Dispositional willingness to provide personal data online: antecedents and the mechanism

Vatroslav Skare
University of Zagreb, Faculty of Economics & Business
Sigitas Urbonavicius
Faculty of Economics and Business Administration, Vilnius University
Dalia Laurutyte
Faculty of Economics and Business Administration, Vilnius University
Ignas Zimaitis
Faculty of Economics and Business Administration, Vilnius University

Acknowledgements:
This project has received funding from the Research Council of Lithuania (LMTLT), Agreement No P-MIP-19-12.

Cite as:
Skare Vatroslav, Urbonavicius Sigitas, Laurutyte Dalia, Zimaitis Ignas (2020), Dispositional willingness to provide personal data online: antecedents and the mechanism. *Proceedings of the European Marketing Academy*, 49th, (60890)

Paper from the 49th Annual EMAC Conference, Budapest, May 26-29, 2020.

Dispositional willingness to provide personal data online: antecedents and the mechanism

Abstract

Consumer data help marketers in developing analytical insights in order to create targeted value propositions and individualized services. However, this is partly hampered by consumer hesitation to disclose personal information, which includes new aspects in the context of the GDPR implementation. This requires to analyse dispositional factors and mechanisms that predetermine consumer willingness to disclose personal data. The aim of this study is to assess how disposition to value privacy, online privacy concerns, privacy awareness and the perceived regulatory effectiveness influence the disclosure of personal data. The analysis and SEM modelling on the basis of survey data obtained in Lithuania showed that the analysed antecedents influence consumer willingness to disclose personal data indirectly, with mediation of disposition to value privacy. Additionally, privacy awareness mediates the influence of the perceived regulatory effectiveness on disposition to value privacy. This allowed to disclose a new mechanism among dispositional factors of privacy-linked consumer behaviour and to suggest new directions for further research.

Key Words: privacy, willingness to disclose personal data, digital marketing

Track: Digital Marketing & Social Media

1. Introduction

The current marketing landscape has been described as "The Era of Big Data and Personalization" (Weiss, 2018), since the recent technological developments have enabled the organizations to use advanced analytical tools in order to employ vast quantities and various types of consumer data. Detailed consumer profiles and analytical insights assist in creating value propositions for the customers (Hu, 2018). However, the potential of data-driven business practices is partly hampered by consumer hesitation to disclose information, as they express concerns for the loss of control over their personal information and the loss of privacy (Grosso & Castaldo, 2014). Consumer might refuse to disclose personal data or falsify the information they provide (Bansal, Zahedi, & Gefen, 2016). At the same time, there is a societal interest to ensure that consumers are aware of their rights to privacy and data protection (Park, 2013). As a result, policymakers around the world are adapting data protection laws to suit both, a new technological reality with advanced data use capabilities, and consumer concerns over information collection, use and control, as illustrated by the new General Data Protection Regulation (the GDPR) in the EU, adding to the challenge for online marketers. Consequently, there is an increasing need to understand willingness/unwillingness of consumers to disclose various types of their private data.

Generally, a number of privacy-related factors can be dispositional, that is, belong to or are impacted by an individual's pre-existing attitudes, beliefs, tendencies, knowledge and skills, or situational – driven by context-dependent and 'situation-specific privacy factors' and their perceptions, e.g. related to a specific online company or situation (Kehr, et. el, 2015; Li et al., 2011). This suggests that the insights derived from the analysis of the mechanisms between dispositional factors and willingness to disclose personal data may set the ground for further studies that include situational factors.

The study concentrates on key dispositional antecedents of willingness to disclose personal data. These include disposition to value privacy, online privacy concerns, privacy awareness and the perceived regulatory effectiveness; each of them representing a specific aspect of one's disposition that is linked with personal data disclosure.

2. Theoretical Background

With the continuing growth of public concern for online privacy and personal data management, online privacy issues have captured the interest of researchers in a number of fields, including, but not limited to law and public policy (Miltgen & Smith, 2015),

(behavioral) economics (Acquisti, John, & Loewenstein, 2013), social sciences (Walrave & Heirman, 2012), computing and information management systems (Malhotra et al., 2004; Bansal et al., 2016), as well as marketing and consumer research (Akhter, 2014). With the growing importance of relationship marketing and data-driven marketing decision-making and in the context of the e-commerce research, the topic has been particularly important for marketing scholars and practitioners (Grosso & Castaldo, 2014). This particular stream of research mainly concentrates on the consumer level domain of online privacy (Smith et al., 2011). The central variable of this study is willingness to disclose personal information online, defined as "*individual's willingness to reveal personal information to a firm online*" (Mothersbaugh et al., 2012). Willingness to disclose information can be treated as a general personal disposition, isolated from the circumstances of the disclosure (e.g. Anic et al., 2018), though it is also possible to analyse it as a situational intention to disclose information to a vendor (Li et al., 2011; Bansal et al., 2016).

In the literature, personal information disclosure is usually modelled as an outcome variable, focusing on antecedents of declared disclosure intentions or actual behaviour (Grosso & Castaldo, 2014). There is a number of theoretical perspectives employed. It may be approached from the standpoint of the value-based evaluation of privacy (commodity view) and psychological ownership of the personal information (Smith et al., 2011; Kehr et al., 2015). In this case, it has been argued that due to this ownership-risk interaction, behavioural mechanisms, described by the prospect theory (Kahneman & Tversky, 1979), add to unwillingness to give away personal information. This concept has evolved into the privacy calculus framework that assumes that consumers are rational in their decision-making and that there is an inherent trade-off, since disclosure is perceived to have negative consequences due to the loss of some control over the piece of information exchanged (Kehr et al., 2015). Since this included planned behaviours, a number of studies referred to the theory of planned behaviour (TPB) by Ajzen (1985), which states that intentions are indicative of actual behaviour (Smith et al., 2011). However, studies that measured actual behaviour found significant differences between declared willingness and actual disclosure behaviour (Grosso & Castaldo, 2014). This allowed to conceptualize the privacy paradox – an empirically observed disparity between users' privacy attitudes (such as privacy concerns and perceived risks) and actual behaviours (such as disclosure actions or reported intention) (Weinberger & Zhitomirsky-Geffet, 2017). This ambiguity suggested searching for alternative theoretical backgrounds supporting consumer willingness to disclose personal data.

One of the possible alternatives may be the "antecedents-privacy concern-consequences paradigm" (Anic et al., 2018). In this framework, privacy concern is put as a central variable, caused or affected by certain factors (individual, situational or macro-level), and in return it has an impact on consumer's response, such as privacy protection and disclosure behaviour. The framework was applied in consumer privacy literature almost two decades ago (Phelps et al.,2000); later, based on the extensive privacy literature review, Smith et al. (2011) proposed a comprehensive "APCO (Antecedents-Privacy Concerns-Outcomes) Macro" model which puts privacy concerns as the closest "proxy" to privacy concept at the centre of the model and follows the same causal principle. Ideally, the APCO model should be a macro model and it should work across disciplines and contexts (Smith et al., 2011). However, it holds well for the analysis of dispositional (universal) factors and mechanisms of the willingness to disclose personal data if it is considered as a personal disposition. This approach is taken to the core of the current study, where dispositional and privacy-related factors are chosen for further analysis as antecedents of consumer willingness to disclose personal information to companies online for personalization purposes.

3. Hypotheses Development

Some individuals might be naturally more inclined towards certain privacy behaviours and disposition to value privacy as an inherent need and trait which reflects the extent to which people are inclined to maintain their personal information private as much as possible. Individuals who value privacy as higher are less willing to disclose it since the risk of disclosure is perceived by them as higher (Xu et al., 2008). Additionally, Xu et al. (2011) proposed that disposition to value privacy could be a mediating or moderating factor in privacy decisions thus calling for further research on the interactions between disposition to value privacy, online privacy concerns and other characteristics. Our first hypothesis states:
***H_1**: Disposition to value privacy has a negative influence on consumer willingness to disclose personal information online.*

A regulatory aspect of each person's privacy and awareness of practical steps are subjected to the Internet users' literacy and skills to ensure their data protection (Hoofnagle & Urban, 2014). The regulatory approach to address information privacy matters has been applied since 1970s (Miltgen & Smith, 2015). The European Union privacy laws have been characterized as stricter compared to the U.S. (Jentzsch, 2002). Following this tendency, the GDPR aims to give individuals even more control over how their personal data is processed, improve trust in the digital economy and harmonize privacy protection practices of the

organizations even further (General Data Protection Regulation, 2016). Privacy regulation can be operationalized in two ways: either as a situational variable with several possible manipulations of privacy regulation "regimes" regarding data protection requirements, or as a dispositional construct which uncovers how each individual subjectively perceives the privacy regulation to be such as perceived effectiveness of privacy regulation as operationalized by Lwin et al. (2007) and Miltgen and Smith (2015). The latter approach is also adopted in this study in using the awareness of privacy practices ("privacy awareness") as a dispositional construct that reflects how aware an individual is of company practices, regulatory policies and privacy-related matters in the society (Xu et al., 2008). Individuals, highly aware of privacy practices, are more likely to "closely follow privacy issues, the possible consequences of a loss of privacy due to accidental, malicious or intentional leakage of personal information and the development of privacy policies" (Xu et al., 2008). The knowledge of regulatory contexts allows to apply privacy-related practices. This allows proposing the hypothesis:

***H_2**: Perceived regulatory effectiveness has a positive influence on privacy awareness.*

Privacy awareness has been considered to have an impact on various antecedents of online privacy concerns (Xu et al., 2011), being a significant predictor of disposition to value privacy in e-commerce: the higher the privacy awareness, the stronger is the disposition to value privacy (Xu et al., 2008). Therefore, we develop the hypothesis:

***H_3**: Privacy awareness has a positive influence on disposition to value privacy.*

Alternatively, both, the perceived regulatory effectiveness and privacy awareness, may directly influence the factors that are linked with personal information disclosure (Škrinjarić, Budak, & Žokalj, 2018). This allows raising the hypotheses:

***H_4**: Perceived regulatory effectiveness has a positive influence on consumer willingness to disclose personal information online.*

***H_5**: Privacy awareness has a positive influence on consumer willingness to disclose personal information online.*

Privacy concern dominates the consumer-level privacy research, identified as a central construct in empirical privacy research (Smith et al., 2011). General online privacy concern is a pre-existing concern, which is defined as "*an individual's general tendency to worry about information privacy*" (Li et al., 2011). There is empirical support for online privacy concern as having a direct negative effect on willingness to disclose personal information in e-commerce and social networking contexts (Li et al., 2011; Bansal et al., 2016; Anic et al., 2018) as well as for online marketing requests (Walrave & Heirman, 2012). This allows to develop the hypothesis:

***H_6**: Online privacy concern has a negative influence on consumer willingness to disclose personal information online.*

On the other hand, numerous studies report a negative indirect influence of online privacy concern (mediated by risk-related factors) on willingness to disclose personal information (Malhotra et al., 2004). In our model, the key dispositional factor that influences willingness to provide personal information is disposition to value privacy. In terms of its content it is close to online privacy concern which allows them to be related in the model:
***H_7**: Online privacy concern has a positive influence on disposition to value privacy.*

4. Methodology

The data were collected in Lithuania by means of the internet survey and a self-administered questionnaire which included the scales, successfully used in former studies and showing satisfactory reliability and validity. All items were measured on a 1-7 Likert scale. More specifically, a 3-item scale for disposition to value privacy was originally developed by Xu et al. (2008) with Cronbach's α=0.88 and adapted by Xu et al. (2011), Li (2014). The perceived regulatory effectiveness scale (3 items, α=0.83) was adapted from Lwin et al. (2007) with a minor alteration that includes GDPR as an example. The privacy awareness scale (3 items) taken from Xu et al. (2008), was later adopted by Xu et al. (2011) and showed good reliability (α=0.865). This particular scale measures one's privacy literacy does not overlap with other measured variables, ensuring good discriminant validity. Online privacy concern has been assessed with the Internet Users Information Privacy Concerns scale by Malhotra et al. (2004). The scale includes 10 items and measures general privacy concerns. It includes three subscales: collection, control over personal information and awareness of privacy practices. Willingness to disclose personal data was measured by a scale adopted from a 14-item "index" list from Robinson (2017) which showed good reliability (α = 0.87) and was the most relevant and recent scale of this type. The original items' list was reduced from 17 to 11 items by removing entirely technical items that would not be known by general population. The scale was amended with 5 items on data is collected online automatically in line with the consent of a person.

The survey collected 439 questionnaires usable for analysis. The sample included respondents from 18 to 69 years old; 32.1% represented the age group of 18-22; 33.0% the group of 23-35; remaining 34.9 were 36 or elder. By gender, 25.1% were male and 74.9 female. 54.9% of respondents had bachelor or lower educational degrees and 45.1% master's or higher.

One item was removed from willingness to disclose the personal data scale because of high skewness (2.532) and curtosis (5.799). Other data was included into the confirmatory factor analysis (maximum likelihood; Promax rotation with Kaiser normalization). Kaiser-Meyer-Olkin measure of sampling adequacy was 0.877, Bartlett's test of sphericity was significant (0.000), approx. Chi-square 7401.378 and df=496. Extracted factors explained 57.860 of the total variance. The reliability of scales was satisfactory: disposition to value privacy $\alpha = 0.835$; perceived regulatory effectiveness $\alpha = 0.746$; privacy awareness $\alpha = 0.829$; online privacy concern $\alpha = 0.901$; willingness to disclose personal data $\alpha = 0.893$.

A subsequent confirmatory factor analysis showed a good model fit: CMIN/DF=2.297; TLI rho^2=0.909; CFI=921; RMSEA=0.054. This allowed to test the hypotheses.

5. Hypotheses Testing

A causal model outlined two alternative ways how the analysed factors may impact willingness to disclose data: directly and via the mediation of disposition to value privacy. Additionally, privacy awareness mediated the relation between the perceived regulatory effectiveness and Disposition to value privacy. The fit of the model was satisfactory: CMIN/DF=2.319; TLI rho^2=0.908; CFI=919; RMSEA=0.0554, which allowed to test the hypotheses. The test based on the analysis of the direct relations among the predicted factors is shown in Table 1.

Table 1 Regression Weights

			Estimate	S.E.	C.R.	P
Privacy_Awar	<---	Perc_Reg_Effect	0.342	0.070	4.868	***
Disposition_TVP	<---	Onl_Priv_Concern	0.515	0.074	6.977	***
Disposition_TVP	<---	Privacy_Awar	0.425	0.053	8.021	***
WTD	<---	Perc_Reg_Effect	0.116	0.072	1.625	0.104
WTD	<---	Privacy_Awar	0.100	0.065	1.542	0.123
WTD	<---	Onl_Priv_Concern	-0.118	0.084	-1.403	0.161
WTD	<---	Disposition_TVP	-0.468	0.074	-6.357	***

The findings disclose that only the disposition to value privacy has a significant direct impact on willingness to disclose personal data. This impact is negative and strong (r=-0.468, sig=0.000). This allows to support $\mathbf{H_1}$. Hypotheses $\mathbf{H_4}$, $\mathbf{H_5}$, and $\mathbf{H_6}$ are rejected since the relation between the variables is not significant. However, the predicted relations between the antecedents of willingness to disclose data are significant, which allows to accept the remaining hypotheses: $\mathbf{H_2}$, $\mathbf{H_3}$, and $\mathbf{H_7}$.

6. Discussion, Conclusions and Further Research

In general, the findings of the study allow to see the mechanism how the tested factors influence willingness to disclose personal data: the influence of all of them is mediated by disposition to value privacy, but remains noticeable (WTD <--- Onl_Priv_Concern -0.163; WTD <--- Perc_Reg_Effect -0.028; WTD <--- Privacy_Awar -0.191). The analysis also shows a positive indirect (mediated by privacy awareness) influence of the perceived regulatory effectiveness on disposition to value privacy. This presents a scientific novelty in research on private data disclosure. Additionally, the study suggested further conceptualization of willingness to disclose personal data as a dispositional variable. The used scale for measuring willingness to disclose personal data (Robinson, 2017), included two types of data (provided by a person and collected online automatically). Though this study did not specify these groups as possible sub-constructs, an exploratory factor analysis showed the relevance of this concept. Moreover, it seems that individually provided data additionally falls into two categories: the data that is provided as facts about the personal parameters, and the data (addresses) of used social/communication engines (like Facebook, LinkedIn, Skype). This was additionally supported during a confirmatory factor analysis where errors of the similar data types were highly correlated. All this suggests that further conceptualization of dispositional willingness to provide personal data is needed as a further research direction. The concentration on this issue may show whether the construct includes three sub-dimensions or even three separate constructs that represent different types of willingness to provide personal data online.

References

1. Acquisti, A., John, L. K., & Loewenstein, G. (2013). What Is Privacy Worth? *The Journal of Legal Studies*, *42*(2), 249–274.
2. Ajzen, I. (1985). From Intentions to Actions: A Theory of Planned Behavior. In J. Kuhl & J. Beckmann (Eds.), *Action Control: From Cognition to Behavior,* 11–39. Berlin, Heidelberg: Springer Berlin Heidelberg.
3. Akhter, S. H. (2014). Privacy concern and online transactions: the impact of internet self-efficacy and internet involvement. *Journal of Consumer Marketing*, *31*(2), 118–125.
4. Anic, I.-D., Budak, J., Rajh, E., Recher, V., Skare, V., & Skrinjaric, B. (2018). Extended model of online privacy concern: what drives consumers' decisions? *Online Information Review*, *7*(3), 41.

5. Bansal, G., Zahedi, Fatemeh M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management*, *53*(1), 1–21.
6. Dinev, T., & Hart, Paul. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, *17*(1), 61–80.
7. General Data Protection Regulation (GDPR) - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L119:1-88, April 2016. Accessed on: https://eur-lex.europa.eu/eli/reg/2016/679/oj (viewed on 10 April 2019).
8. Grosso, M., & Castaldo, S. (2014). Retailer-Customers Relationships in the Online Setting: An Empirical Investigation to Overcome Privacy Concerns and Improve Information Sharing. In F. Musso & E. Druica (Eds.), *Handbook of Research on Retailer-Consumer Relationship Development* (pp. 404–425). Hershey, PA: IGI Global.
9. Hoofnagle, C. J., & Urban, J. (2014). Alan Westin's Privacy Homo Economicus. *Wake Forest Law Review*. (49).
10. Hu, Y. (2018). Marketing and Business Analysis in the Era of Big Data. *American Journal of Industrial and Business Management*, *08*(07), 1747–1756.
11. Jentzsch, N. (2002). The Economics and Regulation of Financial Privacy - A Comparative Analysis of the United States and Europe. *SSRN Electronic Journal.*
12. Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, *47*(2), 263.
13. Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*(6), 607–635.
14. Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems*, *51*(3), 434–445.
15. Li, Y. (2014). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision Support Systems*, *57*, 343–354.
16. Lwin, May, Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses: a power–responsibility equilibrium perspective. *Journal of the Academy of Marketing Science*, *35*(4), 572–585.

17. Malhotra, N. K., Kim, S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, *15*(4), 336–355.
18. Miltgen, C. L., & Smith, H. (2015). Exploring information privacy regulation, risks, trust, and behavior. *Information & Management*, *52*(6), 741–759.
19. Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., & Wang, S. (2012). Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information. *Journal of Service Research*, *15*(1), 76–98.
20. Park, Y. J. (2013). Digital Literacy and Privacy Behavior Online. *Communication Research*, *40*(2), 215–236.
21. Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing*, *19*(1), 27–41.
22. Robinson, S. C. (2017). Disclosure of personal data in ecommerce: A cross-national comparison of Estonia and the United States. *Telematics and Informatics*, *34*(2), 569–582.
23. Škrinjarić, B., Budak, J., & Žokalj, M. (2018). The effect of personality traits on online privacy concern. *Ekonomski Pregled*, *69*.
24. Smith, H., Dinev, T., & Xu, H. (2011). *Information privacy research: An interdisciplinary review* (Vol. 35).
25. Walrave, M., & Heirman, W. (2012). Adolescents, Online Marketing and Privacy: Predicting Adolescents' Willingness to Disclose Personal Information for Marketing Purposes. *Children & Society*, *38*.
26. Weinberger, M., Bouhnik, D., & Zhitomirsky-Geffet, M. (2017). Factors Affecting Students' Privacy Paradox and Privacy Protection Behavior. *Open Information Science*, *1*(1), 1.
27. Weiss, E. (2018, May 25). How to Convince Customers to Share Data after GDPR. *Harvard Business Review*. Retrieved from https://hbr.org/2018/05/how-to-convince-customers-to-share-data-after-gdpr (viewed on 20 May 2018).
28. Xu, H., Dinev, T., Smith, J., & Hart, Paul. (2011). Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. *Journal of the Association for Information Systems*, *12*(12), 798–824.
29. Xu, Heng; Dinev, Tamara; Smith, H. Jeff; and Hart, Paul, "Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View" (2008). ICIS 2008 Proceedings. Paper 6. Proceedings. Paper 6. http://aisel.aisnet.org/icis2008/6