2021

Individual Privacy Empowerment: Exploring the Trade-Offs Between Information Sensitivity and Compensation

Bright Frimpong
The University of Texas Rio Grande Valley

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

Recommended Citation

Frimpong, B. and Sun, J. (no date) 'Individual Privacy Empowerment: Exploring the Trade-Offs Between Information Sensitivity and Compensation', in Proceedings of the 54th Hawaii International Conference on System Sciences 2021. Hawaii International Conference on System Sciences 2021, pp. 4623–4631.

Individual Privacy Empowerment: Exploring the Trade-Offs Between Information Sensitivity and Compensation

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

*To provide personalized services and remain competitive, many online companies depend on individual disclosure of personal information. An emerging common theme, in the quest for privacy solutions, is the idea to empower individuals to control the management of their personal information. This study proposes a third-option design that seeks to empower users when signing up for an online service. We also measure individual privacy empowerment in a 2*2 experimental design study (reward/utility-limit mechanism to high/low sensitivity information context) using the proposed third-option design. Results from the multigroup analysis indicate that respondents prefer a reward mechanism over a utility-limit mechanism when asked to disclose less sensitive data. However, the utility-limit mechanism is preferred in the highly sensitive group indicating that a simple linear relationship does not exist between monetary rewards and information sensitivity. Theoretical and practical implications are discussed.*

1. Introduction

Touted as the currency of the information economy, data has become an increasingly valuable commodity in the big data era. To provide personalized services and remain competitive, many online companies depend on the individual disclosure of personal information. Companies often rely on self-disclosure mechanisms like site registrations and opt-in forms to collect demographic and other types of personal data. However, self-disclosure is a misnomer as a lot of companies have developed sophisticated monitoring systems and data mining tools to discreetly gather personal information without individual consent. Companies have been found to use clickstream tools, cookies and tracking software to unobtrusively collect individual private data. This apparent lack of transparency behind data collection and mining practices constitutes an abuse of individual privacy rights.

Since the dawn of the Internet, information privacy has progressively become an important issue to individuals, companies, policy advocates and government regulatory bodies. The primary objective of privacy researchers and regulatory bodies is to develop the perfect blend of privacy tools and legal frameworks to concurrently protect individual privacy rights and facilitate data collection. Over the years, several privacy tools have been developed and implemented to help protect online consumer privacy. One of such tools is the privacy seal program which has been developed to help consumers identify websites that follow a basic set of privacy rules. Similar tools, TRUSTe and P3P, also provide seals to websites that follow strict privacy policies set by the Online Privacy Alliance (OPA). These tools provide assurances to customers that websites with seals abide by codes of online information practices and promote fair information collection. However, their impact in curbing online data abuse have been abysmal due to their lack of uniformity. Also, it has not been practically feasible for these seal programs to monitor all the websites on the internet and as such, consumers who choose to use only seal approved websites will be limited to a much restricted number of websites to access.

Over the years, researchers and privacy advocates have continued the debate and search for practical yet effective solutions to information privacy rights abuse. An emerging common theme, in the quest for privacy solutions, is the idea to empower individuals to control the management of their personal information. Consumer empowerment is attained by providing customers the privacy control options and rights to control the nature and content of data collected about them. Recent studies have defined and operationalized individual privacy empowerment [1-2]. These studies have also identified several dimensions that seek to measure individual privacy empowerment and further evaluated the impact it has on other privacy constructs like trust and privacy concern [1]. To comprehend and

URI: https://hdl.handle.net/10125/71178
978-0-9981331-4-0

Table 1- Definitions of Terms

Terms and Dimensions	Definition
Third-option design	a sign-up template where users are provided with a partial consent option regarding the sale of the personal data to third parties
Information sensitivity	the level of privacy concern an individual show when asked to disclose information in a specific situation
Reward/utility-limit mechanism	for full consent- the reward mechanism promises participants a one-time $20 gift card while the utility-limit mechanism only grants them full access to the online service for partial consent (declining the collection and use of secondary data)- the reward mechanism provides full access to the service but no gift card while the utility-limit mechanism provides access to a limited functional version of the online service
Privacy Empowerment	providing consumers with the privacy control options and rights to control the nature and content of data collected about them
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.
Optionality	the provision of privacy options and tools to individuals to manage the use, access and distribution of their personal information
Controllability	the extent to which individuals are satisfied with the consequences of their privacy decisions

advocate for individual privacy empowerment, we argue the need for continuous in-depth experimental studies to analyze the trade-offs between information disclosure, compensation and data control. Adopting previously defined dimensions, we intend to measure individual privacy empowerment in a 2*2 experimental design study (reward/utility-limit mechanism to high/low sensitivity information context) using a third-option online sign-up design.
The use of the reward and utility-limit mechanism is based on previous studies which have found compensation rewards as a primary influencer of information disclosure[3-4].

The purpose of this study is to determine the impact of rewards and utility-limit on individual privacy empowerment in an information sensitivity context when signing up for an online service. In the next section, we discuss the underpinning theories of this study, proceeded by the conceptual framework and research design. The other half of the paper is devoted to the discussion of results and contribution of the study to both literature and practice.

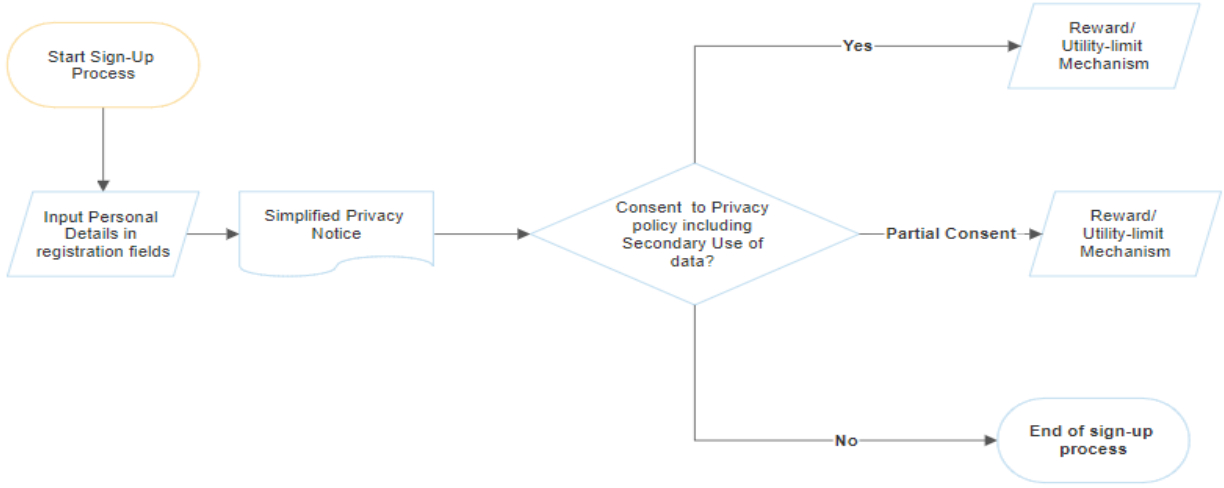
2. Information Sensitivity and Disclosure

Information sensitivity is the level of privacy concern an individual show when asked to disclose information in a specific situation [5]. Request for highly sensitive information has been found to be positively correlated with privacy concern. This is because people perceive disclosure of sensitive information to be riskier than non-sensitive information [6]. Several psychological theories have been adapted to explain how individual behavior influences information disclosure. One of such theories is the theory of procedural justice which posits that individuals are more likely to disclose personal data for organizational use when they perceive that fair procedures have been implemented to protect their individual privacy. Also, the social response theory asserts that an individual will voluntarily disclose their personal information in response to a similar disclosure from another individual or organization. The theory further describes the need for companies to build reciprocal relationships with their customers to enhance voluntary information disclosure. Li suggests that companies can start with the exchange of less sensitive data and subsequently, increase the level of sensitivity depending on the intimacy of the relationship [7]. The reciprocity theory, much similar to the social response theory, also explains "the willingness of individuals to match the level of intimacy in the disclosure they return with the level of intimacy in the disclosure they receive"[8]. Individuals often desire to exhibit fairness in their transactions with third-parties but also will not hesitate to retaliate or reward third-party behavior when considered appropriate [9]. For instance,

interviewers are likely to receive more responses from surveys with attached monetary rewards than from surveys with no attached monetary rewards. Also, websites that request for registration (demographic data) even before providing any service are less likely to receive much data and even if they do, may receive falsified and inaccurate data.

The privacy calculus theory asserts that an individual's intention to disclose personal information is dependent on some form of risk-benefit analysis. According to the risk-benefit or utility theory, information disclosure is primarily influenced by monetary reward [10]. Culnan and Armstrong found that individuals expect economic value or benefits at the expense of surrendering control of their personal data [11]. Further, recent studies show that users are often willing to trade off their privacy for both financial and non-financial rewards [12,4,6].

Figure 1. The third-option design



Empirical evidence from these studies reveal that consumers are more likely to accept cash considerations or free complete software package benefits in exchange for their information. Interestingly, a couple of researchers and policy analysts have raised issues that involve treating consumer data as labor worthy of compensation [13]. The debate seems to have shifted from privacy awareness to user compensation for data. Research shows that online consumers have been denied the opportunity to share in the wealth created by their personal data which is valued around 156 billion dollars annually [14]. To achieve individual privacy empowerment, we argue the need for continuous in-depth experimental studies to analyze the trade-offs between information disclosure, compensation and data control.

3. Privacy Empowerment

To empower is to grant an individual the power, right or authority to perform various acts or duties [15]. The central theme of empowerment is the delegation of control. Alshibly and Chiong asserts that empowerment is related to control while Hoffman et al. defines consumer empowerment as "shifting the balance of power from service providers, who have traditionally held power, to the consumers who have traditionally been powerless" [16, 17]. Consumer empowerment is attained by providing customers the privacy control options and rights to control the nature and content of data collected about them. Van Dyke et al. identified three dimensions: notice, choice and access which sought to measure individual privacy empowerment in an e-commerce context [1]. Frimpong and Sun further incorporated privacy design principles and redefined these dimensions (notice as informativity, choice as optionality and access as controllability) to measure individual privacy empowerment in an information sensitivity context [2].

Hoepman argues that "the natural starting point to derive privacy preserving strategies is to look at when and how privacy is violated, and then consider how these violations can be prevented" [18]. Research shows that privacy violations often occur during software installation processes and online service sign-ups [19-21]. In line with Hoepman's argument and previous literature, we illustrate (using a sign-up template in figure 1) how privacy design tools and behavioral theories can be adopted and implemented to empower individuals against online privacy violations. The rationale behind the use of an online sign-up template is to demonstrate how individuals can be empowered to act autonomously and control

the use and sharing of their data in a single consent decision. In the proceeding section, we illustrate the proposed sign-up process (third-option design) of an online service under the framework of privacy empowerment dimensions: informativity, optionality and controllability.

3.1 Informativity

Companies spell out the kind of information they are going to collect from users in privacy notices and end-user license agreements (EULA's). These privacy notices and EULA's outline the contractual obligations and rights between the service provider and individual user. However, multiple surveys and research reveal that most people have limited understanding of privacy notices and even if they do, possess little to no desire to read such lengthy notices [19-21]. Research shows that these notices are written "by lawyers for lawyers" due to the complexity of the legal jargons and length of clauses which severely limit user's ability to understand and make informed decisions [19-21]. For instance, a software provider included a $1,000 cash prize offer in the company's privacy statement which was displayed during the installation process. Interestingly, the prize was only claimed after the software had been installed over 3,000 times in 4 months [22]. This provides evidence that most people simply ignore these privacy notices and as such have no idea what they consent to when they choose to use the provided service. Privacy notices therefore becomes a conduit for online companies and service providers to violate individual privacy rights.

Informativity is the most essential principle and first step in the process of empowering users to take control of their data management. This dimension provides guidelines to ensure transparency in the data-collection process. It states that companies need to ensure that their privacy documents are worded with everyday simple language and provides answers to questions like how, why and what information are expected to be collected from individuals. Companies need to ensure they adopt interactive privacy designs that make it easier for individuals to read and understand privacy notices in a shorter time frame. These should enable users make rational privacy decisions that reflect their level of privacy sensitivity and concern. This presents a win-win situation for both firms and most particularly, consumers since privacy policies are clearly communicated and as such are able to make properly informed decisions. Users can then make informed decisions whether to sign-up for or decline the use of online services.

As such we hypothesize that the use of a simplified privacy notice in the third-option design has a significant effect on informativity.

Hypothesis 1: The third-option design has a significant effect on informativity.

3.2 Optionality

Easy interpretation and comprehension of privacy notices do not necessarily lead to informed decisions if users are being limited to two forced options in existing mandated disclosure forms. In a sense, this design flaw negates all the advancements that have been made to try and make it easier for users to read and understand such complex privacy notices. Individuals are expected to make informed decisions as to which software packages and online services to use based on their privacy concerns [23]. However, current EULA and privacy notices employ a forced consent design where individuals are provided with only two options when signing up for an online service or downloading a software package. The mandatory disclosure design presents the user with "Yes, I agree" and "No, I do not agree" options and as such do not offer any motivation for users to read or pay attention to the EULA and privacy notices [19]. Even when motivated, privacy conscious users who are most likely to pay attention or read such notices are unable to do so. According to the privacy calculus theory, individuals often compare the utility benefits of the online service to the possible negative consequences of signing up for online services. Therefore, they are most likely to sign up for such services if the positives outweigh the negatives, a situation which most often is the case. In the situation where users might not agree with the privacy notice or remain uncomfortable with the monitoring and data collection practices of the company, the only option available to such users is to decline the terms of the privacy notices which means they cannot use said software or online service.

After informativity, there is the need to provide users the options and means to control the use of their personal information after they have been informed of the data collection activity. In this instance, the optionality dimension posits that individuals should be able to control the collection and use of secondary data (data not required for the primary function of the service but more so for marketing and third-party sharing purposes). We argue that sign-up templates ought to be designed to allow users decide the type and sensitivity level of data they are willing to share. For instance, companies can then classify their data collection into two types: primary data (for registration

purposes and service functionality) and secondary data which is mostly for marketing and third-party sharing purposes. Users can then partially consent to either one or both of the requested data types depending on their privacy sensitivity level and still have access to the service. This represents a shift from 'the one size fits all' privacy approach where users have to consent to the entire privacy notice to have access to the service. Therefore, we postulate that the provision of a partial consent (a granular form of privacy consent) in the third-option design has a significant effect on optionality.

Hypothesis 2: The third-option design has a significant effect on optionality.

3.3 Controllability

Research findings also reveal that users are likely to trade off their information privacy for monetary rewards or full product features [12,4,6]. Therefore, users who clearly agree that their information should be collected and shared should receive some form of compensation or perhaps a share of the economic value generated from their data [9]. Arguments have been advanced that such compensation framework ought to be designed and introduced in privacy notices [13]. As previously stated, current privacy notices are regulated by the mandated disclosure law which offers only two options and as such users can only decline or agree to privacy notices. This forced consent design do not offer any motivation for users to read or pay attention to the EULA and privacy notices since there is no real incentive in doing so [24]. To achieve individual privacy empowerment, there is the need to design a new sign-up template that introduces "a trade-off option" in the sign up process providing users the option to decide if they want companies to collect secondary information and if so, their deserving compensation. We argue that this mechanism should not be an afterthought but rather a default privacy principle embedded in the sign-up process.

The controllability dimension describes the extent to which individuals feel satisfied with the outcomes 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. Companies need to adopt privacy designs that ensure high informativity and optionality to provide consumers the sense of control they desire to feel empowered. The third-option design is guided by two design principles based on the theory of reciprocity and rational choice. The first principle assumes that individuals will prefer a reward mechanism when asked to disclose less sensitive information. Also, the second principle asserts that individuals will prefer a utility-limit mechanism when asked to disclose highly sensitive information. We elaborate more on both mechanisms in the next section. Overall, we argue that the proposed design mechanism should have significant impact on controllability together with informativity and optionality.

Hypothesis 3: The third-option design have a significant effect on controllability.

4. Methodology

4.1 Research Design

An experimental survey was conducted to measure privacy empowerment using a 2x2 factorial design where two levels of information sensitivity were paired with a reward and utility-limit mechanism. To ensure novelty and practicality, respondents were provided the context of signing-up for a hypothetical online dating service (LetsHang.com). A survey tool was designed to imitate the sign-up template described in the previous section. Four different versions of the tool were developed to reflect the 4 dimensions in Figure 2 below.

	REWARD MECHANSIM	UTILITY-LIMIT MECHANISM
HIGHLY SENSITIVE DATA	Required Information: Basic Demographic data Location and Activity data Yes – *A one-time $20 gift card* Partial Consent - *No gift card but full access to the service*	Required Information: Basic Demographic data Location and Activity data Yes – *Full Access to Online Service* Partial Consent –*Access to Online Service with Limited Functionality*
LOW SENSITIVE DATA	Basic Demographic data Yes – *A one-time $20 gift card* Partial Consent - *No gift card but full access to the service*	Basic Demographic data Yes – *Full Access to Online Service* Partial Consent –*Access to Online Service with Limited Functionality*

Survey tool 1 and 2 both included low sensitive information, however, both tools were assigned different mechanisms (reward or utility-limit). The same procedure was repeated for survey tool 3 and 4 using highly sensitive information. The reward mechanism promised participants a one-time $20 gift card for full consent while the utility-limit mechanism only granted them full access to the online service. For partial consent (declining the collection and use of secondary data), the reward mechanism provided full

access to the service but no gift card while the utility-limit mechanism provided access to a limited functional version of the online service. An initial pilot study was conducted among a section of graduate students to check for measurement errors. After which, corrected versions of the survey tools were made available online to the respondents.

The sample was divided into two groups: high and low sensitivity context. To achieve our research objectives, a within-subject experimental design was used to measure perceived privacy empowerment under two treatment mechanisms: reward and utility-limit. Respondents in both groups (high and low sensitivity) were exposed to the two treatment mechanisms (reward and utility-limit). The within-subject design is appropriate for relatively small sample sizes and also ensures that, individual differences do not distort the results since each respondent serve as his/her own baseline.

4.2 Sample and Measures

This study adopted a quantitative online survey-based approach with a sample of 73 respondents. Survey respondents were randomly sampled from the student population at a large university in Texas. There were 146 usable responses (due to the within-subject experimental design) and no reported missing data in the dataset. The sample comprised 34 males (46%) and 39 females (54%). More than half of the respondents (63%) were found to be between ages 18 to 24 while 17% fell between ages 25 to 29. The measurement scale for the three dimensions in the privacy empowerment construct was developed based on an extensive literature review [1,2,25]. 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).

5. Results

The model was estimated using Smart PLS statistical software due to the presence of both reflective and formative scales. We assessed the reliability and validity of the construct measures to ensure that the constructs were accurately measured and represented.

Figure 3. Estimated Model

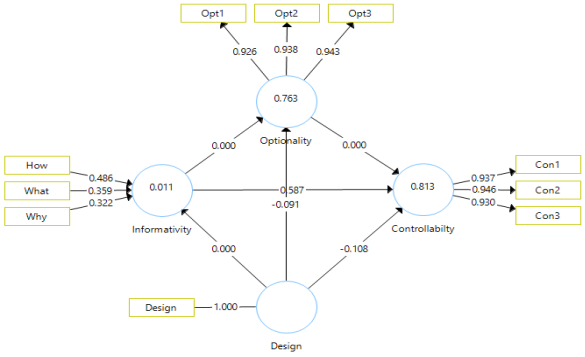


Table 2. PLS Reliability and Validity Statistics

Statistic	Design	Informativity	Optionality	Controllability
Cronbach's Alpha	1.000		0.929	0.931
Composite Reliability	1.000		0.955	0.956
Average Variance Extracted	1.000		0.875	0.879
HTMT			0.145	0.127
VIF's	1.000	1.994 1.882 1.582	3.298 3.866 4.139	3.744 4.283 3.552

Table 3. PLS Model Fit

	Saturated Model	Estimated Model
SRMR	0.029	0.029
d_ULS	0.047	0.047
d_G	0.110	0.110
Chi-Square	93.778	93.778
rms Theta	0.233	
NFI	0.930	0.930

The figures shown in Tables 2,3 and 4 are estimated using the Smart PLS software. As the estimated model in Figure 3 shows, the factor loadings of reflective constructs (i.e., Optionality and Controllability) were pretty high (above 0.9), supporting reliability and convergent validity. Meanwhile, the formative construct of Informativity comprised three components that exhibited different weights. In addition, we checked for the model's predictive accuracy by assessing the coefficient of determination. The R^2 for the two endogenous constructs, optionality (0.763) and controllability (0.813), signaled that the model explained the majority of their variance. in particular, over 80% of the variance in controllability

was explained. All the fit indexes were satisfactorily within the accepted thresholds (Appendix -table 3).

With the confidence in the model, we conducted a multigroup analysis to determine the effect of the mechanisms (rewards and utility-limit) on individual privacy empowerment among the two groups (high and low sensitivity). From Table 4, we found that the design has a significant effect on informativity in both groups indicating support for hypothesis 1. For hypothesis 2, the design has a significant effect on optionality in the low sensitivity group but not in the high sensitivity group. This implies that hypothesis 2 is confirmed in the low sensitivity group but not in the high sensitivity group. Further, we found that hypothesis 3 was only supported in the high sensitivity group.

Table 4. Multi-group Analysis

	Low Sensitivity Group		**High Sensitivity Group**	
	Path Coefficient	p-value	Path Coefficient	p-value
Design -> Informativity	0.586	0.000	-0.712	0.000
Design -> Optionality	0.156	0.020	-0.094	0.115
Design -> Controllability	0.072	0.202	-0.124	0.032

Also, the results in Table 4 provide support for the previously discussed design principles. The multigroup analysis indicates that the low sensitivity group preferred the reward mechanism to feel empowered. The high sensitivity group rather preferred the utility-limit mechanism to feel empowered. For the low sensitivity group, the third-option design has significant effect on both informativity and optionality but not controllability. This means that participants in the low sensitivity group depend on optionality to act as a full mediator to feel empowered. However, this is not the case in the high sensitivity group as optionality is not significant as a mediator.

6. Discussions

When requesting information from individuals, companies can enhance privacy empowerment by providing adequate notice of data collection and suitable privacy control options. Van Dyke et al. asserts "that the provision of adequate notice is empowering because it allows individuals to protect their own interests and make decisions based on informed consent" [1]. We found the use of a simplified privacy notice in the third-option design to be adequate enough to satisfy informativity so far as individuals were informed of the type of data to be collected, the data collection methods and the reasons for the data-collection. Moreover, simplifying the notice in the design made it easier for respondents to understand and process, thereby ensuring that subsequent individual disclosure decisions were based on a genuine informed consent. Further, the design had a significant effect on optionality indicating that respondents preferred the additional "third choice option". Previous literature posits that perceived empowerment can be achieved through the flexibility in defining one's data control choices and as such individuals ought to be provided with data control choices reflecting both primary use (needed to provide the service) and secondary uses such as marketing and third-party disclosure [1,25]. The third option design increases individuals' flexibility since it allows them to control the primary and secondary use of their personal data in a single consent decision. The partial consent in the design allows individuals to consent to the primary use of their data for service personalization while forbidding any further secondary use which is in stark contrast to the existing mandated disclosure design. The design also has significant effect on controllability and accounts for 81% of the variation in controllability. Therefore, the respondents perceive that the design include fair and transparent procedures to protect their privacy. Other than justifying the procedural justice theory, the result also implies that respondents were strongly satisfied with their individual disclosure decisions. Previous research indicates that consumers attain privacy empowerment when they are satisfied with the outcomes resulting from their privacy decisions [2].

Results from the multigroup analysis indicates that respondents prefer the reward mechanism over the utility-limit mechanism when asked to disclose less sensitive data. Individuals expect reciprocity in their relationship with companies and as such conduct a cost-benefit analysis to determine the fairness of any exchange they partake. In this instance, the respondents perceive the low sensitive data to be less risky and as such consider the $20 gift card to be a fair return for any potential disclosure cost. Therefore, we interpret that individuals are more likely to be satisfied with the outcome of their privacy decisions when companies attach monetary rewards when requesting low sensitive data.

However, the utility-limit mechanism is preferred in the highly sensitive group indicating that a simple linear relationship does not exist between monetary rewards and information sensitivity. In this instance, respondents perceive the highly sensitive data to be very risky and as such do not consider the $20 gift as

a fair return in the exchange. However, they are rather satisfied with the utility-limit mechanism which offers full access to the dating service. Faja found that individual privacy concern increases when consumers are asked to disclose highly sensitive information for financial rewards than for other benefits [26]. We offer two possible explanations for this phenomenon. Respondents might have subjectively valued the full service access to be higher than the $20 gift card and therefore perceive the offer as a fair return for any potential disclosure risk. This rationale is supported by Hwansoo et al. who asserts that "individuals perceive monetary rewards as decoys and as such request for sensitive data increases their uneasiness and raises doubts about the motives behind monetary reward offers" [12]. Also, due to the fair and transparent procedures in the design, respondents might have felt more comfortable and less concerned exchanging their sensitive information for the service than the monetary reward. This action confirms the reciprocity theory's assertion that individuals are likely to reciprocate appropriate behavior (fair procedures in the design) with a reward of their own. It should be noted that individual disclosure preferences are not objective measures of the attractiveness of both mechanisms but rather, the relative contributions of the mechanism to perceived privacy empowerment.

This study also offers practical suggestions to companies regarding consumer empowerment. To empower consumers, companies should treat information disclosure as a "relationship" rather than a transaction. Hwansoo et al., postulates that highly sensitive information requests are often appropriate for loyal users who have had multiple transactions with the company signaling the existence of a "trusting relationship" [12]. Also, companies seeking to develop a trusting and transparent relationship with their customers regarding information disclosure should move away from mandated disclosure forms to a more simplified form of privacy notices with flexible options for privacy control. Previous research indicates that monetary rewards are more appropriate for low sensitive general information [12]. Therefore, information-collecting companies should design their reward mechanisms prudently as monetary rewards exhibit a negative influence on information privacy concerns specifically in a higher sensitivity context.

7. Conclusion

The growth of big data analytics has coincided with the surge in data breaches and security threats. Consequently, individual privacy concerns have increased partly due to these security breaches and the abuse of privacy rights by data-hungry organizations. According to previous literature, privacy rights abuse can be prevented through privacy empowerment and if possible, eliminate all privacy concern issues. This study proposes a third-option design that seeks to empower users when signing up for an online service. We have found that companies can empower their consumers by adopting fair and transparent privacy policies. Subsequently, consumer empowerment should lead to a positive information disclosure behavior. Also, companies should offer a blend of monetary and non-monetary rewards in the appropriate data sensitivity contexts. To sum it up, privacy empowerment provides a possible win-win solution for both companies and their respective consumers and as such, companies are advised to proactively adopt privacy policies that embody this principle.

At this time, the respondents used for the study were from the academic community at a large university. This provides limitation on the extent to which the results can be generalized to the general population. However, plans are underway to conduct a second data-collection activity to expand the sample size and include working professionals in the study. We anticipate this to increase the sample size, validity and generalizability of the study. Also, this study focused only on privacy empowerment and did not consider its impact on other privacy constructs like the privacy paradox, trust and privacy concern. Further, future studies may consider possible legal policies and regulations which can enhance the adaptability and applicability of privacy control designs like the proposed third-option design in the study.

8. References

[1] T. P. Van Dyke, V. Midha, and H. Nemati, "The effect of consumer privacy empowerment on trust and privacy concerns in e-commerce," Electronic Markets, vol. 17, no. 1, pp. 68–81, 2007.

[2] B. Frimpong and S. Jun, "Individual Privacy Empowerment in Electronic Service," presented at the 26th Americas Conference on Information Systems, Salt-Lake City, Utah.

[3] E. M. Caudill and P. E. Murphy, "Consumer online privacy: legal and ethical issues"," Journal of Public Policy & Marketing, vol. 19, pp. 7–19, 2000.

[4] J. Phelps, G. Nowak, and E. Ferrell, "Privacy concerns and consumer willingness to provide personal information," Journal of Public Policy & Marketing, vol. 19, no. 1, pp. 27–41, 2000.

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

[6] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model," Information Systems Research, vol. 15, no. 4, pp. 336–355, 2004.

[7] Y. Li, “Theories in online information privacy research: A critical review and an integrated framework,” Decision Support Systems, vol. 54, no. 1, pp. 471–481, 2012.
[8] A. Mathews, V. J. Derlega, and J. Morrow, “What is highly personal information and how is it related to self-disclosure decision-making? The perspective of college students,” Communication Research Reports, vol. 23, no. 2, pp. 85–92, 2006.
[9] A. Acquisti and J. Grossklags, “Privacy and Rationality in Individual Decision Making, IEEE Security and Privacy,” IEEE Computer Society, vol. 3, no. 1, pp. 26–33, 2005.
[10] E. Xie, H. H. Teo, and W. Wan, “Volunteering personal information on the internet: Effects of reputation, privacy notices, and rewards on online consumer behavior,” Marketing letters, vol. 17, no. 1, pp. 61–74, 2006.
[11] M. J. Culnan and P. K. Armstrong, “Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation,” Organization Science, vol. 10, no. 1, pp. 104–115, 1999.
[12] L. Hwansoo, D. L., H. K., H. Z., and A. P. C, “Compensation paradox: the influence of monetary rewards on user behavior,” Behavior & Information Technology, vol. 34, no. 1, pp. 45–56, 2015, doi: 10.1080/0144929X.2013.805244.
[13] J. Lanier and E. G. Weyl, A Blueprint for a Better Digital Society. Harvard Business Review, 2018.
[14] Montes, R., Sand-Zantman, W. and Valletti, T.M. The value of personal information in markets with endogenous privacy.2015.
[15] Empower, In Merriam-Webster.com. 2011.
[16] Alshibly H, Chiong R. Customer empowerment: Does it influence electronic government success? A citizen-centric perspective. Electronic Commerce Research and Applications. 2015 Oct 1;14(6):393-404.
[17] Hoffman, L.D., Novak, T.P. and Peralta, M. (1999), “Building consumer trust online”, Communications of the ACM, Vol. 42 No. 4, pp. 80-5
[18]J. H. Hoepman, “Privacy design strategies,” in IFIP International Information Security Conference, Berlin, Heidelberg, Jun. 2014, pp. 446–459.
[19] C. Jensen and C. Potts, “Privacy policies as decision-making tools: an evaluation of online privacy notices”,” in Proceedings of ACM CHI 2004, Vienna, Austria, 2004, pp. 471–478.
[20] J. Bruce, “Defining Rules for Acceptable Adware”,” Dublin, Ireland, 2005.
[21] S. J. C, “A United States Perspective on the Ethical and Legal Issues of Spyware”,” Xi’an China, 2005.
[22] P. C. Pitstop, It pays to read EULAs. 2005.
[23] H. Smith, T. Dinev, and H. Xu, “Information Privacy Research: An Interdisciplinary Review,” MIS Quarterly, vol. 35, no. 4, pp. 989–1015, 2011, doi: 10.2307/41409970.
[24] Shklovski I, Mainwaring SD, Skúladóttir HH, Borgthorsson H. Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. InProceedings of the SIGCHI Conference on Human Factors in Computing Systems 2014 Apr 26 (pp. 2347-2356).
[25] C. Prince, “Do consumers want to control their personal data? Empirical evidence,” International Journal of Human-Computer Studies, vol. 110, pp. 21–32, 2018.