



Impacts of Trust in Government and Privacy Risk Concern on Willingness to Provide Personal Information in Saudi Arabia

¹ Alharbi Nesreen Nasser A., ² Yanhui Li

^{1,2} School of Information Management, Central China Normal University, Wuhan, China

Abstract: The current study followed a quantitative research design to determine the significance of the relationships presented in the research model. The relationships between Privacy risk concerns, benefit to disclose, trust, and willingness to provide personal information has been tested using SPSS. An online questionnaire in Arabic language was used collect data by distributing survey link via WhatsApp, Twitter, Snapchat, Facebook and Instagram. The sample consists out of 268 respondents. The results of the study indicate that trust has a positive impact on the privacy disclosure revenue whereas privacy risk concerns have a negative impact on the benefits of privacy disclosure. Also the privacy disclosure revenue has a positive impact on the willingness to disclose personal information. Users will increase the quantity and quality of information disclosure when the perceived benefit of personal information disclosure is high. The study also suggests that trust has a positive impact on the willingness to disclose personal information, and the user's degree of trust in government protection policies and information environment will directly disclose the user's information. Finally, privacy risk concerns have a negative impact on the willingness to disclose personal information, reduce the user's perception of the risk of the policy environment and technical environment, and will increase the willingness of users to disclose personal information. Keeping the above points in consideration the Saudi government to keep their aims high towards strong legislations regarding personal data sharing, privacy right and security of the data so that the trust of citizens can be gained towards e-governance.

Keywords: Privacy risk concerns, Benefit to disclose, Trust in government, Willingness to provide personal information, Privacy in Saudi Arabia

1. Introduction

Due to the increasing popularity of advancement in information technology and development of various industries, there is a growing popularity of electronic services in many fields. Among these developments, e-government platforms play an important role. E-government platforms involve the use of modern information technology and network technology. The main objective of e-government platform is to provide efficient, transparent and standardized electronic office for citizens. Governments which have e-government platforms are characterized as being open, transparent, simple and effective. Moreover, enterprises and citizens are provided with high level of service. However, there are some drawbacks which are associated with the use of e-government platforms. Particularly, uncertainty related with network information and lag of government protection results in increasing problems with information privacy. Increasing problems involve system intrusion, cyber-attacks, information disclosure and privacy violations. These factors are believed to impact negatively on government operations and there is a huge threat to the privacy of public information. Most of the scholars attempted to study the main motivation of people by involving them into different contexts. It has been reported that people are more likely to compare the benefits and risks in online social networks, general interest transactions and mobile phone activities before information disclosure decision is made. Moreover, people also take into consideration perceived enjoyment and perceived ownership of information. These two factors also play critical role as a motivation for people in online disclosure of information.

There is another approach to analyze the trust by analyzing the individual suggestion, social or government institutions. Trust and risk is combined feature that are managed by the vendors through their database system to control the interference with the unknown users into their system. In this context, Saudi Arabia is used as an example to investigate the privacy concerns and privacy disclosure intentions of e-government with surveys, and empirical

analysis. This study is similar to the previous studies in its interest in the field of privacy of personal information and its impacts on consumer, but it differs in its application in e-government transactions that provide to citizens who may have the incentive and benefit of providing sensitive personal information to these sites, in the presence of a secure website, excellent privacy policy and regulation that protects their rights in case of violation or loss of data.

2. Model Construction and Hypothesis

2.1 Statistics of the E-commerce Industry

Users require trust to use the web feature in order to make their successful transactions (Corbitt, Thanasankit, and Yi, 2003). Disclosing the information by the youngsters on the commercial website suggest their confidence and trust on the online feature (Heirman et al, 2013). It is indeed necessary for the electronic vendor to fulfill the requirement of privacy policy and regulation in order to attract and develop the trust of the users in future. However; currently online business is having new era and most of the users or consumers are likely to make online transaction because of their experience and trust on the website. In the past studies suggested that trust having direct impact upon the willingness of the users to disclose their information more freely (Frye and Dornisch, 2010).

It is effective to get the trust of the users through online and maintain this position in future to ensure that users should be retained and deliver the right and personal information with the confidence that their information should be used appropriately rather than breaching it (Mesch, 2012). Based on the theory of privacy computing, users will conduct a simple risk-return calculation when disclosing personal information. If the revenue is higher than the risk, they will choose to disclose more information. Therefore, we believe that privacy benefits have an important impact on privacy disclosure. The aim is to build a model among Privacy risk concern, trust, Benefit to Disclose and willingness to provide personal information and interpret it.

2.2 Hypotheses Development

Trust is highly effective feature in the communication; irrespective physical contact or virtual contact. Apart from the online trust; it can be analyzed the trust of the individual on the organization influences during the online communication (Mesch, 2012). In order to undertake the trust and its proposition for the disclosure; researcher is intended to initiate the assessment of trust of the people. It is quite difficult to complete a certain transaction without disclosure of some personal data. Precisely, it is quite complicated even if the disclosure is made to the trusted third party. In this regard, privacy becomes really important concern in e-commerce. In practice, with the presence of trusted people, the benefit of disclosing of personal information often outweigh its risks. In the case of trust and risk associated with the online (Park, Gunn and Han, 2012). Trust is the basic feature that requires by the user on the website that its privacy control should not allow others to access their information or intervene in the online transaction. It is suggested that as the risk of privacy exist then the consumer trust will be high which is evident as the trust urges the users to make online transactions and enjoy the benefits adequately without considering any risk involve in using the internet based transactions (Pavlou, 2003). Trust increases the confidence and willingness to share the information more freely while if the privacy controls are not adequate then it is likely possible it will impact upon the trust of the users and information will not be collected accurately (Henderson and Gilding, 2004). Trust of the user is being analyzed in different areas of research such as: relation with the market researchers (Moorman, Deshpande and Zaltman, 1993) seller and purchaser relations (Doney and Cannon, 1997). Trust is the main feature in the online transaction for the consumers that reduces the intensity of the risk adequately (Pavlou, 2003). In other words; as the trust increases the user did not feel threat or risk in the online transaction and it will develop the strong relation between the buyer and seller. As the risk becomes low the trust level will be high which will increase the electronic commerce maturity and confidence of the customers (Salam, Rao and Pegels, 2003). As far as the information and compliance is concern it is a mediating feature for both; however trust is the predictor of the information disclosure (Castro and Bettencourt, 2017).

Therefore, we conclude:

H1: Trust have positive impact on benefit to disclose

Majority of people are believed to do simple cost-benefit analysis while deciding whether to disclose their personal information or not (Laufer & Wolf, 1971). Providing privacy notice is really critical for the risk reduction when it comes to provide the personal information online. This allows consumers to be aware of companies information

practices. Consequently, it will be easier for the users to decide whether they want to disclose their personal information or not (Milberg, 1998). Most scholars paid great deal of attention to study the relationship between the users privacy concern and information disclosure behavior. Furthermore, scientists also use different methods in order to analyze this relationship. One of the most famous theories is known as utility maximization theory (Rust et. al, 2002) from the science of economics and social contract theory (Milne and Gordon, 1993) and social exchange theory (Andrade et al, 2002) from social psychology. All of these investigations were based on disclosing the personal information based on cost benefit analysis of users decisions. Privacy calculus takes into consideration the benefits and some other potential negative risks related to disclosing the personal information (Stone & Stone, 1990). According to Awad and Krishnan (2006) users are ready to disclose some personal information if they believe that benefits involved in revealing are far greater than the risks involved in such disclosure (Culnan, 2003). In accordance with Diney and hart (2006) Internet privacy concerns are believed to decrease the willingness of users to provide personal information online. This finding was also confirmed by Premazzi (2010) who found out that privacy concern decrease the consumer willingness to provide personal information with third parties in internet. Therefore, we conclude:

H2: privacy risk concerns have negative impact on benefit to disclose.

Majority of consumers believe that providing personal data can be beneficial. Particularly, many people are aware of the fact that the more detailed the information, the more relevant messages and promotion strategies and direct messages will be directed towards consumers. Thus, it can be stated that customers are ready to provide personal information given that certain conditions are met (Godin, 1999). It has been suggested by many researchers that consumers are ready to disclose personal information if they believe that it is going to be beneficial for them. Precisely, they do comparison between the potential gains and losses from the disclosure of the information. If the potential benefits outweigh the potential risks, then, customers are ready to disclose their information. In other words, they consider the trade off.

The other feature which is introduced as the second exchange to illustrate the non financial exchange include the privacy calculus, then the consumers are willing to bring their information to get the best quality services and other offers of discount (Culnan and Bies, 2003). Consumers enjoy tangible and intangible benefits such as (Discounts, rewards, coupons, social benefits and others (Glazer, 1991; Milne and Gordon, 1993; Chellappa and Sin, 2005). The focus is being towards the relations between the privacy concern and information disclosure behavior was given by the researchers.. The research conducted by Smith, Dinev and Xu (2011) studied the potential gains from the information privacy by studying the notion of privacy in the form of commodity. According to Smith et al (2011) there are three main categories of information privacy gains including financial rewards, personalization and social adjustment benefits. The consumers usually perform benefit and risk analysis if they feel it is having no risk then it is favorable for the organization to get the required information easily and get more privacy control on the website. There are different benefits that are offered online to the consumers such as; opportunity, bargain, purchase and privacy; in the case of opportunity benefit consumer is offered some special pricing of products that are less as per the market or having positive results. Bargain benefit is gaining best deal to buy the products online; purchase benefits such as; best quality services, customized products and special discounts (Gupta et al, 2010). Privacy benefits that consumers are assured if they make online transaction their information will be secured and safe adequately. The studies suggested that consumers agree on the cost benefit lay off on the basis of the consumer's decision to deliver the personal information. As far as the privacy calculus includes the acceptance of advantages and potential adverse results that are being caused due to the disclosing the personal information. In the case of disclosing the information on the website use performs the cost benefit analysis adequately (Laufer and Wolfe, 1977; Stone and Stone, 1990). Therefore, we conclude:

H3: Benefit to disclose have a positive impact on willingness to provide personal information.

It has been found out that there is a strong positive connection between the trust and willingness of the user to provide personal information during the online transactions. Privacy policies play an important role in gaining the trust of the users. The results of research findings show that in order to build the trust, it is important to establish informative privacy policies. Moreover, users should be convinced that providing and disclosing personal information is regarded as a low risk proportion (Milne&Boza, 2000). The importance of trust can be seen both in public as well as in private sector. Trust plays crucial role in business as well as in social relationships. Due to the existence of trust climate,

private sectors are found to make investment easier whereas for public sector , trust allows them to perform better. Carter and Weerakkody (2008) service oriented trust relies on two important factors. The first factor is considered to be service provider whereas another factor mediates the provision of that factor. Moreover, the other two factors should be taken into account which impact on government. These factors include trust in e-government and trust towards that way services are provided (Yildirim, 2010, Teo, 2005). Trust in technology, how it is used, has also crucial impact on how services are being delivered to customers. Thus, it can be concluded that e-government plays a crucial role in formulating the trust of customers.

Therefore, we conclude the following:

H4: Trust have a positive impact on willingness to provide personal information.

Willingness to provide privacy information online is closely related to concern over privacy. Online risk is the degree to which user anticipate that there information can be lost and can be steal by the unknown party for their benefit. Most of the consumers are not relying on the online transaction because of their information breach concern that increases the risk factor in their mind and restrict them to make any transaction online (Dutton and Shepherd, 2006).

Overwhelming usage of personal information is believed to have a negative impact on consumer privacy. It can be seen in terms of two ways. Lack of appropriate privacy controls results in improper utilization of personal information (Smith, 1996). Consequently, it may result in unsolicited e-mails, credit card fraud and identity theft. Moreover, personal information can be used for another purposes other than planned (Culnan, 1993).

The excessive use of personal information hurts consumer privacy in two major ways. First, the improper use of personal information due to lack of appropriate privacy controls (Smith et al. 1996), such as by unsolicited e-mails, credit card fraud, or identity theft. Second, the unauthorized use of personal information without the consumer's consent for purposes outside of the original exchange (Culnan 1993). Accordingly, concerns about information privacy relate to the improper use of personal information, disclosure of personal information to outside parties, and the unauthorized secondary use of personal information without the individual's consent. When individuals face privacy threats, such as the unauthorized use, modification or dissemination of their private information, they can lessen their exposure to others simply by deciding not to disclose personal information. The communication is electronic and easily terminated or avoided. Also, Li et al. (2011) made a comprehensive study of antecedents to information disclosure in online transactions and found significant relationships between perceived fairness, perceived privacy risks and benefits and intention to disclose personal information. Legal personnel in the public sector or in the private sector such as banks, hospitals and communication companies and shops that have information, such as name, age, sex, address and means of communication, financial and health status, and interests of the person in the shop. Unfortunately, some companies or employees "sell this information as well as phone numbers of their customers for advertising companies with huge amounts of money, and has some marketing communications companies. And also has some shops do withdrawals on gifts may be illusory, awards and monitor a large number of shoppers information used in spam. Generally, great privacy concerns indicate a lack of confidence in the reliability and integrity of others, and this inevitably leads to a corresponding reduction in self-disclosure, because the potential risks to individuals are substantial.

H5: Privacy risk concerns has a negative impact on willingness to provide personal information.

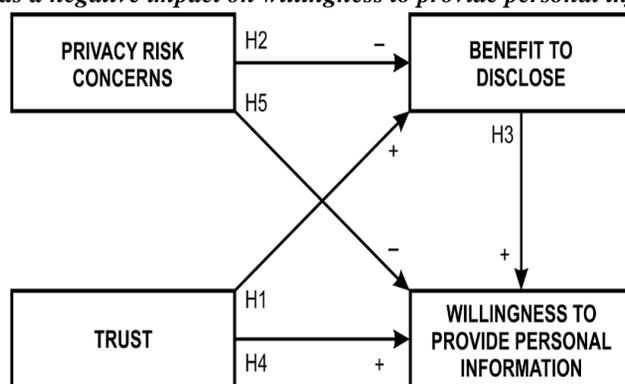


Figure 1: Research Model

3. Data collection

An online questionnaire to identify the relationships between each FTC category in online privacy statements of websites/Government regulation and its effect on trust/privacy concern and relationships with willing to provide personal information and benefit to disclose has been conducted. The questionnaire was translated to Arabic language and data was collected online via Whats App, Twitter, Snapchat, Facebook and Instagram. The sample consists out of 268 respondents. The variables are trust, privacy risk concerns, willingness to provide information, benefit of disclose, the five FTC principles (notice, choice, access, security, enforcement) and Government regulation. The research uses 5-Point Likert-type scales with anchors ranging from 1 strongly disagree to 5 strongly agree for all variables, additional to demographic information.

Out of total 268 respondents 130 were male and 138 were female respondents. The frequency distribution shows that the respondents between the age of 16 and 24 were around 10%, 25 and 34 were around 40%, 35 and 44 were around 33% while the respondent of 45 years and above were around 17%.

4. Data Analysis

Demographic Characteristics, missing data, outliers, normality about Model 2 were shown in chapter 4, therefore, we will analyze linearity and research hypotheses in directly in this section.

Table 1: Correlation matrix of variables in Model 2

		WILLINGNESS TO PROVIDE			
		PERSONAL INFORMATION	BENEFIT TO DISCLOSE TRUST	PRIVACY RISK CONCERN	
WILLINGNESS TO PROVIDE PERSONAL INFORMATION	Pearson Correlation	1	.413**	.592**	-.524**
	Sig. (2-tailed)		.000	.000	.000
	N	268	268	268	268
BENEFIT TO DISCLOSE TRUST	Pearson Correlation	.413**	1	.443**	-.458**
	Sig. (2-tailed)	.000		.000	.000
	N	268	268	268	268
PRIVACY RISK CONCERN	Pearson Correlation	.592**	.443**	1	-.594**
	Sig. (2-tailed)	.000	.000		.000
	N	268	268	268	268
PERSONAL INFORMATION	Pearson Correlation	-.524**	-.458**	-.594**	1
	Sig. (2-tailed)	.000	.000	.000	
	N	268	268	268	268

** . Correlation is significant at the 0.01 level (2-tailed).

In order to distinguish two models, the hypotheses of model 2 are denoted by (b).

Table 2: Hypotheses of the Study (Model 2)

H1b: Trust have positive impact on benefit to disclose.
H2b: Privacy risk concerns have negative impact on benefit to disclose.
H3b: Benefit to disclose have a positive impact on willingness to provide personal information.
H4b: Trust have a positive impact on willingness to provide personal information.
H5b: Privacy risk concern has a negative impact on willingness to provide personal information.

Table 3: Regression 1

Dependent Variable	Independent variables
Benefit to Disclose	TRUST PRIVACY RISK CONCERN

Table 4: Regression (1) in model (2)

Hypotheses	Independent Variables	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
H1	PRIVACY POLICY	.279	.070	.265	4.015	.000
H2	GOVERNMENT REGULATION	-.370	.081	-.300	-4.558	.000

a. Dependent Variable: Benefit to Disclose

Table 5: Regression 2

Dependent Variable	Independent variables
Willingness to Provide Personal Information	BENEFIT TO DISCLOSE TRUST PRIVACY RISK CONCERN

Table 6: Regression (2) in model (2)

Hypotheses	Independent Variables	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
H3	BENEFIT TO DISCLOSE	.127	.053	.133	2.426	.016
H4	TRUST	.404	.061	.399	6.590	.000
H5	PRIVACY RISK CONCERN	-.267	.072	-.226	-3.710	.000

a. Dependent Variable: TRUST

Table 7: Summary of Hypotheses (Model 2)

Hypotheses of the Study (Model 2)	P-value	Results
H1b: Trust have positive impact on benefit to disclose.	.000	Supported
Privacy risk concerns have negative impact on benefit to disclose.	.000	Supported
Benefit to disclose have a positive impact on willingness to provide personal information.	.016	Supported
Trust have a positive impact on willingness to provide personal information	.000	Supported
Privacy risk concern has a negative impact on willingness to provide personal information.	.000	Supported

The above table of summary of hypotheses show that all hypotheses presented in model 2 are supported as their p-values are less than 0.05 showing the significant positive impact of trust on benefit to disclose, significant negative impact of privacy risk concern on benefit to disclose, significant positive impact of benefit to disclose on willingness to

provide personal information, significant positive impact of trust on willingness to provide personal information and significant negative impact of privacy risk concern on willingness to provide personal information.

5. Discussion of Key Results

H1b: Trust have positive impact on benefit to disclose.

The result of the H1b suggested that trust has a positive impact on benefit to disclose ($\beta = 0.265$, $P < 0.05$). Trust is considered as the most expanded topic in different context and areas. Trust can be defined as the readiness of the one individual including the risk of the actions of other person indulging with the perception of getting some benefit unconditionally (Mayer, 1995). Trust is having relation with the repetitions of using the particular technology (Guzzo, 2016). Trust is having adverse relation with the online feature: sharing the information and presenting online enhances the trust of the individual (Henderson 2004). Trust on the internet is considered as the cyber trust; in other words; trust on the technology and its capability of communication (Dutton 2006). Trust is highly risky in the case of online transaction therefore; majority of the people are reluctant to adopt the technology and have the interaction with the technology (Wallace, 2001). Those individuals that are having low level of trust on the other person did not accept the cyber trust and internet cannot be accepted by the individual as the trustworthy feature (Rose, 2003). Trusted consumers are intended to make their shopping through internet (Uslaner, 2004).

The researcher conducted the study in order to analyze the relations between institutional trust and consumer perceived risk; it is suggested that as the trust increases the risk decreases in the institutions (Salam, 2003). As the risk becomes low the trust level will be high which will increase the electronic commerce maturity and confidence of the customers (Salam, Rao and Pegels, 2003). The degree of trust varies: there are different stages of the trust in the publish sector because of the corruption (Arnold, 2012). As far as the information and compliance is concern it is a mediating feature for both; however trust is the predictor of the information disclosure (Castro and Bettencourt, 2017). In the current studies; it is analyzed between the relations of trust in organization and disclosing the personal information that do not produce evident conclusion (Mesch, 2012). Influence of trust on the benefit of disclosing the information. The findings of the study suggested that previously conducted researches are having similar findings about the electronic government which will increase the tendency of declaring the information among people.

H2b: Privacy risk concerns have negative impact on benefit to disclose.

The result of the H2b suggested that privacy risk concern has a negative impact on benefit to disclose ($\beta = -0.300$, $P < 0.05$). The requirement of the communication with the technology needs information about the people. It is evident that internet is having highly impact in daily routine life; in the phase of interaction, acquiring knowledge, using different application and others. In order to get benefited from the applications; it is important for the users to input the information into the technology. That kind of information that is personal increases the fear and concern considerably. Privacy is highly important feature that is considered the concern for the users. The highly used and important feature of information and communication technology (ICT) and the internet is the e-government. E-Government website provides information and services to the users. The data and knowledge that is being collected by the government website enhancing; but it is a concern that how much their information is being secured (Al Jamal and Abu Shanab, 2015).

The internet and privacy are the main issues that required by the researchers to conduct research (James Wilson, 2000). In the past studies developed the privacy concern the most serious result of the studies. Concern for Information Privacy (CFIP) highly focused upon citizens behavioral intentions. CFIP is used to illustrate the readiness to present the personal data (Dinev and Hart, 2000) or intention to make online transaction (Brown and Muchira, 2004). In the case of privacy calculus person analyze the cost and benefit analysis in order to disclose their information to the government (Laufer and Wolfe, 1977). Those citizens are likely to disclose their personal information if they are being assured by the privacy policy of the organization or government (Culnan and Armstrong, 1999). The model was developed for the assessment of online transactions (Dinev and Hart, 2006).

Customers or consumers are having issues or concern in order to face the internet because majority considered that it is highly risky to disclose the personal information because there are many features or technologies available that can breach the privacy policies adequately and steal their information which increases their concern and did not allow them

to trust or use the online transaction approach (Hui et al, 2006). However; it is relatively easy and quick to get the desired product or service through conducting online transaction. Website vendors are not able to ensure their users that their information will not be misleading in future but due to the latest technologies has increases the chances of interference into the database through different links and sources that can increases the threat or risk of the consumers (Hoffmann et al, 1999).

H3b: Benefit to disclose have a positive impact on willingness to provide personal information

The result of the H3b suggested that benefit to disclose has a positive impact on willingness to provide personal information ($\beta = 0.133$, $P < 0.05$). Disclosing the personal data in return of some benefits is a usual phenomenon in the online marketing context. If the person is disclosing their email address or other information they might get future discount or benefits in the purchases. The result is associated with the exchange benefit in providing the personal information. In the case of accepting the financial benefits discounts are the most likely forms to be received by the person (Xu et al.2009). People are encouraged to display their information through internet because of different causes including the economic benefit (Benndorf and Normann, 2017), this research is based upon the discussed phenomena. It is evident that consumers are offered highly attractive packages in response to get the desired information; these benefits are financial, or non financial, entertainment as well (Aydoğan, Öztürk, and Razeghi, 2017).

It is also possible that person are intended to provide the information because they are being treated individually (Graeff and Harmon, 2002). Once the analysis of the consumers is being that benefits increased than the risk they will be motivated to present more information personally (Milne and Culnan, 2004) the benefits are having different feature because it depends the usage of the data whether in the social media or in the electronic commerce (Sun, Wang, 2014). Mostly consumers considered that disclosing information to the organization will be beneficial in terms of getting good services, information about the discounts and promotions and others. That is the reason consumers are willing to provide their personal information accurately (Godin, 1999).

In the past researches there is a clear evidence that organizations are motivating the consumers through different means of providing some benefit if they are able to reveal their personal information such as; benefits of discounts, promotions, cash voucher, loyalty points and others which is having value to the consumers (Aydoğan et al, 2017). Once the user's expectations are met of receiving the potential benefits then it is likely possible that organization will be able to get the trust and confidence to get the more personal information for their benefit (Liebermann and Stashevsky, 2002). It is suggested that these benefits are highly important for the consumers because it helps them to make the decision and accept the offer of the organization (Sun et al, 2014).

H4b: Trust have a positive impact on willingness to provide personal information.

The result of the H4b suggested that trust has a positive impact on willingness to provide personal information ($\beta = 0.399$, $P < 0.05$). The researcher conducted the study in order to analyze the relations between institutional trust and consumer perceived risk; it is suggested that as the trust increases the risk decreases in the institutions (Salam, Rao and Pegels, 2003). As the risk becomes low the trust level will be high which will increase the electronic commerce maturity and confidence of the customers (Salam, Rao and Pegels, 2003). Moreover; trust on the internet comes with the experience if the users feel safe and secure in order to successfully conduct their online transaction which will increase the behavior intention of the users towards the online purchases while on the other hand; it will be adverse if the privacy control or trust has been broken due to the breach in the privacy controls (Corbitt, Thanasankit and Yi, 2003). For online organization trust is the key to success for conducting their business if the users are not find privacy feature adequate then it will be highly ineffective for the online vendors to run their business because the trust of the users has been broken due to the breach of their personal data information. Trust develops the willingness of the user to share the information with the organization through online and enable the organization to use their information for their respective area rather than handing over to the other parties that can misuse the information (Boritz and No, 2011).

In the past studies it is being suggested through the findings that trust and willingness or behavior intention is having positive significance in disclosing the information to the electronic vendors because trust is the key feature that emerge the motivation and urge the consumers to pass the required information to the organization. The level of trust should be high then it will be easy for the organizations to gain the required data and influence the consumer intention to

willingly disclose the personal information (Salam, Rao and Pegels, 2003). The degree of trust is directly associated with the willingness of the user to disclose information on the request. It will be apprehended if the users are having prior experience of using the online transaction features and they are having fully trust upon the privacy control of the website or organization online; then it will be feasible for the users to develop relations and provide the information on consistent basis (Mesch, 2012).

H5b: Privacy risk concern has a negative impact on willingness to provide personal information.

The result of the H5a suggested that privacy risk concern has a negative impact on willingness to provide personal information ($\beta = -0.226, P < 0.05$). Personal data is considered as the currency in the case of information economy (Fife and Orjuela, 2012). Providing personal data is the way of enhancing the value of the information (Montes et al, 2016) which is being gathered; processed and used in order to provide confirmation about the privacy control of the organization (Wu et al, 2011). In the past literature two features are highly prominent that is privacy of the personal data and self disclosure is being analyzed in the perceived benefits against the information provided. This feature also exists in the Privacy Calculus Theory (Culnan and Armstrong, 1999;).

There are major two factors that impact upon the individual to disclose their personal information that are endogenous and exogenous (Culnan and Bies, 2003; Phelps et al, 2000). Therefore; these features impact upon the behavior of the person likewise; their choice of variety of regulations and willingness to disclose the information. The study in the past based upon the behavior towards the privacy and to share information along with the intention to provide the personal data (Miyazaki and Krishnamurthy, 200) and react to the privacy breaching technology (Thiesse, 2007). In the past research study the analysis was made about the individual's willingness to disclose personal information to get some benefits through the privacy protection online (Park et al, 2012). The composite index was developed for the nine personal data to assess the intention of the users to what extent data information can be provided. Summarizing the several data sets of intentions of the user to disclose the information but it is evident that it will impact upon the user privacy control of the users. There is an ambiguity about what kind of information impact the person's control upon the personal data. It is suggested that new technology is the biggest threat for the privacy controls because it is possible to intervene into the firewall and breach can be possible to access the personal information (Reed et al, 2016). Unknown source can access the information which includes the reviewing, track, behavior of browsing trends, internet traffic through cookies, location access, identity tracking, access to the email, theft of digital ID and others. Collective data is not an issue or having any threat to the privacy policy of the user that are collected from different users. In the case of advance technology era; it is possible to identify the identity of the individual get the personal information and can give threat of publishing the personal information online (Reed et al, 2016).

It is suggested that anonymous data is gathered prior to the sharing purpose; the data can be accessed by the individual by over passing the privacy control and get matched the data with the different database in order to link the individual data particularly with the different sources of information online (European Voice, 2014; Christiansen, 2011). The previous study suggested the similar feature that unknown identity can access the information with the users with the help of other sources of information (Chen et al, 2009; Jiang et al, 2002). Vendors online can increase the confidence and trust of the users through offering the privacy controls effectively which increases the effectiveness of the website proficiency and secure online transactions. However; majority of the online vendors ensures to the user that their website is following the regulation and privacy control but ultimately it is being observed that privacy control are lacking and their personal data is being used by the other parties adequately (Uslaner, 2004).

6. Conclusion and Contributions

6.1 Conclusion

The research contributions to the existing body of knowledge are provided as follows. First, trust has a positive impact on the privacy disclosure revenue. Users will perform simple income risk calculation when information disclosure, and trust will adjust the user income calculation. Second, privacy risk concerns have a negative impact on the benefits of privacy disclosure, and high-risk attention will reduce the perceived benefits of users. Third, the privacy disclosure revenue has a positive impact on the willingness to disclose personal information. Users will increase the quantity and quality of information disclosure when the perceived benefit of personal information disclosure is high. Fourth, trust has a positive impact on the willingness to disclose personal information, and the user's degree of trust in government

protection policies and information environment will directly disclose the user's information. Fifth, privacy risk concerns have a negative impact on the willingness to disclose personal information, reduce the user's perception of the risk of the policy environment and technical environment, and will increase the willingness of users to disclose personal information.

6.2 Implications and Contributions

The current study followed a quantitative research design to determine the significance of the relationships presented in the research models. Acquiring an in-depth understanding of the phenomena can help with training and awareness of using e-government and educating the citizen regarding online privacy and security can be another variable. Future studies can devised the model keeping this point in consideration to understand the usefulness of such education. In view of the discussion there is high concern should be given by the organization that privacy control should be adequate that cannot be accessed by the unknown party that violate the regulation of the government privacy policy and did not allow any other person to publish the personal information of the users. Keeping the above points in consideration the Saudi government to keep their aims high towards strong legislations regarding personal data sharing, privacy right and security of the data so that the trust of citizens can be gained towards e-governance.

References

- Arnold, C., E. V.Sapir, G.Zapryanova. Trust in the institutions of the European Union: A cross-country examination. *European Integration Online Papers*, 2012, 16(2):29–59.
- Benndorf V , Hans Milheo Normann. The willingness to sell personal data. *Scandinavian Journal of Economics*, 2017, 120(4). [Crossref](#)
- Boritz J E., No W G. E-Commerce and privacy: Exploring what we know and opportunities for future discovery. *Journal of Information Systems*, 2011, 25(2):11-45 [Crossref](#)
- Chen H., Xiao Y., Hong X , et al. A survey of anonymity in wireless communication systems.
- Security & Communication Networks, 2009, 2(5):427-444. [Crossref](#)
- Christiansen L . Personal privacy and Internet marketing: An impossible conflict or a marriage made in heaven?. *Business Horizons*, 2011, 54(6):0-514. [Crossref](#)
- Corbitt B J , Thanasankit T , Yi H . Trust and e-commerce: a study of consumer perceptions.
- *Electronic Commerce Research and Applications*, 2003, 2(3):203-215. [Crossref](#)
- Culnan M J, Armstrong P K. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, 1999, 10(1):104-115. [Crossref](#)
- Culnan M J, Bies R J. Consumer Privacy: Balancing Economic and Justice Considerations. *Journal of Social Issues*, 2010, 59(2):323-342. [Crossref](#)
- Culnan M J. "How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use.. *Mis Quarterly*, 1993, 17(3):341-363. [Crossref](#)
- Dinev T , Hart P . Internet privacy concerns and their antecedents - measurement validity and a regression model. *Behaviour & Information Technology*, 2004, 23(6):413-422. [Crossref](#)
- Dinev T, Xu H, Smith J H, et al. Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, 2013, 22(3):295-316 [Crossref](#)
- Godin S. Permission Marketing: Turning Strangers into Friends and Friends into Customers. *Journal of Marketing Research*, 1999, 77(4):171-174. [Crossref](#)
- Graeff T R , Harmon S . Collecting and using personal data: consumers' awareness and concerns. *Journal of Consumer Marketing*, 2002, 19(4):302-318. [Crossref](#)
- Guzzo T, Ferri F, Grifoni P. A model of e-commerce adoption (MOCA): consumer's perceptions and behaviours. *Behaviour & Information Technology*, 2016, 35(3):196-209. [Crossref](#)
- Heirman, Wannes, Walrave, et al. Predicting Adolescents' Disclosure of Personal Information in Exchange;for Commercial Incentives: An Application of an Extended Theory of;Planned Behavior. *Cyberpsychology Behavior & Social Networking*, 2013, 16(2):81-87. [Crossref](#)
- Henderson S , Gilding M . "I've Never Clicked this Much with Anyone in My Life": Trust and Hyperpersonal Communication in Online Friendships. *New Media & Society*, 2004, 6(4):487-506. [Crossref](#)
- Hui K L, Goh C Y, Goh C Y. Online information disclosure: Motivators and measurements. 2006. Hui K L, Tan B C Y, Goh C Y. Online information disclosure: Motivators and measurements. *ACM Transactions on Internet*

- Technology (TOIT), 2006, 6(4): 415-441. [Crossref](#)
- James S W. The Use Of Survey Data In Privacy Research[D]. North Carolina: the faculty of the School of Information and Library Science of the University of North Carolina at Chapel Hill,2000
 - Laufer R S , Wolfe M . Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. Journal of Social Issues, 1977, 33(3). [Crossref](#)
 - Lee D J , Ahn J H , Bang Y . Managing Consumer Privacy Concerns in Personalization: A Strategic Analysis of Privacy Protection. MIS Quarterly, 2011, 35(2):423-444. [Crossref](#)
 - Liebermann Y , Stashevsky S . Perceived risks as barriers to Internet and e-commerce usage. Qualitative Market Research: An International Journal, 2002, 5(4):291-300. [Crossref](#)
 - Mayer R C, Davis J H, Schoorman F D. An Integrative Model of Organizational Trust. Academy of Management Review, 1995, 20(3):709-734. [Crossref](#)
 - Mesch G S . Is online trust and trust in social institutions associated with online disclosure of identifiable information online?. Computers in Human Behavior, 2012, 28(4):1471-1477. [Crossref](#)
 - Milne G R , Maria [†] ugenia Boza. Trust and Concern in Consumers' Perception of Marketing Information Management Practices. Journal of Interactive Marketing, 1999, 13(1):5-24. [Crossref](#)
 - Milne G R , Maria [†] ugenia Boza. Trust and Concern in Consumers' Perception of Marketing Information Management Practices. Journal of Interactive Marketing, 1999, 13(1):5-24. [Crossref](#)
 - Milne G R , Maria [†] ugenia Boza. Trust and Concern in Consumers' Perception of Marketing Information Management Practices. Journal of Interactive Marketing, 1999, 13(1):5-24. [Crossref](#)
 - Park Y J , Campbell S W , Kwak N . Affect, cognition and reward: Predictors of privacy protection online. Computers in Human Behavior, 2012, 28(3):1019-1027. [Crossref](#)
 - Pavlou P A . State of the information privacy literature: Where are we now and where should we go?. MIS Quarterly, 2013, 35(4):977-988. [Crossref](#)
 - Phelps J, Nowak G , Ferrell E . Privacy Concerns and Consumer Willingness to Provide Personal Information. Journal of Public Policy & Marketing, 2000, 19(1):27-41. [Crossref](#)
 - Phelps J , Nowak G , Ferrell E . Privacy Concerns and Consumer Willingness to Provide Personal Information. Journal of Public Policy & Marketing, 2000, 19(1):27-41. [Crossref](#)
 - Reed P J , Spiro E S , Butts C T . Thumbs up for privacy?: Differences in online self-disclosure behavior across national cultures. Social Science Research, 2016: 59, 155-170 [Crossref](#)
 - Reyhan Aydoğan, Pinar Özturk, Razeghi Y . Negotiation for Incentive Driven Privacy- Preserving Information Sharing// International Conference on Principles and Practice of Multi-Agent Systems. Springer, Cham, 2017. [Crossref](#)
 - Rose R. The dynamics of digital choice//paper delivered at the Information, Communication, Society Symposium, Oxford Internet Institute, University of Oxford. 2003, 19.
 - Salam A F, Rao H R, Pegels C C. Consumer-perceived risk in e-commerce transactions. Communications of the ACM, 2003, 46(12): 325-331. [Crossref](#)
 - Smith H J , Burke M S J . Information privacy: Measuring individuals concerns about organizational practices. MIS Quarterly, 1996, 20(2):167-196. [Crossref](#)
 - Smith H J , Milberg S J , Burke S J . Information privacy: Measuring individuals' concerns about organizational practices. MIS quarterly, 1996: 167-196. [Crossref](#)
 - Smith J H , Dinev T , Xu H . Information privacy research: An interdisciplinary review. Social Science Electronic Publishing, 2011, 35(4):989-1015. [Crossref](#)
 - Stone, E.F., & Stone, D.L.. Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. Research in Personnel and Human Resources Management, 1990,8(3) 349-411.
 - Sun Y, Wang N, Shen X L. Perceived Benefits, Privacy Risks, and Perceived Justice in Location Information Disclosure: a Moderated Mediation Analysis//PACIS. 2014: 135.
 - Uslaner E M. Trust, civic engagement, and the Internet. Political Communication, 2004, 21(2): 223-242. [Crossref](#)
 - Wallace P. The psychology of the Internet. Cambridge University Press, 2015. [Crossref](#)
 - Wu K W , Huang S Y , Yen D C , et al. The effect of online privacy policy on consumer privacy concern and trust. Computers in Human Behavior, 2012, 28(3):889-897. [Crossref](#)
 - Wu K W, Huang S Y, Yen D C, et al. The effect of online privacy policy on consumer privacy concern and trust. Computers in human behavior, 2012, 28(3): 889-897. [Crossref](#)

- Xu H, Teo H H, Tan B C Y, et al. The role of push-pull technology in privacy calculus: the case of location-based services. *Journal of management information systems*, 2009, 26(3): 135-174. [Crossref](#)
- Xu H, Teo H H, Tan B, et al. The role of push--pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems*, 2009, 26(3):135-174. [Crossref](#)