Aug 10th, 12:00 AM

INDIVIDUAL PRIVACY EMPOWERMENT IN ELECTRONIC SERVICE

Bright Frimpong
The University of Texas Rio Grande Valley, bright.frimpong01@utrgv.edu

Jun Sun
The University of Texas Rio Grande Valley, jun.sun@utrgv.edu

Individual Privacy Empowerment in Electronic Service

Completed Research

Bright Frimpong
University of Texas Rio Grande Valley
bright.frimpong01@utrgv.edu

Jun Sun
University of Texas Rio Grande Valley
jun.sun@utrgv.edu

Abstract

This study is motivated by the many reports on the lack of individual privacy empowerment in Facebook's and Google's recent research programs. Literature on privacy empowerment has mostly focused on the e-commerce context where participants are often perceived as potential customers and data collected are mostly for advertising purposes. In this study, we demonstrate how e-service companies can empower individuals to participate in their research programs and how such perceived empowerment can differ in different scenarios of data sensitivity. Three dimensions of privacy empowerment (informativity, optionality and controllability) are identified and modeled in an information sensitivity context. Findings indicate that while informativity is very crucial at all levels of data sensitivity, optionality is only essential to achieving privacy empowerment in a highly sensitive data context. Practically, we recommend companies to integrate both informativity and optionality into their research designs to provide participants with a perceived sense of privacy empowerment.

Keywords

Privacy empowerment, e-service, information sensitivity, privacy control.

Introduction

Multiple surveys and opinion polls have found information privacy to be a very important topic among numerous stakeholders including consumers, scholars, privacy activists, policy analysts and government regulatory bodies (Smith et al. 2011). Several privacy tools (TRUSTe and P3P) and legal frameworks have been developed and implemented to help protect online consumer privacy. However, the impact of such tools on curbing online privacy abuse is abysmal due to their low popularity among online consumers. An emerging common theme, championed by the Federal Trade Commission (FTC), is the idea to empower individuals to control the management of their personal information. Midha (2012) defines privacy empowerment as an individual's perception of the extent to which one can control the dissemination and use of personal information. The concept of individual privacy empowerment is supported by several research findings which suggest that information privacy abuse can be addressed if individuals are given flexible control (Phelps, 2000), allowed to opt-in to data collection and provided access to prior collected data (Midha et al. 2004).

Context has been found to have a significant moderating influence on the nature of privacy constructs (Malhotra et al. 2004). For instance, previous studies have found that consumer disclosure behavior can be moderated by these contexts; the company collecting the information and the type of information being collected (Phelps et al. 2000; Sheehan and Hoy 2000). Literature on privacy empowerment have mostly focused on the e-commerce context where participants are often perceived as potential customers and data is mostly collected for personalized advertising purposes (Van Dyke et. al 2007; Prince 2018). As such, this study looks at privacy empowerment in the electronic service (e-service) context where tech-companies like Dell, IBM, Google and Facebook conduct research programs with the intention to provide cutting-edge products and generate analytical insights to strategically improve service offerings.

Over the years, a lot of tech-companies have conducted large-scale market research programs to enhance their product offerings and will continue to do so for the foreseeable future. However, critics claim that adopted procedures in these research programs do not empower individuals to make informed decisions prior to participating in the programs despite the monetary incentives offered to participants. The background of this study is motivated by the many reports on Facebook's and Google's deception practices in their recent research programs which was found to have preyed on unsuspecting individuals and contained multiple instances of privacy violations. Google's research program was conducted to collect facial scans of people to improve its facial recognition software for the company's line of pixel phones while Facebook's research program spied on participants through a designated research app and reportedly collected sensitive data including web searches, emails, browsing activity and private messages. After receiving criticism for the deceptive practices and non-ethical privacy violations, both companies publicly committed to ensuring that future research and data collection programs will be designed to empower individuals make informed decisions regarding their participation. In this study, we provide participants with hypothetical scenarios depicting Google's and Facebook's recent research programs and proceed to measure individual privacy empowerment using information sensitivity. We seek to demonstrate how the aforementioned companies can empower participants in their research programs and how such perceived empowerment can differ in both scenarios due to the differences in the data sensitivity. Due to the nature of data collected in both research programs, we tag Google's research program as a low sensitive research program and that of Facebook as a high sensitive research program.

For individuals to feel empowered in a data collection activity, they need to be duly informed of the data collection activity in a transparent manner (Van Dyke et al. 2007). This provision of adequate and transparent notice is a necessary and first prerequisite in all data collection activities without which privacy empowerment cannot be attained. Second, individuals ought to be provided with privacy options including opt-in choices, access to their collected data and other options appropriate to the data collection context. Unlike the first prerequisite, we assert that the provision of privacy options is not a necessary prerequisite for privacy empowerment. We argue that individuals can feel empowered with their privacy decisions in the absence of privacy options depending on the type of information being requested in the research program. For instance, previous studies have shown that individuals are more protective of some categories of information particularly financial data and personal identifiers but less protective of lifestyle and demographic information (Nowak and Phelps 1992; Vidmar and Flaherty 1985; Wang and Petrison 1993). Findings also indicate individuals rationally perceive sensitive information (financial data and personal identifiers) to be riskier than non-sensitive information (lifestyle and demographic) and therefore express higher privacy concerns when such sensitive information is requested (Malhotra et al. 2004). Fueled by such privacy concerns, we assert that individuals are likely to demand more privacy options for sensitive information in comparison to less sensitive information. The demand for more privacy options is supposed to serve as a self-assuring mechanism against any post-disclosure abuse. Also, we expect consumers to demand less or no privacy options for low sensitive information due to their relative lower privacy concerns and potential threats. Therefore, we postulate that individuals desire for privacy empowerment will differ per the level of their sensitivity to requested information in an e-service research program.

Weible (1993) defines information sensitivity as the level of privacy concern an individual express when a specific type of information is requested in a particular situation. In this study, we intend to differentiate information types by sensitivity level and measure how they relate to individuals' desire for privacy options in achieving privacy empowerment. This study serves to answer the research question of how individuals' desire for privacy empowerment differ per data sensitivity level. Hence, the purpose of this study is to measure individuals' privacy empowerment in an information sensitivity context under an e-service data-collection framework. In the proceeding sections, we address the concept of privacy empowerment and redefine its dimensions. The next section is devoted to discussing the related literature and the study's research design. Finally, we explain the results and its implications to theory and practice.

Research Background

Empowerment is a multi-disciplinary construct used to describe the social process through which people gain control over their lives. The construct originates from psychology and management literature (Thomas

and Velthouse 1990; Van Dyke et al. 2007) and emphasizes the delegation of control in diverse contexts. In a business context, empowerment is demonstrated in two forms: employee and consumer empowerment. Both forms share in common, the idea of delegating control from higher levels down to the individual level. Midha (2012) defines privacy empowerment as an individual's perception of the extent to which one can control the dissemination and use of personal information. Hoffman et al. (1999) asserts that consumer empowerment occurs when the balance of power is transferred from business organizations, which have traditionally held power, to consumers, who have traditionally been powerless.

Consumer privacy empowerment is relatively a new construct in IS privacy context. The construct was introduced in an e-commerce setting and operationalized by Van Dyke et al. in a 2007 study to explain its effect on consumer trust and privacy concerns. The authors found delegation of control to be fundamental to both consumer empowerment and information privacy. Other authors have also emphasized the importance of control to the concept of privacy. Fried (1984) provides such emphasis in his claim that "privacy is not simply an absence of information about us in the minds of others, rather it is the control we have over information over ourselves". Prince (2018) asserts that control over personal data flows is regarded as a central dimension to individuals' privacy. Previous studies also show that; privacy and control are complementary concepts that support each other (Van Dyke et al. 2007), consumers demand more control in situations where there are increased privacy threats (Olivero and Lunt 2004), and people desire more privacy control in scenarios where consumer data is shared with a third party (Clarke 1999). Further, Van Dyke et al. (2007) suggest that companies can enhance privacy empowerment by adopting privacy policies that relinquish control of privacy decisions to individuals. Other studies support this suggestion that privacy concern issues can be addressed if consumers are given control (Phelps 2000), allowed to opt-in to data collection and provided access to prior collected data (Midha et al. 2004). Midha (2012) later argues that, while individual privacy control has been found to be effective in literature, its application is however missing in practice. In summary, literature has found the delegation of control as an essential component in achieving consumer privacy empowerment.

Previous studies have identified three dimensions underlying individual privacy empowerment: notice, choice and access (Van Dyke et al. 2007; Prince 2018). These dimensions are directly adapted from the FTC's Fair Information Practices (FIP) which serve as guidelines for the collection of online data. The "notice" dimension urges companies to inform consumers about their information practices such as: the prior notice to collect any personal information, the nature and use of the collected information and the intent to share the collected information with third parties. The "choice" dimension advises companies to grant consumers the right to opt-in/opt-out of any secondary use and third-party data sharing. The "access" dimension recommends that companies provide reasonable access to collected information for consumers to review the information and correct any inaccuracies. The deliberate use of the verbs: urge, advise and recommend, to describe the dimensions reflects the self-regulatory nature of the online industry over issues of information collection and use. This is due to the lack of a central authority to strictly monitor and legally enforce these dimensions resulting in the lackadaisical application of privacy standards in industry. The FTC has made strides in this regard; however, we believe there is still much to be done in achieving a complete and effective oversight of privacy standards in industry.

Research Framework

This study attempts to redefine the dimensions of privacy empowerment and explore their perceived relationship in an information sensitivity context. Notice, choice and access are adapted from the FTC's data collection principles and further, redefined as informativity, optionality and controllability as in Table 1. The rationale for redefining the dimensions is to incorporate privacy design principles and strategies into the already existing FTC's dimensions. The use of design principles and strategies reflect the fundamental approach to achieve certain design goals such as enhancing the rigor and practicality of the existing dimensions. The eight "privacy design" strategies include: minimize, separate, aggregate, hide, inform, control, enforce and demonstrate (Hoepman 2014). As some of these design principles overlap with the existing FTC dimensions, this study only addresses the design strategies needed to form the proposed dimensions.

Dimensions	Definition	Reference
Informativity	The provision of transparent notices to consumers regarding the type of data being collected, reasons for the data collection and, how the data is being collected.	Van Dyke et al. (2007).
Optionality	The provision of privacy options and tools to individuals to manage the use, access and distribution of their personal information	Prince (2018)
Controllability	The extent to which individuals are satisfied with the consequences of their privacy decisions	Cho, H., Lee, J. S., and Chung, S. (2010)

Table 1. Dimensions and Definitions

To begin with, the dimension of informativity reflects the idea of transparency and is the most essential principle in the data-collection process. Informativity combines ideas from both the FTC's "notice" dimension and the "inform" design principle. Both principles suggest that individuals should be notified of a company's data collection practices including the type of data collected, data collection processes (direct or indirect means like bots and cookies), reasons for data collection, third-party sharing agreements, choice options, accessibility and security mechanisms developed to protect consumers. Thus, companies should create awareness by disclosing this information to individuals before any data collection activity. Research suggests that notice alone is never sufficient as consumers often fail to understand and process information (Howells 2005), therefore the inform design principle recommends companies to adopt user interactive design patterns (simple privacy notices with embedded text mining and classification tools) that ensure informed consent. The use of an interactive privacy design should potentially prevent any information asymmetry that might occur. Companies can enhance informativity by ensuring that individuals are well informed of data collection practices through a transparent and user interactive privacy design.

The dimension of optionality assumes that properly informed individuals should have the authority over the processing of their personal data. After informativity, individuals have the right to a clear privacy interface that allows them to make informed choices about who has access to their data and how it is used. Individuals ought to be given the options and means to control the use of their personal information after they have been informed of the data collection activity. Such options include whether to authorize the secondary use of their personal data for marketing purposes and third-party disclosure. For FTC's "choice" dimension, the means to control are often available in the form of 'opt-in' or 'opt-out'. For design principle "control", agency represents the use of design patterns to provide consumers the privacy option tools to exert their data protection rights and to decide whether to use a certain system. Privacy option tools ranges from simple consent forms to advanced privacy settings such as activity tracking and ad option settings. Van Dyke et al. (2007) asserts that the flexibility in choice-set and privacy options afforded a consumer has significant positive effect on perceived empowerment.

Finally, the dimension of controllability captures the eventual outcome of privacy empowerment. The controllability dimension describes the extent to which consumers are satisfied with the consequences of their privacy decisions. People are well positioned to make informed choices when they are properly informed and provided with suitable privacy control tools, and as such more likely to be satisfied with the outcome of their choices. The privacy calculus theory asserts that consumers tend to evaluate the risk of disclosing personal information against compensation before receiving a monetary reward from a data-collection company. This theoretical framework highlights the trade-off decisions between benefits and risks associated with information disclosure (Dinev and Hart 2006; Hoffman 2014). Companies need to adopt privacy designs that ensure high informativity and optionality to provide consumers the sense of control they desire to feel empowered. We should emphasize that this sense of empowerment and control originates from how the consumer is able to reflect his/her privacy sensitivity in the rationality of the privacy decision. Rationality is subjective and dependent on the privacy sensitivity level of the individual consumer. Prince (2018) asserts that consumers ought to integrate their privacy concern into their privacy

decision to exercise privacy controls. Therefore, we postulate that consumers are empowered when they are satisfied with the outcomes resulting from their own informed privacy decisions. As such, we develop a research model in Figure 1. We assert that, when users are given notice of data collection and provided with transparency in the data collection process (informativity), they should be satisfied with the consequences of their privacy decisions (controllability). Also, providing users with adequate notice (informativity) will encourage them to seek the necessary steps and precautions to protect their privacy interests (optionality). Further, when users are provided with adequate privacy options to take precautions and protect their privacy interests (optionality), they will be satisfied with the outcome of their privacy decisions (controllability).

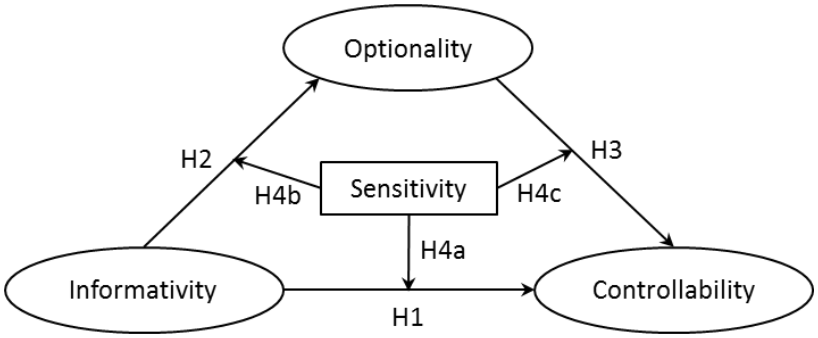

Figure 1. Research Model

The three dimensions of privacy empowerment as conceptualized are likely to comprise a mediating relationship. The direct relationship between Informativity and Controllability is captured by the first research hypothesis (H1). Their indirect relationship through the mediator of Optionality comprises the next two hypotheses (H2 and H3).

H1: Informativity has a positive effect on controllability.
H2: Informativity has a positive effect on optionality.
H3: Optionality has a positive effect on controllability.

Information sensitivity is likely to moderate the relationships between the dimensions. As information sensitivity increases in a data disclosure setting, individuals' privacy concerns are heightened due to potential privacy threats and as such they are more likely to alter their privacy behavior to match their privacy attitude. Therefore, when individuals are duly notified of the data collection activity, they are likely to demand more privacy options in a high sensitivity data context as compared to a low sensitivity data context. We argue that individuals in a low sensitivity data context can attain privacy empowerment in the absence of privacy options as a mediator. These propositions assume that individuals are rational and will therefore require that privacy options matches the level of data sensitivity requested for disclosure. Thus, we test these propositions using hypotheses H4a, H4b and H4c.

H4a: Sensitivity negatively moderates the relationship between informativity and controllability.
H4b: Sensitivity positively moderates the relationship between informativity and optionality.
H4c: Sensitivity positively moderates the relationship between optionality and controllability.

Methodology

Facebook initiated a research program where participants were offered up to $20 to download an application which allowed the company to have root network access to their mobile phones. This allowed Facebook to spy and reportedly collect sensitive data including web searches, emails, browsing activity and private messages. Google also conducted a marketing research program to collect facial scans of people to improve its facial recognition software. Participants were offered $5 gift cards and made to sign a consent form. The data collected by Facebook's research program was considered as more intrusive and sensitive than that of Google's program which was considered to be low on the data sensitivity spectrum. We

therefore assigned Facebook's research program as a high sensitivity context and Google's program as a low sensitivity context. Further, we designed a survey tool containing hypothetical scenarios of both research programs and their respective privacy statements. Respondents were made to assume that they were being asked to participate in one of the research programs. This added practical relevance and rigor to the study as participants could easily relate to the questionnaire items in a specific real world context.

To achieve our research objectives, we adopted a between-subject experimental design to measure perceived privacy empowerment in two treatment conditions; high and low sensitivity context. For the high sensitivity context, we included a hypothetical description of Facebook's research program together with a copy of their privacy statement. For the low sensitivity context, we similarly described Google's facial data collection program and attached a copy of the related privacy statement. We randomly assigned respondents to both conditions to ensure that observed differences between the groups were due to the differing conditions. Also, another reason for the randomization was to limit confounding variables such as individual differences. As such, one group of respondents was exposed to the high sensitivity condition (Facebook's research program) and the other group was also assigned to the low sensitivity condition (Google's research program).

This empirical study adopted a quantitative survey-based approach where data was collected through an online survey administered to a sample of 64 respondents. Survey respondents were randomly sampled from the academic community at a large university in Texas. All responses were usable as no missing data was reported in the dataset. 70 percent of the respondents were found to be between ages 18 to 24 while 17% fell between ages 25 to 29. The sample had 41 males (64%) and 23 females (36%) in an approximate 2:1 ratio.

The measurement scale for the three dimensions in the privacy empowerment construct was developed based on an extensive literature review (Van Dyke et. al 2007; Prince 2018). Each of the three dimensions (informativity, optionality and controllability) contained three items each. All items were assessed using a 7-point Likert scale ranging from 'strongly disagree' to 'strongly agree' with the exception of demographic questions (age, gender).

Results

We assessed the reliability and validity of measurement instruments to ensure that the constructs were accurately measured and represented. Two of the constructs, optionality and controllability were represented as reflective constructs while informativity was measured as a formative construct in the model. For the reflective constructs, both the Cronbach's alpha and composite reliability were above 0.7 indicating internal consistency reliability (Hair et al. 2006). Also, the path loadings and average variance extracted (AVE) for the reflective indicators were above .70 and .50 respectively providing evidence of their convergent validity (Hair et al. 2006). Further, we found the heterotrait-monotrait (HTMT) ratio to be below 0.9 establishing discriminant validity (Henseler et al. 2015) proving that the constructs indeed measured what they were intended to measure. For the formative construct, controllability, we assessed content validity through extensive literature review (Van Dyke et. al 2007; Prince 2018). As shown in table 2 below, there were no problems with multicollinearity as the variance inflation factors (VIFs) were less than 5 (Hair et al. 2006).

Statistic	Informativity	Optionality	Controllability
Cronbach's Alpha		0.927	0.934
Composite Reliability		0.954	0.958
Average Variance Extracted		0.873	0.883
rho_A		0.928	0.941
HTMT		0.708	
VIF's	2.591	3.126	4.367

	2.24 2.909	4.449 3.856	3.776 3.763

Table 2. Reliability and Validity Statistics

The model was estimated with partial least squares (PLS) due to the presence of one formative latent variable (i.e. Informativity) along with two reflective ones (i.e., Optionality and Controllability). We checked for the model's predictive accuracy by assessing the adjusted coefficient of determination (R^2) for the two endogenous constructs, optionality and controllability. The adjusted R^2 for optionality (0.569) and controllability (0.478) signaled that the model had a moderate level of predictive accuracy. Further, we interpreted that approximately 48% of the variance in controllability was explained by the model. The R^2 values of the two endogenous were statistically significant. All the path coefficients were significant which provided support for the predicted relationships between the constructs. All the fit indexes were satisfactorily within the accepted thresholds. The path coefficients and p-values provided significant support for hypotheses 1,2 and 3 proving that informativity had positive effects on both optionality (H1) and controllability (H2) while optionality had a positive effect on controllability (H3). As such, the model predicts that individuals are more likely to feel empowered when they are provided with adequate notice of data collection and adequate privacy options.

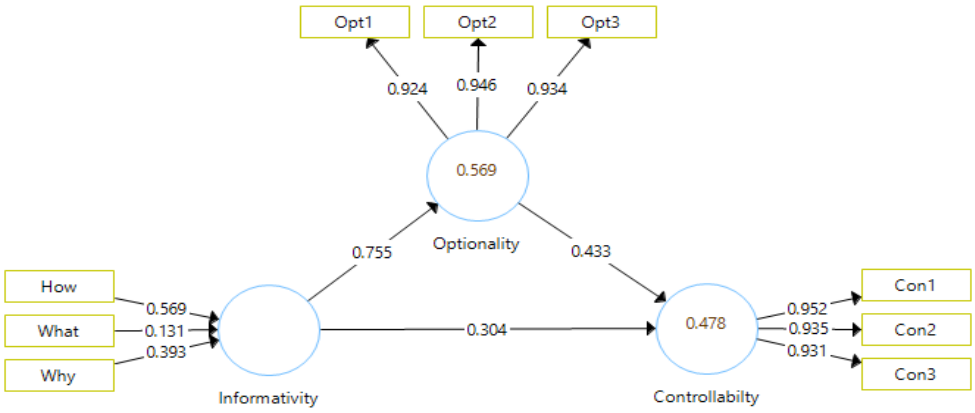

Figure 2. Results of Model Estimation

Since the model passed both significance and good fit test, we conducted a multigroup analysis to determine the effect of the condition treatments (low and high sensitivity groups) on the relationships between the endogenous variables in the inner model. As indicated in Table 3 below, we found that the path coefficient between informativity and controllability was positively significant for the low sensitivity group indicating. However, the path coefficient between optionality and controllability was not statistically significant. This indicates that optionality has no mediation effect on the relationship between informativity and controllability in the low sensitive context. The path coefficient from informativity to controllability was found to be statistically insignificant for the high sensitivity group. All other path coefficients were significant. We found optionality to be a full mediator between informativity and controllability in the high sensitivity context.

	Low Sensitivity Group		High Sensitivity Group	
	Path Coefficients	p-values	Path Coefficients	p-values
Informativity -> Controllability	0.47	0.036	0.337	0.087
Informativity -> Optionality	0.618	0	0.794	0

Optionality -> Controllability	0.273	0.164	0.433	0.022

Table 3. Group Path Coefficients and P-values

The results show that sensitivity negatively affects the relationship between informativity and controllability providing support for hypothesis 4a. At a lower sensitivity level, respondents strongly depend on informativity to achieve controllability. However, at a higher sensitivity level, respondents rather depend on optionality as a mediator to attain controllability. This shows that, an increase in data sensitivity level leads to the decrease in the direct effect between informativity and controllability as evidenced by the path coefficients and p-values in table 2 above. Also, the results provide support for hypothesis 4b and 4c. Path-coefficients in the high sensitivity group relating to both informativity-optionality (H4b) and optionality-controllability (H4c) are higher than those in the low sensitivity group. This indicates that sensitivity positively moderates the relationship between informativity-optionality (H4b) and optionality-controllability (H4c).

Discussions

In this study, we demonstrated how e-service companies can empower individuals to participate in their research programs and how such perceived empowerment can differ in different scenarios of data sensitivity. Findings from the multigroup analysis indicated that individuals' desire for privacy options differed per level of information sensitivity. To feel empowered when making privacy decisions, individuals desired higher forms of privacy options for more sensitive data and no forms of privacy options for less sensitive data. We found that respondents in the high sensitivity group (Facebook) felt empowered making information disclosure decisions under two conditions: informed notice (informativity) and presence of privacy control options (optionality). For the low sensitivity group (Google), respondents felt empowered from the sole provision of informed notice and did not require privacy options as a mediator. One reason for this behavior is because of the higher privacy concerns associated with highly sensitive data (Malhotra et al. 2004). Since previous studies indicate that a decrease in privacy concern levels has a positive effect on privacy empowerment (Van Dyke et al. 2007), we assert that the desire for privacy options in the high sensitivity group could possibly be a precautionary mechanism for individuals to offset their privacy concerns and subsequently, increase their perceived sense of privacy empowerment.

This study has found that informed notice and transparent (informativity) is very crucial at all levels of data sensitivity. As such, e-service companies can empower individuals through the use of transparent privacy design principles. To begin with, e-service companies ought to abolish the use of traditional legal jargons in privacy notices and provide simplified privacy notices with non-legal grammar to participants of research programs. Other studies have suggested highlighting potential sections of interest for users (Wardell et al. 2016; Good et al. 2005) by embedding text mining and classification tools in privacy notices. For instance, typical sections of interest that can be highlighted include secondary use of data, backdoor access, third party sharing, marketing intentions among others. Participants can then be presented with all the possible ways data abuse can occur and as such, enhance their ability to properly evaluate the potential benefits and risks (Midha, 2012) associated with their participation. Further, participants should not have to search for privacy notices, rather websites and applications should be designed to nudge them to these simplified privacy notices before they are asked to disclose any form of information. Also, companies need to experiment and implement more flexible forms of privacy options and avoid the one-fits-all approach that has become the norm. We believe these actions are likely to trigger participants to make informed privacy decisions leading to a more stable perception of privacy empowerment.

E-service companies seeking to persuade individuals to disclose their personal data in research programs should focus on changing consumers attitude to data collection. This involves designing research and data collection programs to include both informed notices (informativity) and adequate privacy options (optionality) regardless of data sensitivity levels. This way firms can ensure that individuals achieve a more stable and favorable perception of data collection activities. Therefore, e-service giants like Google and Facebook need to adopt policies that delegate privacy control decisions to individuals and also communicate such policies in a transparent manner so as to build a stable sense of empowerment (Van Dyke et al. 2007).

Companies have to be transparent and truthful about their research programs and ensure that individuals explicitly understand the kind of data they are disclosing, available privacy options and other related privacy implications. These actions could help reduce, if possible eliminate, the continuous backlash they receive over their privacy policies and research activities. Also, privacy empowerment has a positive influence on trust (Prince 2018) and empowering individuals will allow companies build lasting relationships with individuals and enjoy a favorable public image.

Conclusion

The demand for consumer data is gradually evolving into a full-fledged labor market. There exists some sort of control inequality between e-service companies and customers which can be bridged by individual privacy empowerment. The time has come for companies to concentrate on empowering individuals to generate a more stable and positive attitude to research and data collection activities. We have also found that the provision of privacy options is very essential to achieving individual privacy empowerment particularly in a highly sensitive data context. Therefore, relying solely on monetary rewards to stimulate information disclosure might not be a viable venture for e-service companies. Rather, companies should integrate informativity and optionality into their privacy designs during research and data collection activities to provide consumers with a perceived sense of empowerment and control over their private data.

Respondents used for the study were mainly from the university community. This provides limitation on the extent to which the results can be generalized to the general population. However, we plan to conduct a second data-collection activity to include working professionals in the study. We expect this activity to increase the sample size and also, enhance the validity and generalizability of the study. Also, this study did not measure actual privacy empowerment but rather individual's perceived privacy empowerment. While Van Dyke et al. (2007) asserts that it is logical to assume the relationship between actual and perceived privacy empowerment, we encourage future studies to look into this relationship for possible discrepancies between actual and perceived privacy empowerment.

REFERENCES

Acquisti, A. and Grossklags, J. 2005. "Privacy and Rationality in Individual Decision Making," IEEE Security and Privacy, IEEE Computer Society, Vol. 3, No. 1, January/February 2005, pp. 26-33

Andrade, E. B., Kaltcheva, V., and Weitz, B. 2002. "Self-Disclosure on the Web: The Impact of Privacy Policy, Reward, and Brand Reputation," in Advances in Consumer Research, S.M. Broniarczyk and K. Nakamoto (eds.), Valdosta, GA: Association for Consumer Research, pp. 350-353.

Bruce, J. 2005. "Defining Rules for Acceptable Adware", in the Proceedings of the Fifteenth Virus Bulletin Conference, Dublin, Ireland.

Caudill, E.M. and Murphy, P.E. 2000, "Consumer online privacy: legal and ethical issues", Journal of Public Policy and Marketing, Vol. 19, pp. 7-19.

Cespedes, F. V., and Smith, H. J. 1993. "Database Marketing: New Rules for Policy and Practice," Sloan Management Review (34:4), pp. 7-22.

Cho, H., Lee, J. S., and Chung, S. 2010. "Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience." Computers in Human Behavior, 26(5), 987-995.

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

Eastlick, M. A., Lotz, S. L., and Warrington, P. 2006. "Understanding Online B-to-C Relationships: An Integrated Model of Privacy Concerns, Trust, and Commitment," Journal of Business Research (59:8), pp. 877-886.

Gomez, J., Pinnick, T., and Soltani, A. 2009. "KnowPrivacy: The Current State of Web Privacy, Data Collection, and Information Sharing," School of Information, University of California Berkeley (http://www.knowprivacy.org/).

Good, N., Dhamija, R., Grossklags, J., Thaw, D., Aronowitz, S., Mulligan, D., and Konstan, J. 2005. "Stopping spyware at the gate: a user study of privacy, notice and spyware." In Proceedings of the 2005 symposium on Usable privacy and security (pp. 43-52). ACM.

Hwansoo L., Dongwon L., Hyerin K., Hangjung Z. and Andrew P. C. 2015. "Compensation paradox: the influence of monetary rewards on user behavior," Behavior and Information Technology, 34:1, 45-56, DOI: 10.1080/0144929X.2013.805244

Hoepman, J. H. (2014, June). "Privacy design strategies." In IFIP International Information Security Conference (pp. 446-459). Springer, Berlin, Heidelberg.

Isin, E., and Ruppert, E. 2015. "Being digital citizens." Rowman and Littlefield International.

Jensen, C. and Potts, C. 2004 "Privacy policies as decision-making tools: an evaluation of online privacy notices", in: Proceedings of ACM CHI 2004, Vienna, Austria, pages 471-478.

Lanier, J., and Weyl, E. G. 2018. "A Blueprint for a Better Digital Society." Harvard Business Review.

Malhotra, N.K., Kim, S.S., and Agarwal, J. 2004. "Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model." Information Systems Research, 15 (4), 336–355.

Milne, G. R., Rohm, A., and Boza, M.-E. 1999. "Trust Has to Be Earned," in Frontiers of Direct Marketing, J. Phelps (ed.), New York: Direct Marketing Educational Foundation, pp. 31-41.

Nowak, G. J., and Phelps, J. 1995. "Direct Marketing and the Use of Individual-Level Consumer Information: Determining How and When 'Privacy' Matters," Journal of Direct Marketing (9:3),pp. 46-60.

Oliveira, T., Alhinho, M., Rita, P., and Dhillon, G. 2017. "Modelling and testing consumer trust dimensions in e-commerce." Computers in Human Behavior, 71, 153-164.

PC Pitstop 2005. "It pays to read EULAs." Available at http://www.pcpitstop.com/spycheck/eula.asp (last accessed May 24, 2005)

Phelps, J., Nowak, G., and Ferrell, E. 2000. "Privacy concerns and consumer willingness to provide personal information." Journal of Public Policy and Marketing, 19 (1), 27–41.

Phelps, J.E., D'Souza, G. and Nowak, G.J. 2001. "Antecedents and consequences of consumer privacy concerns: an empirical investigation", Journal of Interactive Marketing, Vol. 15 No. 4, pp. 2-17.

Prince, C. 2018. "Do consumers want to control their personal data? Empirical evidence." International Journal of Human-Computer Studies, 110, pp.21-32.

Shklovski, I., Mainwaring, S., Skúladóttir, H., and Borgthorsson, H. 2014. "Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use Mobile." Conference on Human Factors in Computing Systems - Proceedings. 10.1145/2556288.2557421.

Sipior J. C. 2005. "A United States Perspective on the Ethical and Legal Issues of Spyware", in Proceedings of Seventh International Conference on Electronic Commerce, Xi'an China.

Smith, H., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review." MIS Quarterly, 35(4), 989-1015. doi:10.2307/41409970

Hann, I.H., et al. 2007. "Overcoming online information privacy concerns: an information-processing theory approach." Journal of Management Information Systems, 24 (2), 13–42.

Stone, E.F., et al. 1983. "A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations." Journal of Applied Psychology, 68 (3), 459–468.

Waddell, T. F., Auriemma, J. R., and Sundar, S. S. 2016. "Make it simple, or force users to read:? Paraphrased design improves comprehension of end user license agreements." In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (pp. 5252-5256). ACM.

Weible, R.J. 1993. "Privacy and Data" (Doctoral dissertation, doctoral dissertation, Mississipi State Univ).

Van Dyke, T. P., Midha, V., and Nemati, H. 2007. "The effect of consumer privacy empowerment on trust and privacy concerns in e-commerce." Electronic Markets, 17(1), 68-81.

Xie, E., Teo, H.H. and Wan, W. 2006. "Volunteering personal information on the internet: Effects of reputation, privacy notices, and rewards on online consumer behavior." Marketing letters, 17(1), pp.61-74.

Xu, H., Teo, H. H., and Tan, B. C. Y. 2005. "Predicting the Adoption of Location-Based Services: The Roles of Trust and Privacy Risk," in Proceedings of 26th International Conference on Information Systems, D. Avison, D. Galletta, and J. I. DeGross (eds.), Las Vegas, NV, December 11-14, pp. 897-910.

Xu, H., Teo, H. H., Tan, B. C. Y., and Agarwal, R. 2010. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services," Journal of Management Information Systems (26:3), pp. 137-176.