% between 64 and 69 years, 1.6% between 70 and 75 years, 1% higher They have been since 75 years. Of these respondents, 37.8% were men and 62.2% were women. Among all the respondents, 50% were married, 34.9% were single, and 15.1% chose other items. 5.5% under diploma, 5.5% diploma, 15.1% of respondents were people with postgraduate education, 34.4% bachelor, 28.4% postgraduate, 11.2% PhD.

Agricultural Marketing and Commercialization Journal
7(2), 15-42, 2023, ISSN Print: 2676640X, ISSN online: 2676-7570

The score of research variable structures

Table 1. The descriptive structures of research variables

Research variables	minimum	maximum	average	standard deviations
privacy Concerns	1	5	1.81	.081
Personal relevance	1	5	2.13	0.81
Perceived level of control	1	5	3.11	1.65
Customers' Intention to Accept Permission Requests	1	4.33	2.26	0.46
Awareness of privacy	1	5	1.69	0.83
risks	1	4.5	1.23	0.63
Trust	1.2	5	4.32	0.96
Culture	1	5	2.3	0.73
permission	1	5	2.72	0.87

In the above table, the range of changes in the scores of the variables, their mean and standard deviation are mentioned. As can be seen, the highest average value for the trust variable with an average value of 4.32, and the lowest average value for the privacy risks variable with an average value of 1.23. According to the significance level of the Kolmogorov-Smirnov test, which was less than 0.05 for the research variables, it was concluded: the frequency distribution of the research variables was not normal, and therefore, Smart PLS structural equation software was used to check the research hypotheses.

Inferential findings

Inferential findings the results of the hypothesis test showed that:

Table 2. The final results of hypothesis testing

Research hypotheses	intensity of impact	T value	level of significance	result
Hypothesis 1- Gender is related to concern about privacy.	-0.003	0.16	0.86	rejected
Hypothesis 2- Age is related to privacy concerns.	0.01	0.18	0.87	rejected
Hypothesis 3- Culture is related to privacy concerns.	0.11	4.28	0.001	confirmed
Hypothesis 4- Privacy awareness is related to privacy concerns.	-0.24	6.45	0.001	confirmed
Hypothesis 5- Perceived privacy control is effective on privacy concerns.	-0.324	11.384	0.001	confirmed
Hypothesis 6- Privacy concerns affect the intention to accept permissions.	-0.184	3.606	0.001	confirmed
Hypothesis 7- The probability of the intention to grant permission to accept permission requests by consumers has an effect on their permission.	0.396	5.966	0.001	confirmed
Hypothesis 8- Perceived personal connection as the perceived benefits of consumers is related to the permission of marketing activity.	0.282	6.208	0.001	confirmed
Hypothesis 9- Customer trust is effective in his concern about privacy.	-0.116	3.029	0.008	confirmed
Hypothesis 10- The amount of perceived risk is effective on Customers' Intention to Accept Permission Requests permission requests.	-0.543	8.311	0.001	confirmed

Source: research findings

To test the measurement model, in this research, Cronbach's alpha and composite reliability were used to check the reliability of the measurement model, and convergent validity and divergent validity tests were used to check the validity of the measurement model. The results of which are as follows:

Table 3. Cronbach's alpha of research variables

Research variables	Cronbach's alpha	situation
privacy Concerns	0.968	acceptable
Personal relevance	0.953	acceptable
Perceived level of control	0.97	acceptable
Customers' Intention to Accept Permission Requests	0.769	acceptable
Awareness of privacy	0.859	acceptable
risks	0.918	acceptable
Trust	0.946	acceptable
Culture	0.694	acceptable
permission	0.847	acceptable

Table 4. Composite reliability of research variables

Research variables	Composite reliability (p Dillon-Goldstein)	situation
privacy Concerns	0.974	acceptable
Personal relevance	0.969	acceptable
Perceived level of control	0.98	acceptable
Customers' Intention to Accept Permission Requests	0.715	acceptable
Awareness of privacy	0.914	acceptable
risks	0.942	acceptable
Trust	0.961	acceptable
Culture	0.835	acceptable
permission	0.929	acceptable

Table 5. Convergent validity of research variables

Research variables	Convergent validity AVE (average variance)	situation
privacy Concerns	0.862	acceptable
Personal relevance	0.913	acceptable
Perceived level of control	0.843	acceptable
Customers' Intention to Accept Permission Requests	0.587	acceptable
Awareness of privacy	0.781	acceptable
risks	0.803	acceptable
Trust	0.834	acceptable
Culture	0.637	acceptable
permission	0.867	acceptable

Table 6. Coefficient of determination and average index of sharing of research variables

Research variables	R Square	Communality	situation
privacy Concerns	-	0.862	acceptable
Personal relevance	0.498	0.913	acceptable
Perceived level of control	-	0.843	acceptable
Customers' Intention to Accept Permission Requests	-	0.587	acceptable
Awareness of privacy	-	0.781	acceptable
risks	-	0.803	acceptable
Trust	-	0.834	acceptable
Culture	0.417	0.637	acceptable
permission	0.880	0.867	acceptable

Divergent (diagnostic) validity and diagnostic validity were conducted by Fornell and Larcker and the results confirm the validity of the model.

Table 7. Q2 criterion of research variables

Research variables	Q2 criterion	situation
privacy Concerns	0.799	acceptable
Personal relevance	0.769	acceptable
Perceived level of control	0.82	acceptable
Customers' Intention to Accept Permission Requests	0.47	acceptable
Awareness of privacy	0. 545	acceptable
risks	0.655	acceptable
Trust	0.757	acceptable
Culture	0.31	acceptable
permission	0.503	acceptable

And finally, the general fit of the model was evaluated by the general "GOF" criterion (Tennenhas et al. (2004)). This criterion is related to the general part of structural equation models and many researchers have used it in their research (Hair et al., 2013, p. 185). The amount of GOF in the current research model is as follows:

$$GOF = \sqrt{\overline{Communality} * \bar{R}^2} = \sqrt{0.825 * 0.452} = 0.61$$

Wetzels and his colleagues (2009) introduced values of 0.01, 0.25, and 0.36 of this index for weak, medium, and strong fit, respectively (Davari and Rezazadeh, 2012: p. 153). Considering that the GOF value is equal to 0.61; therefore, it can be said that the overall fit level of the model is excellent and acceptable.

Discussion

According to the discussions that have been raised so far and considering the results of the calculations regarding the questions of the research questionnaire, the discussion about the hypotheses and the results is as follows:

Hypothesis 1: Gender is related to privacy concerns.

Are men less concerned about online privacy than women? Even though in some studies men and women were equally concerned about online privacy in many categories: (Taddicken, 2014; Bergstrom, 2015) but most studies show It shows that women are more concerned about their online privacy than men (Anić et al., 2016; Gionosar et al., 2017). Individuals' knowledge, online experiences, and personality traits explain gender differences in privacy concerns (Li, 2011). In this way, men have a more favorable attitude toward online shopping and information sharing (Khare et al., 2011). Men take more risks and show more interest in technology. They tend to use the Internet more than women. On the other hand, women are more

concerned about online threats and abuse and want more control over their private information (Graeff et al., 2002). According to the PLS analysis, there is no direct relationship between gender and concern about privacy. The first hypothesis was not confirmed, which indicates that a person's gender does not have an effect on his tendency to worry about privacy and therefore on giving permission.

Hypothesis 2: Age is related to concern about privacy.

One thing that may come to mind is that: younger people are less concerned about privacy than older people. Some studies show that there is a positive relationship between age and concern about privacy (Gionosar & et al., 2017; Zukowski & et al., 2007). While others did not find the differences insignificant (Bergstrom, 2015) or significant differences between age groups (Heerman et al., 2013; Kansal, 2014). Young users show more practical use regarding privacy (Sheehan, 2002). Also, young people are more aware of the costs, benefits, and methods of data collection (Zukowski & et al., 2007), have a more positive attitude toward data management, and are more confident in preventing potential data misuse (Miltgen & et al., 2014). Previous studies also show that older users are more sensitive and concerned about privacy threats (Graeff & et al., 2002) and are more likely to control their private information. On the other hand, some studies show that young consumers are more excited and act faster towards adopting new technologies, e-commerce, and using the Internet (Zhang & et al., 2008). This hypothesis was also not confirmed with a correlation coefficient of -0.01 due to lack of significance, which shows that people's age does not play a role in worrying about privacy and permission in our statistical population. In the present project, this hypothesis has been rejected contrary to the background, perhaps due to the special conditions of our country in terms of limited access, or the inability to choose options, especially in the use of applications or sites, and the installation force to accept the conditions for use and user, age difference in performance. Do not create users and their concerns. On the other hand, researchers have investigated the effect of demographic variables such as age, gender, and education level on customers' perception of privacy and have found a significant relationship between these variables and the intention to grant permission. It should be noted that in the research literature, researchers such as (Acquisti et al, 2006, Cecere et al., 2015) have indirectly investigated the role of demographic factors (outside of the main model) and the effect These factors have been confirmed. But some studies have directly examined the role of demographic variables on the relationships between the variables introduced in the conceptual model of research (Kansal, 2014; Taddicken, 2014; Bergstrom, 2015) who found that men and women were equally concerned about online privacy in many categories. (Li, 2011; Anic et al., 2016; Gionsar & et al, 2017) found that women are more concerned about their online privacy than men. Also, Li (2011) explains people's perceived knowledge, online experiences, and personality characteristics of gender

differences in privacy concerns. In this way, men have a more favorable attitude toward online shopping and information sharing (Graeff & et al, 2002; Khare & et al., 2011). Men take more risks and show more interest in technology. They tend to use the Internet more than women (Zhang et al., 2013). On the other hand, women are more concerned about online threats and abuse and want more control over their private information (Graeff & et al, 2002).

Examining the third hypothesis: culture is related to concern about privacy.

That the boundaries and content of what is considered personal privacy or privacy (that is, a person or a group can separate themselves or information related to themselves and as a result can reveal themselves or their information to others by their own choice) are different among different cultures and people. But their main theme is common, and the concept of privacy has influenced the concept of security (from abuse to information security) and immunity from the invasion of privacy by governments, companies, or individuals has been made as privacy protection laws in many countries, even in some cases. It is stated in their constitution. Although sometimes people voluntarily disclose their private information (for example, to gain benefits, for advertising, when participating in contests and sweepstakes, etc.) and each person, company, culture, or country has different definitions of privacy (physical privacy, informational privacy). have, but concerns about privacy and the need to protect it when collecting and storing digital or non-digitally data and information that specifically identifies a person are more apparent, and this shows that the root and basis of the privacy problem are related to inappropriate and uncontrolled disclosure. It is personal data and those information privacy problems are actually related to different sources of data and information. Therefore, consumers' privacy concerns may be different in different national cultures (Baazeem et al, 2020). Our current research can explore the effects of privacy specifically by addressing the border conditions of cultural values in Iran. It is hypothesized that privacy concerns are much more intense in collectivist societies (eg, China) than in individualistic societies (eg, Germany or the United States (Guo et al., 2020; Hallikainen et al., 2018). It needs to be investigated. How cultural values affect the perception of privacy. In a research, it was determined that a person's motivational access to buy or use a digital device or service based on information and communication technology is formed by various social, cultural, and psychological factors. When, in 2014, it was discovered that users were exposed to various cultural harms in the field of privacy violations while using virtual social networks of mobile phones, which had a great impact on the family life and cultural identity of the users. Being aware of these harms, while reducing social problems, provides the possibility of optimal use of new technologies. And it makes the path of micro and macro cultural planning and policymaking of the country smoother for those in charge. Many previous pieces of research show that cultural differences, social norms, and privacy policies can affect the privacy of consumers (Miltgen, Pierrat-Gaillard, 2014; Mostler, Poudar, 2017;

Wang, 2019). According to the results of PLS analysis, it was shown that with more than 99% certainty, culture is directly related to concern about privacy. The direct, linear, and significant effect of culture on concern about privacy is 0.11. In other words, if the effect of culture improves by one unit, the concern about privacy in our statistical population will increase by 11%.

Examining the fourth hypothesis: Privacy awareness is related to privacy concerns.

Privacy awareness, as a personal characteristic, refers to the evaluation of the importance of privacy, threats to privacy, and policies that regulate privacy, thus positively and/or negatively affecting concern about online privacy. In other words, if users feel safe and protected, they express a lower degree of concern about privacy. In the context of social networks, user awareness has a positive effect on information disclosure (Benson et al., 2015). However, if users have more information about the privacy policy, but notice a leak in the system, they may be more concerned about privacy. Highly privacy-aware individuals are more concerned about privacy and tend to comply with privacy-related issues (Diniv, Hart, 2006). In terms of concerns about users' privacy and information security awareness, Lowery et al. (2011) used social exchange theory and combined it with the attitudinal aspect of the theory of reasoned action and explicitly argued in favor of true self-disclosure. The research of McCormac et al., 2017 indicates the existence of a positive relationship between awareness and information security. Awareness of information security affects behavior and is often measured based on how people understand and think about information security (Tsohou et al., 2015, Bartsch and Dinelin, 2016). To address these perceptions, researchers have taken different approaches to understanding how awareness, knowledge, and perception of information security affect each other. Sundar et al. (2013) found that when participants became aware of how their personal information was being used illegally, their intention to Disclosure of personal information was lower than participants who were only aware of their benefits. Likewise, in the disclosure of personal information, it is the participants' inability to make informed decisions about privacy that increases their vulnerability to privacy violations. Hirschprung et al. (2016) found that when people do not have the necessary knowledge, they base their decisions on speculation. However, the more awareness and knowledge an individual has, the more rational these decisions and related behavior become. This was confirmed by Van Schaik et al. (2018). They found that Facebook users who are more aware of their privacy are generally more satisfied with their privacy settings (i.e. the visibility of their personal information). The latter findings are in line with those of Miltgun and Pirat-Gaillard (2014), who conducted a similar privacy-based study in several European countries. This hypothesis was confirmed with a path coefficient of -0.24, which shows that there is a significant, linear but inverse relationship between awareness of privacy and concern about people's privacy. That is, if the awareness of privacy improves by one

unit, the concern about privacy in the statistical population of the research will decrease by 24%.

Examining the fifth hypothesis: Perceived privacy control is related to privacy concerns.

"Privacy anxiety" refers to "feelings of anxiety about personal privacy." Consumers are known to have high privacy concerns and to express apprehension about companies collecting and using their personal data. While privacy concern is considered critical in understanding consumer behavior, Akhtar (2014) points out that few studies examine the antecedents of privacy concern. In Akhtar's (2014) study on consumers' privacy concerns in online shopping, banking, and online investment transactions, Internet self-efficacy played an important role in influencing privacy concerns. The main core of this Internet self-efficacy was consumers' perceived ability/competence and self-confidence to successfully perform an online task (Akhtar, 2014). In the field of mobile behavioral advertising, it is related to the ability of people to manage tools and privacy settings on their mobile phones in order to increase their personal privacy. A variety of client-side privacy tools and settings are available on mobile phones to help people control their privacy, including the ability to block ads. However, as pointed out by (Jung et al., 2018), privacy assurance tools are sometimes too complex for users to understand and/or manage effectively. Consumers may also lack confidence in the effectiveness of client tools to help them effectively manage their privacy. According to social contract theory, the perception of the inability to protect privacy can lead to anxiety. In a study conducted among Facebook users, Zlatolas et al. (2015) found that privacy controls had a negative effect on privacy concerns. In a study that focused on users of four different types of websites, e-commerce sites, social networking sites, financial sites, and healthcare sites. Excessive app permission requests that “go beyond the app's essential functionality” (Harris et al., 2016: 445) are less likely to be accepted by mobile users due to privacy concerns about personal information (Chin et al., 2018). It has been reported that more than 100,000 apps on the Google Play Store collect data on mobile users that are inconsistent with their stated functions, such as unnecessary location tracking or excessive access to contact lists (Robertson, 2012). We hypothesize that increasing concerns for app permission requests will lead to an increase in users' overall privacy concerns. According to the results, it was found that perceived privacy control has a direct but inverse relationship with privacy concerns.

Examining the sixth hypothesis: Privacy concerns affect the intention to accept app permission.

App users may refuse to accept app permission requests not only because they want to respond to an intrusive request, but also because they experience privacy concerns, here "individual concerns" as the potential loss of privacy. As a result, the disclosure of information to a specific external agent is defined. Research on the antecedents and consequences of privacy concerns has led to mixed results. Several studies have shown that privacy concerns lead to reduced behaviors, such as keeping or falsifying personal information, and

using privacy-enhancing methods (eg encryption or requesting removal from mailing lists) (lwin et al., 2007). Several studies in the field of information privacy have shown this relationship (Crossler et al., 2019; Wang et al., 2019). Extensive findings from marketing, information systems, and business ethics literature have reported the negative impact of privacy concerns on online users' decisions and behaviors (Mostler, Podar, 2017; Hong, Tang, 2013). The results show that privacy concerns have a direct but inverse effect on the intention to accept app permission.

Examining the seventh hypothesis: the probability of granting permission to accept permission requests by users is related to their permission.

Past research shows that attitudes positively affect behavioral intentions, which in turn have a positive effect on service use (Acquisti et al., 2015). Some studies (Yang et al., 2007; Khare, Rakesh, 2011) show that attitudes affect online search behavior and online purchase intention. On the other hand, consumers with a positive attitude perceive the benefits of online shopping positively and as a result, they become prone to online shopping (Yang et al., 2007). Considering these concepts, lower levels of privacy concerns may lead to respondents' positive attitudes toward online shopping. Therefore, the intention of granting permission to accept users' permission requests is directly effective in allowing them.

Examining the 8th hypothesis: Perceived personal connection as the perceived benefits of users is related to the permission of marketing activities.

The need for relevant information can be the main factor that drives users to interact with a company. With regard to interactive marketing communications, such information represents significant value and, therefore, influences users' willingness to give permission. In order to receive specific and user-related information, users are often willing to exchange data with companies. Beyond that, Baek and Morimoto (2012) showed that perceived personalization is negatively related to advertising skepticism as well as advertising avoidance, and the degree of personalization reduces skepticism towards communication media. Regarding location-based marketing, Zhao et al. (2012) show that personalization, which is defined as an external benefit, has a positive effect on users' intention to disclose information. Smith et al. (2002) emphasize the influence of the importance of both relevance and personalization on users' willingness to allow email marketing. In general, personalization has been shown to lead to more relevant offers in direct marketing, thus increasing response rates (Field et al., 2013). According to the Table2. It was found that there is a direct relationship between the personal relationships perceived as the perceived benefits of users with the permission of marketing activities.

Examining the ninth hypothesis: Customer trust is effective on his concern about privacy.

"Trust, like the soul, never goes away and never comes back." By Publilius (2018), users' trust in institutions may be based on the type of product or service of the organizations. For example, in the case of

the famous organization Facebook, which provides social media and communication services and social networks with more than 1.7 billion users (Shiau et al., 2018), trust may be the perception of users about the storage, use, and protection of their shared information. Change the Facebook network platform. Recent announcements of data and privacy breaches by large organizations such as Equifax and social media giant Facebook may raise concerns about user privacy and undermine consumer trust in these organizations. A decrease in user trust in organizations leads to a decrease in the use of operating systems (Antoci et al., 2019). In 2014, Cambridge Analytica, a commercial company based in London, England, which creates audience behavior modification services, began to inappropriately harvest information and comments from Facebook users without permission (Confessore, 2018), which raised concerns about user privacy, and Facebook was destroyed. Despite Facebook's apology, a survey in major markets including the United States and Germany found that users maintained low trust in social media, especially Facebook, regarding their privacy (Khan, Ingram, 2018). The survey also indicated that some users reconsidered their membership or type of interaction with social media platforms. Given the frequent data and privacy violations associated with digital data, it is noteworthy that the nature and effects on the performance of social media brands or organizations are more complex and destructive compared to traditional communication media (Young et al., 2016) (this complexity also It is exacerbated by the inherent risks and unique characteristics of personally identifiable information shared on social media platforms or networks (Tow et al., 2010). Protecting users' privacy is cognitively and psychologically costly. (Jiang et al., 2013). This issue is aggravated in case of violation of users' trust. As it is evident, trust is delicate and previous researches indicate that repairing broken trust in business is very difficult a difficult task, time-consuming, and requires a long process (Lount et al., 2008). It has been shown that trust has a significant relationship with technology acceptance in general and mobile phone applications in particular (D. Dezando, 2023). A study by Cummings et al. (2021) discovered that the more information users are told about how their data will be used, the more willing they will be to provide it. The results of the research showed that the customer's trust has a direct but inverse relationship with his concern about privacy.

Examining the 10th hypothesis: the level of perceived risk is effective on Customers' Intention to Accept Permission Requests permission requests.

The potential loss of privacy has been widely studied as a deterrent to user disclosure (Shankar et al., 2010). User privacy concerns broadly refer to who has access to their personal information and what is done with it. When the user feels that he does not have full control over the storage of personal information (demographics, lifestyle, financial data, shopping habits, location, etc.), he may perceive vulnerability. Privacy issues have been shown to influence attitudes and intentions to use marketing. It has been argued that this may also be true of permission marketing. Consumers' attitudes

towards permission marketing not only include perceptions of the technology itself (such as usefulness and ease of use) but also include beliefs about the trustworthiness of the company providing permission marketing. Risks and nuisances represent the disadvantages (or victimization) associated with permission marketing and may influence consumer attitudes contrary to the effect of perceived usefulness. Perceived risk has a negative relationship with repurchase intention (Sullivan, Kim, 2018). That is, highly risk-averse consumers may have negative opinions about companies' permissive marketing practices despite their usefulness. Furthermore, the improved usefulness of permission marketing programs may not be possible without increased risks. According to the results, the amount of perceived risk is directly and inversely effective on Customers' Intention to Accept Permission Requests license requests.

In the end, it should be mentioned that 88% of the privacy concern variable is mainly explained by independent variables. Also, almost 50% of the dependent variable of permission is explained by other variables. This article indicates that a set of other factors are definitely involved in the explanation of this dependent variable, which we did not find in this research, so it is suggested to do more research in this field in future research. The customer's intention to accept communication requests is 42%, which explains almost half of this variable.

As our results confirm, service providers whose customers have a high level of customer privacy concerns, the likelihood of perceived fraudulent purchase, the extent of information use and disclosure, customer trust, positive and negative evaluations, and behaviors, as well as increased risk perception and They will show more protective behaviors. In order to reduce these hostile effects, active companies should design and provide appropriate strategies and planning in order to reduce concerns related to customer privacy. One method can be developing new goodwill strategies or adding to existing goodwill-related strategies - such as charitable activities or corporate social responsibility - and improving the image and credibility of sellers and companies through advertising in mass media and social media (Okazaki et al., 2020). Another approach is to develop innovative products and services that either protect customer information or use less of such information than is legally required. For example, Apple Inc (2019). and Pryosi. Com offers "credit cards" that limit the sharing or use of customer transaction data and provide services that require the least amount of personal and transaction-specific customer data. While the many concerns of customers about their privacy create many threats for service providers, increasing the awareness of these concerns among managers can reduce their risk and at the same time by protecting the privacy of customers from existing threats, new opportunities for creating yourself This can be achieved by strengthening the communication department with the company's customers and continuously monitoring their privacy concerns. According to Steve Jobs: Ask the customers themselves, they know better themselves. The findings also show that the specific

nature of different sales channels alters the impact of customer privacy concerns on outcomes. For example, web channels show positive effects on positive evaluation and used behaviors, while mobile phone channels reduce trust and protective behaviors. On the other hand, transactions in social channels show increased risk, disclosure, and abuse of behaviors. Therefore, companies that use social channels must be aware of these effects and must also move beyond mere awareness to strategically acquire, store, and destroy customer data to protect their image and reputation (Planger et al, 2015) and create and frequently update safe conditions and usage. With the rise of major incidents of personal information theft—such as the recent Facebook incident, where 78 million accounts were exposed (Rosen, 2018)—concerns about customer privacy, in general, will increase in the future. Companies that collect customers' personal data must prepare for unexpected big data security breaches by establishing specific safeguards to protect and ensure the privacy of customer information. For example, by employing dedicated and expert software engineers who constantly take care of the storage space and deal with any kind of information leakage, or by using efficient and modern technologies to protect physical data and cloud space. On the other hand, it is vital to design and carry out communication campaigns that convey the transparent policies applied. These campaigns, which are created and implemented with appropriate strategies the actions, performance, and transparency of the service provider's company are communicated to the customers, strengthen the trust and reputation of the company and improve relations with customers.

From a practical point of view, it has been warned that unnecessary and excessive requests of the program have a strong impact on the privacy concerns of users and can prevent the acceptance of marketing and communication programs by customers or even cause discomfort to them and the company and communication programs consider it a nuisance. As a result, service providers must ensure that they only use the personal information stored in mobile devices and physical centers when necessary and in a way justified by value-added services such as location tracking for navigation purposes, providing essential health services, etc., information is accessed. The request for permission is reduced to the minimum necessary amount and an attempt is made to justify the requests logically, and also by presenting these requests at appropriate times that are appropriate to the conditions and requirements of the customers, they pay attention to the great effects of privacy concerns and consider them seriously do On the other hand, improvements in the design and submission of permit applications for marketing programs are needed. For example, removing ambiguity and uncertainty about the safety and necessity of communication software licenses can be done with categories and ratings created by companies (which are everywhere on the internet and in the business software market) take place As can be seen from our results, the concerns related to the disclosure of information, the opinions of the customer's peers, the prevailing culture in the society, the lack of knowledge of the

reason for communication and also how to use the personal data of people according to the personality dimensions of the customers have a very important effect on privacy concerns has customers.

Finally, the results of this study reach here that due to the rapid growth of marketing communication programs and the resulting excessive requests for acceptance permission, reducing the concern about the privacy of customers receiving services is more important than ever, which should be done with increasing trust and awareness. As many customers as possible from the process of collecting information and how to keep it, through suitable professional staff who are in direct contact with customers receiving services and can establish trust and ensure the accuracy and security of data storage by direct communication. The positive perceptions of customers in their controls on the amount and manner of use, persons, and infrastructures with access to data. For example, by creating users the customers themselves have more power and ability in the time, amount, and type of providing data, as well as in disconnecting and not providing personal data whenever they feel it necessary to provide the information they want and otherwise they are free to disconnect and delete data, and more importantly, the need to provide more personalized services, which reduces the concerns of the customers receiving the services, and therefore a greater amount of receiving permission and marketing communications with The more customer satisfaction is provided, the more important it becomes. Providing services exactly according to customer needs is one of the main goals of every company, and receiving services according to what is intended is the dream of every customer. Therefore, in this regard, he may deviate from some of his frameworks and obstacles, reduce the level of his worries, and want to communicate more. In this regard, special attention should be paid to cultural, religious, and social issues and needs for communication and privacy. Sometimes customers don't express their opinions and views because of these conditions and sometimes they don't express their desired factors due to fear of some issues and taboos, they perceive more risk, and their worries increase, which sometimes causes complete disconnection of the communication bridge with the companies.

As with all empirical studies, we acknowledge the specific limitations of our study, and in addition to our findings, these can be used to stimulate further research on permission marketing and customer privacy concerns. This survey was conducted with Iranian participants with Iranian culture and prejudices and perspectives. According to Hofstede's cultural dimensions index, Iran is a medium culture (Hofstede et al, 2010). Therefore, customers from other countries with users from purely collectivist or purely individualistic cultures may have different privacy concerns and acceptance of permission requests due to individual and collective interests. Dear future researchers in all parts of the world, it is recommended to: consider the research in other countries and consider the model for testing in other countries with different nationalities and cultures. The time limit is also one of the limitations of the research. The start of the

research, which was accompanied by the covid-19 disease and created many limitations in terms of communication, implementation, and distribution of questionnaires, obtaining permits, etc., caused a time delay, more than the strategy and plan.

The Acknowledgments

"This manuscript is prepared based on PhD thesis of first author at Rasht Branch, Islamic Azad University, and Rasht, Iran."

Funding: The present research was conducted without any financial support from any specific organization.

Authors' Contribution: The role of each of the authors: in the present study, the first author, Mrs. Zahra Mohammadzadeh Emamvardikhan, in writing and conceptualizing the article, collecting and analyzing data, collecting the background, and the second author, Dr. AliReza Farokhbakht Foumani, as a supervisor in coordination With professors and experts, kindergarten managers and the third author, Mr. Dr. Rahmat Ali Saberi Haghaegh, played a role in editing the article as a consultant professor.

Conflict of Interest: There is no conflict of interest for the authors in this study.

References

- Acquisti, A., Brandimarte, L., Loewenstein, G., 2015. Privacy and human behavior in the age of Information. Science 347, 509–514.
- Anić, I. D., Škare, V., Kursan Milaković, I., 2016. Determinants and behavioral consequences of online privacy concerns among young consumers in Croatia. Ekonomski Pregled, 67(5), 377-398. https://onlinelibrary.wiley.com/doi/full/10.1111/j.1745-6606.2009.01146.x.
- Ansari, Asim and Carl F. Mela (2003), "E-customization," Journal of Marketing Research, 40, 2, 131–45.
- Antoci, A., Bonelli, L., Paglieri, F., Reggiani, T., & Sabatini, F. (2019). Civility and trust in social media. Journal of Economic Behavior & Organization, 160, 83–99.
- Apple Inc (2019). Improving Siri's Privacy Protections. [WWW Document]. URL. https://www.apple.com/newsroom/2019/08/improving-siris-privacy-protections/ (accessed 9.1.19).
- Baazeem, R., Qaffas, A. (2020). The relationship between user religiosity and preserved privacy in the context of social media and cybersecurity. In: Emerging Cyber Threats and Cognitive Vulnerabilities. Elsevier, pp. 93–116.
- Baek, Tae H. and Mariko Morimoto (2012), "Stay Away from Me: Examining the Determinants of Consumer Avoidance of Personalized Advertising," Journal of Advertising, 41, 1, 59–76.
- Bartsch, M., Dienlin, T., 2016. Control your Facebook: an analysis of online privacy literacy [Internet] Comput. Hum. Behav. 56, 147–154.
- Barth, S., De Jong, M.D., 2017. The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. Telematics and informatics 34, 1038–1058.
- Bergstrom, A., 2015. Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. Computers in Human Behaviour, 53, 419-426.
- Cecere, G. Le Guel, F. Soulié, N. (2015). Perceived Internet privacy concerns on social networks in Europe, Technological Forecasting & Social Change 96 (2015) 277–287. http://dx.doi.org/10.1016/j.techfore.2015.01.021.

_ Chin, A. G., Harris, M. A., & Brookshire, R. (2018). A bidirectional perspective of trust and risk in determining factors that influence mobile app installation. International Journal of Information Management, 39, 49–59. https://doi.org/10.1016/j.ijinfomgt.2017.11.010.

_ Confessore, N. (2018). Cambridge analytica and facebook: The scandal and the fallout so far. Retrieved fromThe New York Timeshttps://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

_ Crossler Robert E., Bélanger France and Ormond Dustin. (2019). The quest for complete security:An empirical analysis of users' multi-layered protection from security threats. Information Systems Frontiers, 21(2), 343-357. DOI: 10.1007/s10796-017-9755-1.

_ Culnan, M, J., Pamela K. Armstrong. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. Organization Science, 10(1), 104–115.

_ D.Dzandu, M., (2023). Antecedent, behaviour, and consequence (a-b-c) of deploying the contact tracing app in response to COVID-19: Evidence from Europe,Technological Forecasting and Social Change, Volume 187, February 2023, 122217. https://doi.org/10.1016/j.techfore.2022.122217.

_ Dinev, T., McConnell, A.R., Smith, H.J., 2015. Research commentary—informing privacy research through information systems, psychology, and behavioral economics: thinking outside the "APCO" box. Information Systems Research 26, 639–655.

_ Dogruel, L., Joeckel, S., Vitak, J., (2017). The valuation of privacy premium features for smartphone apps: The influence of defaults and expert recommendations. Computers in Human Behavior 77, 230–239.

_ Emami, A., Khajeheian, D., 2019. Social norms and entrepreneurial action: the mediating role of opportunity confidence. Sustainability 11 (1), 158.

_ Ginosar, A., Ariel, Y., 2017. An analytical framework for online privacy research: What is missing? Information & Management, 54(7), 948-957. https://doi.org/10.1016/j.im.2017.02.004.

_ Graeff, T. R., Harmon, S., (2002). Collecting and using personal data: Consumers' awareness and Concerns. Journal of Consumer Marketing, 19(4), 302–318.

_ Gerrya F, Muraszki ewiczb J, aIannelli O. (2018). The drive forvirtual (online) courts and the failure to consider obliganid entification ,protection and privacy of victims. J computer law & security review.1–8. https://doi.org/10.1016/j.clsr.2018.06.002.

_ Groopman, J. (2015). Consumer Perceptions of Privacy in the Internet of Things: What Brands Can Learn from a Concerned Citizenry. Retrieved December 2016 from https://www.prophet.com/thinking/2015/06/new-reportconsumer-perceptions-of-privacy-in-the-internet-of-things/.

_ Goodin, Seth. (1999). Permission Marketing to Turn Strangers Into Friends and Friends into Customers. New York: Simon and Schuster Rockefeller. ISBN 0-684-83633-5. www.SimonSats.com.

_ Guo, J., Li, N., Wu, Y., et al. (2020). Examining help requests on social networking sites: integrating privacy perception and privacy calculus perspectives. Electron. Commer. Res. Appl. 39, 100828.

_ Harris, M. A., Brookshire, R., & Chin, A. G. (2016). Identifying factors influencing consumers' intent to install mobile applications. International Journal of Information Management, 36(3), 441–450. https://doi.org/10.1016/j.ijinfomgt.2016.02.004.

- Hallikainen, H., Laukkanen, T., (2018). National culture and consumer trust in e-commerce. Int. J. Inf. Manag. 38 (1), 97–106.
- Heravi, A., Mubarak, S., Choo, K.K.R., (2018). Information privacy in online social networks: uses and gratification perspective. Computers in Human Behavior 84, 441–459.
- Hirschprung, R., Toch, E., Bolton, F., Maimon, O., 2016. A methodology for estimating the value of privacy in information disclosure systems. Comput. Hum. Behav. 61,443–453.
- Hong, W., & Thong, J. Y. L. (2013). Internet privacy concerns: An integrated conceptualization
- And four empirical studies. MIS Quarterly, 37(1), 275–298.
- Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). Cultures and organizations: Software of the mind – Intercultural cooperation and its importance for survival (3rd ed.). New York:McGraw-Hill.
- Jiang, Z. (Jack), Heng, C. S., & Choi, B. C. F. (2013). Research note — Privacy concerns and privacy-protective behavior in synchronous online social interactions. Information Systems Research, 24(3), 579–595.
- Jozani,M. Ayaburi,E. Myung,Ko. Kim-Kwang Raymond Choo. (2020). Privacy Concerns and Benefits of Engagement with Social Media-enabled Apps: A Privacy Calculus Perspective. Computers in Human Behavior,https://doi.org/10.1016/j.chb.2020.106260.
- Jung, Y., & Park, J. (2018). An investigation of relationships among privacy concerns, affective responses, and coping behaviors in location-based services. International Journal of Information Management, 43, 15–24. https://doi.org/10.1016/j.ijinfomgt.2018.05.007.
- Kansal, P., (2014). Online privacy concerns and consumer reactions: Insights for future strategies. Journal of Indian Business Research, 6(3), 190-212.
- Kahn, C., & Ingram, D. (2018). Americans less likely to trust Facebook than rivals on personal data. Retrieved fromReutershttps://www.reuters.com/article/us-usa-facebook-poll/americans-less-likely-to-trust-facebook-than-rivals-on-personal-data-reuters-ipsospoll-idUSKBN1H10K3.
- Khare, A., Rakesh, S. 2011. Antecedents of online shopping behavior in India: An examination. Journal of Internet Commerce, 10(4), 227-244.
- Kim, D., Park, K., Park, Y., Ahn, J.H., (2019). Willingness to provide personal information:
- Perspective of privacy calculus in IoT services. Computers in Human Behavior 92, 273–281.
- Kim, D.J., Ferrin, D.L., Rao, H.R. (2008). A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents. Decis. Support Syst, 44(2), 544–564.
- Krafft, M, Arden, Christine M., Peter C. Verhoef. (2017). Permission Marketing and Privacy Concerns — Why Do Customers (Not) Grant Permissions?. Journal of Interactive Marketing. 39, 39 – 54. http://dx.doi.org/10.1016/j.intmar.
- Krishnamurthy, S. (2001) A Comprehensive Analysis of Permission Marketing. J Computer Mediated Communication. 6(2). https://doi.org/10.1111/j.1083-6101.2001.tb00119.x.
- Kumar, V. Zhang, XI (Alan). Anita Luo. (2014). Modeling Customer Opt-In and Opt-Out in a Permission-Based Marketing Context. Journal of Marketing Research (JMR), (51)4, 403-419. https://doi.org/10.1509/jmr.13.0169.
- Li, Y., 2011. Empirical studies on online information privacy concerns: literature review and an Integrative framework. Communications of the Association for Information Systems, 28, 453-496.
- Langley, M. (2015). Hide your health: addressing the new privacy problem of consumer wearables. Georgetown Law J. 103

(6), 1641–1660. https://www.researchgate.net/publication/285601528_Hide_Your_Health_Addressing_the_New_Privacy_Problem_of_Consumer_Wearables.

_ Lowry, Paul Benjamin, Jinwei Cao and Andrea Everard. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies:The case of instant messaging in two cultures. Journal of Management Information Systems, 27(4), 163–200. https://www.jstor.org/stable/41304596. doi1002753/MIS074201222270406.

_ Lount, R. B., Zhong, C.-B., Sivanathan, N., & Murnighan, J. K. (2008). Getting off on the wrong foot: The timing of a breach and the restoration of trust. Personality & Social Psychology Bulletin, 34(12), 1601–1612.

_ Lwin, May, Jochen Wirtz, and Jerome D. Williams (2007), "Consumer Online Privacy Concerns and Responses: A Power–Responsibility Equilibrium Perspective," Journal of the Academy of Marketing Science, 35, 4, 572–85.

_ Marr, B., 2018. How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read [WWW Document]. Forbes. URL https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-createevery-day-the-mind-blowing-stats-everyone-should-read/ (accessed 10.21.18).

_ Malm, S., 2018. Hushand divorces wife after seeing her with another man on Google Maps | Daily Mail Online [WWW Document]. URL https://www.dailymail.co.uk/news/article-6264139/Husband-divorces-wife-seeing-cuddling-man-Google-Maps.html (accessed 11.27.19).

_ McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., Pattinson, M., 2017[Internet]. Individual Differences and Information Security Awareness, 69. Comput Human Behav, pp. 151–156.

_ Martin, K.D., Borah, A., Palmatier, R.W. (2017). Data Privacy: effects on Customer and Firm Performance. J. Mark. 81, 36–58. https://doi.org/10.1509/jm.15.0497.

_ Martin, Kelly D., Abhishek Borah, and Robert W. Palmatier. (2017). Data Privacy: Effects on Customer and Firm Performance. Journal of Marketing. 81(1), 36–58.

_ Miltgen, C. L., Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. European Journal of Information Systems, 23(2), 103–125.

_ Mohammadzadeh Emmverdikhan, Z., Farokhbakht Fumani A., Saberi Hqyeq R., Factors affecting parent permission to accept the marketing of companies providing services (kindergartens) with an emphasis on the role of privacy in childrens mental health. J Child Ment Health. 2022; 9(3): 136-152. Doi:10.525447/jcmh.9.3.11.

_ Okazaki, Shintaro, Kirk Plangger, Douglas West and Menéndez Héctor D. (2020). Exploring digital corporate social responsibility communications on Twitter. Journal of Business Research. http://dx.doi.org/10.1016/j.jbusres.2019.09.006.

_ O'Reilly, Lara (2015), "The Online Advertising Industry Is About to Be Severely Disrupted — 'It's the Amputation of a Significant Revenue Stream'," Retrieved December 2016 from http://www.businessinsider.com.au/how-the-new-eu-data-laws-will-affect-the-online-advertising-industry-2015-12.

_ Paul, C., Scheibe, K.P., Nilakanta, S, 2020. Privacy Concerns regarding Wearable IoT Devices: how it is influenced by GDPR? In: Proceedings of the 53rd Hawaii International Conference on System Sciences, p. 10.

_ PEW Research Center, 2019. Demographics of Social Media Users and Adoption in the United

_ States. Pew Research Center: Internet, Science & Tech. URL

https://www.pewresearch.org/internet/fact-sheet/social-media/ (accessed 11.27.19).

- Phelps, Joseph, Giles D'Souza, and Glen Nowak (2001), "Antecedents and Consequences of Consumer Privacy Concerns: An Empirical Investigation," Journal of InteractiveMarketing, 15, 4, 2–17.
- Pour, M.S., Mangino, A., Friday, K., Rathbun, M., Bou-Harb, E., Iqbal, F., Shaban, K., Erradi, A., 2019. Data-driven Curation, Learning and Analysis for Inferring Evolving IoT Botnets in the Wild, in: Proceedings of the 14th International Conference on Availability, Reliability and Security, ARES '19. ACM, New York, NY, USA, pp. 6:1–6:10.
- Publilius, S. (2018). Quotable quote. Retrieved fromhttps://www.goodreads.com/quotes/503006-trust-like-the-soul-never-returns-once-it-is-gone.
- Robertson, J. (2012). Android apps collect too much user data, researcher says. Technology: Security. Retrieved fromThe Sydney Morning Heraldhttps://www.smh.com.au/technology/android-apps-collect-too-much-user-data-researcher-says-20121102-28oie.html.
- Raynes-Goldie, K., (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. First Monday 15.
- Rosen, Guy. (2018). Security Update, Facebook Newsroom. [Available at https://newsroom.fb.com/news/2018/09/security-update/].
- Rocher, L., Hendrickx, J.M., De Montjoye, Y.A., 2019. Estimating the success of reidentifications in incomplete datasets using generative models. Nature communications 10, 1–9.
- Shah, R. (2015). Do Privacy Concerns Really Change With the Internet of Things? Forbes. Retrieved December 2016 from www.forbes.com/sites/rawnshah/2015/07/02/do-privacy-concerns-really-change-with-the-internetof-things.
- Shankar, V., Venkatesh, A., Hofacker, C., Naik, P., (2010). Mobile marketing in the retailing environment: current insights and future research avenues. Journal of Interactive Marketing 24 (2), 111–120.
- Shiau, W.-L., Dwivedi, Y. K., & Lai, H.-H. (2018). Examining the core knowledge on facebook. International Journal of Information Management, 43, 52–63.
- Smith, H.J., Dinev, T., Xu, H. (2011). Information privacy research: an interdisciplinary review. MIS Q. 989–1015.
- Smith, H.J., Milberg, S.J., Burke, S.J., (1996). Information privacy: measuring individuals' concerns about organizational practices. MIS quarterly 167–196.
- Sullivan, Y.W., Kim D.J., (2018). Assessing the effects of consumers' product evaluations and trust on repurchase intention in e-commerce environments. International Journal of Information Management, (2018), 199-219.
- Sundar, S.S., Kang, H., Wu, M., Go, E., Zhang, B., 2013. Unlocking the Privacy Paradox: do cognitive heuristics hold the key? In: Proceedings of the CHI'13 Extended Abstracts on Human Factors in Computing Systems. CHI, pp. 811–816.
- Tsang, Melody M., Shu-C. Ho, & Ting-P. Liang. (2004). Consumer Attitudes toward Mobile Advertising: An Empirical Study. International Journal of Electronic Commerce, 8, 3, 65–78.
- Tsai, H.Y.S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N.J., Cotten, S.R., 2016. Understanding online safety behaviors: a Protection Motivation Theory perspective [Internet] Comput. Secur. 59, 138–150.
- Taddicken, M. (2014). The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. Journal of Computer-Mediated Communication, 19(2), 248–273.

https://academic.oup.com/jcmc/article/19/2/248/4067550.

- Smith, B, Tezinde, T, Murphy, J. (2002). GETTING PERMISSION: EXPLORING FACTORS AFFECTING PERMISSION MARKETING. JOURNAL OF INTERACTIVE MARKETING, 16 (4) AUTUMN 2002. Published online in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/dir.10041.
- Tow, W. N. F. H., Dell, P., & Venable, J. (2010). Understanding information disclosure behaviour in Australian Facebook users. Journal of Information Technology, 25(2), 126–136. https://journals.sagepub.com/doi/10.1057/jit.2010.18.
- Tucker, CE. (2014). Social Networks, Personalized Advertising, and Privacy Controls. Journal of marketing research, (51)5, 546-562. https://doi.org/10.1509/jmr.10.0355.
- Tsohou, A., Karyda, M., Kokolakis, S.,) 2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs [Internet] Comput. Secur. 52, 128–141.
- Van Schaik, P., Jansen, J., Onibokun, J., Camp, J., Kusev, P., 2018. Security and privacy in online social networking: risk perceptions and precautionary behaviour. Comput. Hum. Behav. 78, 283–297.
- Van Doorn, Jenny and Janny C. Hoekstra. (2013). Customization of Online Advertising: The Role of Intrusiveness. Marketing Letters, 24, 4, 1–13.
- Vallina-Rodriguez, N., Sundaresan, S., (2017). 7 in 10 smartphone apps share your data with thirdparty services. The Conversation.
- Verhoef, P.C., Rajkumar Venkatesan, Leigh McAlister, Edward C. Malthouse, Manfred Krafft, & Shankar Ganesan. (2010). CRM in Data-rich Multichannel Retailing Environments: A Review and Future Research Directions. Journal of Interactive Marketing, 24, 2, 121–37. https://www.sciencedirect.com/science/article/abs/pii/S1094996810000204.
- Wang, Y., & Herrando, C. (2019). Does privacy assurance on social commerce sites matter to millennials? International Journal of Information Management, 44, 164–177.
- Warkentin, M., Johnston, A.C., Walden, E., Straub, D.W., (2016). Neural Correlates of Protection Motivation for Secure IT Behaviors: An fMRI Examination. Journal of the Association for Information Systems; Atlanta 17, 194–215.
- Wedel, Michel and P.K. Kannan. (2016). Marketing Analytics for Data-rich Environments. Journal of Marketing, 80, 6, 97–121.
- Westin, A.F., (2003). Social and political dimensions of privacy. Journal of social issues 59, 431–453.
- Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. Decision Support Systems, 106, 44–52. https://doi.org/10.1016/j.dss.2017.12.003.
- Yang B., Lester, D., James, S. (2007). Attitudes toward buying online as predictors of shopping online for British and American respondents. Cyberpsychology & Behavior, 10(2), 198-203.
- Youn, S., Kim, S. (2019). Understanding ad avoidance on Facebook: antecedents and outcomes of psychological reactance. Comput. Hum. Behav. 98, 232–244.
- Xie, En, Hock-H. Teo, and Wen Wan (2006), "Volunteering Personal Information on the Internet: Effects of Reputation, Privacy Notices, and Rewards on Online Consumer Behavior," Marketing Letters, 17, 1, 61–74.
- Zukowski, T., Brown, I., (2007). Examining the influence of demographic factors on internet users' information privacy concerns. In Proceedings of the

2007 Annual Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries, Port Elizabeth, South Africa, October 2-3, pp. 197-204.

- Zhang, R., Chen, J.Q., Lee, C.J., 2013. Mobile commerce and consumer privacy concerns. Journal of Computer Information Systems, 53(4), 31-38.
- Zhao, Ling, Yaobin Lu, and Sumeet Gupta (2012), "Disclosure Intention of Location-related Information in Location-based Social Network Services," International Journal of Electronic Commerce, 16, 4, 53–90.
- Zhu, H., Ou, C.X., van den Heuvel, W.J.A., Liu, H. (2017). Privacy calculus and its utility for personalization services in e-commerce: an analysis of consumer decisionmaking. Inf. Manag. 54 (4), 427–437.
- Zlatolas, L. N., Welzer, T., Heričko, M., & Holbl, M. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. Computers in Human Behavior, 45, 158–167. https://doi.org/10.1016/j.chb.2014.12.012.