https://doi.org/10.15388/vu.thesis.362
https://orcid.org/0000-0003-0067-6513

VILNIUS UNIVERSITY

Ignas Zimaitis

The Impact of Exaggerated Distrust on Willingness to Disclose Personal Data Online

DOCTORAL DISSERTATION

Social sciences,
Management (S 003)

VILNIUS 2022

The dissertation was prepared between 2015 and 2021 at Vilnius University.

The researches were partly supported by Research Council of Lithuania.

Academic supervisor – Prof. Dr. Sigitas Urbonavičius (Vilnius University, Social sciences, Management – S 003).

This doctoral dissertation will be defended in a public meeting of the Dissertation Defence Panel:

Chairman – Prof. Dr. Aida Mačerinskienė (Vilnius University, Social sciences, Management – S 003).
Members:
Prof. Dr. Danuta Diskienė (Vilnius University, Social sciences, Management – S 003);
Prof. Dr. Durdana Ozretic Dosen (University of Zagreb, Social sciences, Management – S 003);
Assoc. Prof. Dr. Agnė Gadeikienė (Kaunas University of Technology, Social sciences, Management – S 003);
Prof Dr. Vida Škudienė (ISM University of Management and Economics, Social sciences, Management – S 003).

The dissertation shall be defended at a public meeting of the Dissertation Defence Panel at 14:00 on 8th of September 2022 in Room 710 of the Faculty of Economics and Business Administration (Vilnius University).
Address: Saulėtekio av. 9, 2nd building, room 710, Vilnius, Lithuania
Tel. +370 5 236 6126; e-mail: evaf@evaf.vu.lt

The text of this dissertation can be accessed at the library of Vilnius University, as well as on the website of Vilnius University:
www.vu.lt/lt/naujienos/ivykiu-kalendorius

https://doi.org/10.15388/vu.thesis.362
https://orcid.org/0000-0003-0067-6513

VILNIAUS UNIVERSITETAS

Ignas Zimaitis

Perdėto nepasitikėjimo įtaka norui atskleisti asmens duomenis internete

DAKTARO DISERTACIJA

Socialiniai mokslai,
Vadyba (S 003)

VILNIUS 2022

Disertacija rengta 2015–2021 metais Vilniaus universitete.

Mokslinius tyrimus iš dalies rėmė Lietuvos mokslo taryba.

Mokslinis vadovas – prof. dr. Sigitas Urbonavičius (Vilniaus universitetas, socialiniai mokslai, vadyba – S 003).

Gynimo taryba:
Pirmininkė – prof. dr. Aida Mačerinskienė (Vilniaus universitetas, socialiniai mokslai, vadyba – S 003).
Nariai:
Prof. dr. Danuta Diskienė (Vilniaus universitetas, socialiniai mokslai, vadyba – S 003),
Prof. dr. Durdana Ozretic Dosen (Zagrebo universitetas socialiniai mokslai, vadyba – S 003),
Doc. dr. Agnė Gadeikienė (Kauno technologijos universitetas, socialiniai mokslai, vadyba – S 003),
Prof. dr. Vida Škudienė (ISM vadybos ir ekonomikos universitetas, socialiniai mokslai, vadyba – S 003).

Disertacija ginama viešame Gynimo tarybos posėdyje 2022 m. rugsėjo mėn. 8 d. 14 val. Vilniaus universiteto Ekonomikos ir verslo administravimo fakulteto 710 auditorijoje. Adresas: (Saulėtekio al. 9, II rūmai, 710 auditorija, Vilnius, Lietuva), tel. 370 5 236 6126 ; el. paštas evaf@evaf.vu.lt

Disertaciją galima peržiūrėti Vilniaus universiteto bibliotekoje ir VU interneto svetainėje adresu:
https://www.vu.lt/naujienos/ivykiu-kalendorius

TABLE OF CONTENTS

INTRODUCTION

Relevance and novelty of the topic. The consumer-generated data has become an important asset for organizations, as the obtained personal consumer data allows businesses to provide tailored online marketing offers, which reflects on a better value proposition (Zhang et al., 2020). According to Barth and Jong (2017), customers typically perceive personalized marketing offerings as advantageous. However, in most cases the value of such offerings is still outweighed by some concerns, thus the customers in general are not willing to disclose their personal data while purchasing online (Wieringa et al., 2019). The reasoning behind unwillingness to disclose personal data online has attracted very significant scholars' attention. This phenomenon is frequently analysed by employing the privacy calculus theory, which states that customers disclose personal data in exchange for benefits (Robinson, 2017). In the scope of the privacy calculus theory, consumer information is treated as a commodity (Smith et al., 2011). Although privacy calculus theory is very frequently used in privacy-related consumer decision-making studies, such an approach has received a significant critique since it overestimates the argument of rationality (Kehr et al., 2015). Thus, other authors claim that privacy-related decisions are not only based on the cost-benefit analysis but instead they are mainly situational and depend on the purpose and the context of information disclosure (Omrani & Souli'e, 2018; Masur, 2019). In addition, it is widely accepted that various dispositional factors are also related to the unwillingness to disclose personal data online (Nikhhah, 2018), which is also outside the scope of privacy calculus theory.

Among such dispositional factors that relate to consumer privacy-related behaviour, trust plays an essential role in modelling numerous internet-based activities (Kulokakis, 2018; Zhang et al., 2020). Although trust is sometimes considered as a continuous construct, some scholars argue that the lowest point of the measurement does not necessarily imply distrust (McKnight & Chervany, 2001; Kim & Ahmad, 2013, Aghdam et al., 2021). Thus, Dinev and Hart (2006) suggest that trust and distrust coexist as separate constructs, the latter being considered a factor that impacts the consumer intentions even more significantly (Moody et al., 2014). Distrust, on the other hand, can also get into various forms, as it is widely accepted that distrust can be categorized into rational and irrational types (Deutsch, 1973). Rational distrust is described as flexible and able to change depending on specific situations. In contrast, irrational distrust implies being inflexible and incapable to respond to the changing circumstances (Deutsch, 1973). As distrust is

widely analysed in the context of consumer behaviour, the impact of its irrational, exaggerated forms is understudied.

Although there are multiple constructs related to the exaggerated distrust, such as technophobia (Nimrod, 2018), cyber-fear (Mason et al., 2014), and social anxiety (van Scoy et al., 2021), this dissertation focuses on two types of exaggerated distrust – paranoia (Kramer, 2008) and conspiracy beliefs (Simone et al., 2021). These two forms of exaggerated distrust are selected due to their distinctiveness – paranoia as a form of exaggerated distrust is more linked with the irrational distrust towards individuals (Colby, 1981), and conspiracy beliefs – toward organizations (van Prooijen & de Vries, 2016). Such an approach is undertaken as it allows investigating the impact of these two forms of exaggerated distrust on the willingness to disclose personal data in different circumstances, depending on the level of formal regulations (personal data disclosure on social media platforms versus purchasing online), which has not been previously analysed in the scientific literature.

Summarizing the relevant research in this field, it can be concluded that there are major gaps in the scientific literature addressing the willingness to disclose personal data online. First, there are no previous attempts to investigate privacy-related behaviour in different contexts, depending on their external formal regulations. Secondly, the impact of exaggerated forms of distrust on the willingness to disclose personal data online is understudied. Finally, there are multiple theoretical approaches that are employed in privacy-related behaviour research, but they overemphasize the aspect of rationality. Thus, such insights into the topic allow the author of this thesis to formulate the **scientific problem** of this dissertation **as a question**: what is the impact of exaggerated forms of distrust on the willingness to disclose personal data online?

In such context, this dissertation offers a novel approach to the privacy-behaviour analysis, suggesting the employment of the Social Exchange Theory (SET). This theory has been surprisingly rarely considered in marketing studies, though the very essence of marketing lies in the relationships and various forms of social exchanges (Bagozzi, 1975; Varey, 2015). SET sees interactions among individuals or companies as a series of social exchanges that differ in their forms and in the objects exchanged. Information (including personal data) is one of the objects that is exchanged with others. SET contains two dimensions – reciprocal and negotiated types of social exchange (Lévi-Straus, 1969; Emerson, 1981). A negotiated type of exchange occurs when the terms of exchange are agreed upon by the

participating parties in advance and are largely formalized. The negotiation typically is about the benefits and costs of the exchange, also considering the needed additional aspects, such as timing, etc. Online purchasing situations typically include interactions, which classify them into the category of negotiated social exchanges (Molm et al., 2000). Reciprocal exchange is based on mutual interactions of exchange participants with the expectation that a partner will reciprocate in a similar manner (Cheng et al., 2011). The terms of the exchange are not necessarily agreed upon or formalized in advance, which makes this type of exchange to be largely based on mutual trust (Molm et al., 2000). Activities in social networks present a good example of reciprocal exchange of personal information with others (Yang, 2019). The exchange of information in social networks is not necessarily driven by rational or economic motivations; people share information seeking to socialize, aiming for recognition, support, and other intangible benefits (Szymczak et al., 2016). Based on mutual trust, the information is shared with high levels of openness and spontaneity (Koohikamali et al., 2017). Based on this, the impact of two forms of exaggerated distrust (paranoia and conspiracy beliefs) on willingness to disclose personal data is studied in the framework of SET.

Thus, **the aim of the dissertation** is to identify how exaggerated forms of distrust influence the willingness to disclose personal data online.

To achieve the aim of the dissertation, the following objectives are set:

1. To conceptualize the phenomenon of distrust and outline its exaggerated forms;
2. To assess the impact of exaggerated forms of distrust on overall consumer behaviour online;
3. To assess the ways how willingness to disclose personal data can be conceptualized and measured;
4. To justify the application of Social Exchange Theory in investigating the impact of paranoia and conspiracy beliefs as forms of exaggerated distrust on willingness to disclose personal data online;
5. To evaluate the impact of paranoia and conspiracy beliefs on the willingness to disclose personal data online in reciprocal and negotiated social exchange environments.

By implementing these objectives, the author of this dissertation aims to defend the following **research statements:**

1. Trust and distrust exist as two distinctive continua distrust can subsequently be classified into rational and exaggerated forms.

2. Exaggerated distrust (in a form of paranoia) plays a significant role in shaping the overall online consumer behaviour.
3. Willingness to disclose personal data is a multidimensional factor – it comprises three types of personal data disclosure: individual facts, social networking data, and online purchasing data.
4. Willingness to disclose personal data can be analysed in the framework of Social Exchange Theory. More specifically, exaggerated distrust (paranoia and conspiracy beliefs) has an impact on data disclosure behaviour in both reciprocal and negotiated social exchange contexts.

Dissertation structure. The dissertation is based on four articles published in the journals that are indexed in the Clarivate Web of Science Core Collection written in co-authorship with other researchers. Thus, the dissertation contains four principal chapters, each corresponding to the individual article which is then followed by conclusions, recommendations for future research, and practical implications sections.

1. The first article "Social Media Use and Paranoia: Factors That Matter in Online Shopping" was published in the scientific journal "Sustainability", co-authored by Assoc. Prof. Dr. Mindaugas Degutis, and Prof. Dr. Sigitas Urbonavičius. The contribution of the author of this thesis to this article includes the literature analysis, the development of methodology, data gathering, and the development of the first draft of the manuscript. The article aims to conceptualize the phenomenon of distrust and discusses the existence of distinctive concepts of trust and distrust as continua. Additionally, the paper outlines the existence of paranoia as a form of exaggerated distrust and then analyses its impact on overall consumer behaviour by investigating its relationship with the attitudes toward purchasing online and the intention to purchase online. The findings of the research reveal the significant impact of exaggerated distrust on attitudes towards purchasing online and intention to purchase online. Thus, the results of the study set the background for further analysis of its implications on a very specific aspect of online behaviour – the willingness to disclose personal data.
2. The second article entitled "Willingness to Disclose Personal Information: How to Measure It?" published in the scientific journal "Engineering Economics" is co-authored by Assoc. Prof. Dr. Mindaugas Degutis, Prof. Dr. Sigitas Urbonavičius, Assoc. Prof. Dr. Vatroslav Škare, and Dalia Laurutytė. The contribution of the author

of the thesis to this article includes the development of methodology, data collection, data analysis and critical revision of the manuscript. The second study had two aims. First, it aimed to conceptualize the factor of willingness to disclose personal data online; second, it intended to clarify methodological issues regarding the measurement of the willingness to disclose personal data. The first task needed to address the concept of willingness to disclose personal data and formulate its distinctive nature, differentiating it from the intention to disclose personal data. The second task aimed to clarify the types of data and ways of their collection and make a clear distinction between the data that are disclosed by a person, the data that are collected by the other part of information exchange, and the items that are linked with permissions to use provided data. The findings of the study show that willingness is linked with three types of data: the willingness to disclose personal data that includes individual facts, social networking data, and online purchasing data. Such findings allowed the usage of the adapted measurement tool in further analyses of the impact of exaggerated distrust-related factors on the willingness to disclose personal data online.

3. The third article "From Social Networking to Willingness to Disclose Personal Data When Shopping Online: Modelling In The Context of Social Exchange Theory" is published in the scientific journal "Journal of Business Research". The article was written in co-authorship with Prof. Dr. Sigitas Urbonavičius, Assoc. Dr. Mindaugas Degutis, Vaida Kaduškeviciute, and Assoc. Prof. Dr. Vatroslav Škare. The thesis author's contribution to this article includes the development of the first draft of literature analysis, selection of the measurement scales, and critical revision of the manuscript. The article applies the willingness to disclose personal data measurement tool, which was modified in the second study of this dissertation, and employs a novel approach toward the analysis of the willingness to disclose personal data. This is done by employing the Social Exchange Theory which provides an insightful outcome – both trust and the exaggerated form of distrust (paranoia) have a positive impact on willingness to disclose personal data in the reciprocal relationships (personal data disclosure in social media); also, data disclosure in reciprocal relationships has a positive impact on the willingness to disclose personal data in the context of online purchasing. Thus, the results of the study set the background for the final research whose

main aim was to investigate the impact of conspiracy beliefs as a different form of exaggerated distrust on the willingness to disclose personal data online.

4. The fourth article "Influence of Trust and Conspiracy Beliefs on the Disclosure of Personal Data Online" was published in the scientific journal "Journal of Business Economics and Management". The article is co-authored by Prof. Dr. Sigitas Urbonavičius, Assoc. Prof. Dr. Mindaugas Degutis, and Vaida Kaduškeviciute. The thesis author's contribution to this article includes the literature analysis, the development of the methodology and results. The paper continues the same research path which was set in the third study of this thesis, and further investigates the possible implications of exaggerated distrust forms on the willingness to disclose personal data. The study extends the model which was developed in the third article and investigates the impact of conspiracy belief (as a form of exaggerated research) on the willingness to disclose personal data in both reciprocal and negotiated contexts. Thus, the application of Social Exchange Theory regarding explaining the willingness to disclose personal data is supported.

Overall contribution. First, the dissertation suggests a new theoretical approach to the analysis of privacy-related behaviour. Following the existing critique of the privacy calculus theory for overly emphasizing the aspect of rationality (Kehr et al., 2015), this dissertation emphasizes the social aspect of data disclosure online (i. e., personal data disclosure in social networks). Following this path, a new theoretical framework based on Social Exchange Theory is employed. Thus, this dissertation contributes to the scientific literature by studying the willingness to disclose personal data from the perspectives of negotiated and reciprocal exchanges and opening a new perspective for future studies.

Secondly, even though there are multiple ways on how the willingness to disclose data is measured, the issue of existing scales being not up to date with the current technological advances is challenged with this dissertation. Thus, the dissertation proposes a modified and validated multidimensional scale to measure willingness to disclose personal data online.

Finally, the dissertation fills the theoretical gap by investigating the impact of exaggerated forms of distrust on the willingness to disclose personal data online depending on the level of formal regulations, which is a novel aspect in the privacy-related consumer behaviour field. Two studies based on Social Exchange Theory disclose that there is a relationship between

reciprocal and negotiated types of exchanges (i. e., trust, which is built in the reciprocal environment, has a positive impact on the willingness to disclose personal data in the negotiated environment). Also, contrary to what was hypothesized, exaggerated distrust motivates the members to participate in the reciprocal exchange (willingness to disclose personal data on social media), which draws a very interesting direction for future research. Moreover, the results of these studies suggest that exaggerated forms of distrust have a direct negative impact on the willingness to disclose personal data in negotiated exchange (purchasing online).

1. SOCIAL MEDIA USE AND PARANOIA: FACTORS THAT MATTER IN ONLINE SHOPPING

The first chapter of this dissertation involves the study "Social Media Use and Paranoia: Factors That Matter in Online Shopping", which was published in the scientific journal "Sustainability". This research sets the foundation for the upcoming studies of the dissertation as it conceptualizes the phenomenon of distrust, distinguishes its mechanism from the trust factor, discusses paranoia and cyber-fear as a form of exaggerated distrust, and explores its impact on overall attitudes towards purchasing online and intention to purchase online.

The aim and scope of the research. The study is based on exploratory quantitative research which aims to fill the existing theoretical gap by analysing paranoia and cyber-fear as the exaggerated types of distrust in the context of social media use, online shopping attitudes and intentions. The main assumption of the research is that paranoia as a type of exaggerated distrust is an antecedent of the attitude toward online purchasing that mediates the effects of other factors towards it. This is confirmed with SEM modelling based on empirical data: the analysis provides evidence that paranoia is an important antecedent of the attitude towards purchasing online and mediates relationships between computer competence, cyber-fear, social media use, and the attitude towards online shopping. As both dependent variables (attitude towards purchasing online and intention to purchase online) are inevitably related to the personal data disclosure, this exploratory research allowed me to set the background for the following studies.

Theory and hypotheses. Trust in the platform is among the most important factors in predicting the consumer intention to purchase online (Joon, 2002). On the other hand, there are factors that influence online purchasing intentions negatively, typically generating some form of distrust (Benamati & Serva, 2007). In this case, trust is suggested to have a stronger effect on low-risk behaviours, while distrust has a stronger negative impact on higher-risk behaviours (Chang & Fang, 2013). Paranoia as an exaggerated form of distrust is not only directed towards the other individuals but also towards the social groups and organizations (Colby, 1981), and, possibly, processes. In such circumstances, paranoia may play a particular role in specific internet-based activities, such as online shopping, as electronic purchasing is almost always associated with specific fears and risks which customers are perceiving. This allows assuming that paranoia, a factor that represents a set of irrational risk perceptions, may be the antecedent

influencing consumer response negatively. Thus, the first three hypotheses are formulated:

H1: Paranoia has a direct negative influence on attitude towards purchasing online.

H2: Paranoia has no direct impact on intention to purchase online.

H3: Paranoia has an indirect negative impact on the intention to purchase online when the relationship is mediated by an attitude towards purchasing online.

In the context of online activities, distrust is associated with other negative factors. All of them originate from a broad background of privacy concerns and related risks. The phenomenon of privacy concern in buyer behaviour is mainly linked to the awareness of privacy-related issues which include the disclosure of personal information to third parties (Buchanan et al., 2007). Many studies agree on a strong negative influence of the privacy concern on the extent of various internet-related activities (Akhter, 2014; van Slyke et al., 2002). Purchasing online is among such factors, and it is claimed that the risk of privacy loss online is negatively related to the purchasing intention (Dai et al., 2007). The influence of the perceived threats may be so strong that individuals may feel an overall fear to perform digital activities, and this may be defined as cyber-fear (Mason et al., 2014). Thus, the following hypotheses are formulated:

H4: Cyber-fear has a direct negative impact on the attitude towards purchasing online.

H5: Privacy concern has a direct negative impact on the attitude towards purchasing online.

H6: Cyber-fear has an indirect negative impact on the attitude towards purchasing online when the relationship is mediated by paranoia.

People who use social media frequently receive unexpected suggestions or recommendations, depending on their previous interactions, preferences and likes. These instances have obvious explanations on the basis of used programming algorithms, however, they may seem unclear and even threatening to the general population, since typical users cannot be professionally aware of the technical side of how internet-based social networks are working. Intensive use of social media increases the number of such interactions and therefore increases the opportunity for paranoid cognition. However, there is no theoretical or empirical evidence that could allow predicting the valence of this relationship, since the relation between the social media use integration and paranoia is expected to be positive, while the

relation between paranoia and the attitude – negative. Since the latter is more strongly justified, we hypothesize as follows:

H7: Paranoia mediates a negative impact of the integration of social media use on the attitude towards purchasing online.

Continuing a similar logic as with the hypotheses on social media use, we state that competent users should have answers to many of unexpected occurrences during the internet-based activities. Therefore, computer competence seems not likely to have a relation (at least positive) with paranoia. However, computer expertise allows us to know how much tracking may be done on the internet, and how badly this accumulated knowledge may be used by somebody with bad intentions (Hung et al., 2010). As a result, the increase in computer expertise may develop a paranoid cognition. As in the case of social media use, we may predict a negative influence of computer competence on the attitude, if mediated by paranoia:

H8: Computer competence has an indirect negative impact on the attitude towards purchasing online when the relationship is mediated by paranoia.

In addition, it is expected that computer competence should have a positive influence on the attitude towards purchasing online:

H9: Computer competence has a direct positive impact on the attitude towards purchasing online.

Methodology. The quantitative research method is used to investigate the relationships between the variables. Data is collected via the internet survey. The analysis is based on 287 respondents from Lithuania. To measure the trait of paranoia, a 5-point 20 items Likert-type general paranoia scale, developed by Fenigstein and Vanable (1992), was used, which is widely accepted as a measurement tool that makes it possible to capture the paranoia in non-clinical samples. The cyber-fear was measured using a 5-point 11 items Likert-type cyber paranoia and fear scale, developed by Mason, Stevenson, and Freedman, which had been originally reported to be loading on two factors–cyber paranoia and cyber-fear (Mason et al., 2014). In the scope of this research, the cyber-fear factor was utilized and taken into consideration. The following factor, the privacy concern was measured by a 5-point 16 items Likert-type attitudinal scale, evaluating the scope of general concerns about privacy on the Internet (Buchanan et al., 2007). The social media use was measured by employing the social media use integration scale (10 items on a 7-point scale) to assess the involvement and emotional connection to the social networks (Jenkins-Guarnieri et al., 2013). Computer competence was measured using 4 items on a 5-point Likert-type internet and computer comfort/competency scale, which is linked with the extent of the computer

and internet skills (Morahan-Martin & Schumacher, 2013). The attitude toward purchasing online (10 items on a 5-point Likert-type scale) and online purchasing intention (4 items on a 5-point Likert-type scale) was taken from a similar study (Zerrard & Debabi, 2012). An exploratory factor analysis with a maximum likelihood extraction and Promax with Kaiser normalization rotation allowed the extraction of 7 factors that explained 60.5% of the variance. The KMO value was 0.815 (> 0.7), and the Bartlett's Chi-square value resulted in 5217.930 (p = 0.00) and demonstrated the sample adequacy and applicability for the analysis. 27 non-redundant residuals equalled 5%, which was an acceptable result for the adequacy. All correlations between the factors were below 0.7, which suggested an acceptable discriminant validity. In addition, all the factor loadings were above 0.5.

Results. The hypotheses of the research were tested using the structural equation analysis, estimating the path coefficients for each relationship. The acceptable level of model fit was confirmed, measuring the following values: $\chi 2$ (278)=584.9, CMIN=499.442, DF=375, CFI=0.974, TLI=0.968, RMSEA=0.034. In total, 9 hypotheses were tested, and seven of them were accepted. The research model with regression weights is presented in Figure 1.

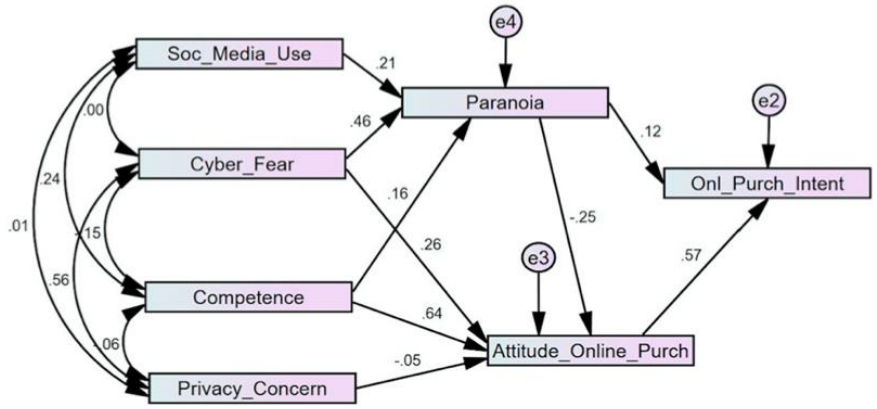

Figure 1. *Structural Model of Study 1*

H1 hypothesis states that paranoia has a direct negative influence on the attitude toward purchasing online. The regression analysis shows a significant negative relationship between paranoia and the attitude toward purchasing online (β=-.306, p =0.000), thus H1 is accepted. H2 states that paranoia has no direct impact on online purchasing intention. However, the regression analysis shows rather contradicting results: this relation is not

significant if $p<0.01$ is issued; however, it would be significant if $p<0.05$ criteria were employed (as it is done in many studies). In this study, we use stricter criteria for significance, therefore the results (β=0.105, p=0.013) allow us to accept H2. H3 hypothesizes that paranoia has an indirect negative impact on the intention to purchase online when the relationship is mediated by the attitude towards purchasing online. An indirect effect on purchase intention, mediated by the attitude towards online purchasing, is found to be negative (β=- 0.026), therefore, H3 is accepted. H4 presumes that cyber-fear has a direct negative impact on the attitude towards purchasing online. However, the results are the opposite: cyber-fear has a direct positive impact on the attitude toward purchasing online (β=0.288, p=0.000), thus H4 hypothesis is rejected. H5 predicts that privacy concern has a direct negative impact on attitude toward purchasing online. A regression analysis shows that this relation is not significant (β=-0.053, P=0.358), therefore, H5 is rejected. H6 presupposes that cyber-fear has an indirect negative impact on the attitude toward purchasing online when the relationship is mediated by paranoia. The assessment of the standardized indirect effect confirms this assumption (β=-0.117), and H6 is accepted. H7 hypothesis predicts that paranoia mediates a negative impact of social media use integration on the attitude towards purchasing online. Standardized indirect effects show the existence of a relatively small (β=-0.53) negative indirect effect, and this allows accepting H7. H8 hypothesizes that computer competence has an indirect negative impact on the attitude towards purchasing online when the relationship is mediated by paranoia. The standardized indirect effects show that due to mediation, computer competence changes the relationship valence and is negative (β=-0.04). Thus, H8 is accepted. H9 proposes that computer competence has a direct positive impact on the attitude towards purchasing online. The regression analysis shows a significant positive relationship between computer competence and the attitude toward purchasing online (β=1.032, P=0.000), thus H9 is accepted.

Discussion and conclusions. The purpose of this study was to examine the role of paranoia in relation to social media use in the context of the online purchasing process. The findings of the study suggest that paranoia is an important psychological antecedent in the attitude toward purchasing online, which is a new element in overall studies of online behaviour. Elaboration on this negative relationship presents the main contribution of the current study since the growing complexity of human interactions with IT systems triggers extreme forms of distrust and even paranoia. The current study might be considered as an extension of the studies on distrust, as

paranoia can be considered the exaggerated type of distrust (Deutsch, 1973) and the current findings broaden the previous knowledge that distrust has a negative impact on attitudes towards purchasing online (Kim, 2012). The current study extends the previous scope of knowledge regarding the antecedents of distrust/paranoia by including the consideration of two factors that represent user competence from two perspectives: the general computer competence and engagement in social media use.

Another important finding of this study is the disclosure of the fact that paranoia mediates the effects of other factors on the attitude of purchasing online. These factors (social media use integration, cyber fear, and computer competence) are different in their nature and their potential influence on online purchasing. However, paranoia is a mediator between them and the attitude toward online purchasing. To our knowledge, this type of relationship has never been found before and presents another noticeable contribution of this study. Paranoia mediates the effects of these three factors but does not play a mediating role between privacy concerns and the attitude toward purchasing online. The exploratory study did not aim to elaborate deeper on this, but these findings suggest interesting directions for future studies. The relation of each factor under analysis (social media integration, cyber-fear, computer competence) with paranoia seems to be really promising, though might require additional theoretical justification and empirical testing.

We assumed that paranoia is an antecedent of the attitude towards online purchasing that has no direct influence on the intention to purchase online. However, empirical evidence has revealed a possibility that this influence might exist. Therefore, it is necessary to test it again on a larger sample in order to conclude whether this observation is a sample-specific case, or it suggests an alternative consideration on the role of paranoia in purchasing, thus inviting us to look for a different theoretical background.

Finally, a smaller and rather unexpected result has been observed in terms of the relation between cyber-fear and the attitude towards purchasing online. Since both paranoia and cyber-fear factors are associated, similar results were expected. However, the relation between cyber-fear and attitude toward purchasing online was positive, and therefore, rather contradictory. Such an unexpected result might be related to the nature of the cyber-fear measurement scale, which originally aims to capture the human attitudes towards the cyber-related threats that are likely to occur or are at least much more realistic in comparison to the cyber-paranoia dimension, which has also been developed by the same authors aiming to evaluate the “unrealistic fears concerning threats via information technologies whereby individuals perceive

themselves to be open to be ‘attacked,’ persecuted or victimized in some way (Mason et al., 2014). Due to this, cyber-fear might be related to the cognition of cyber-related threats, which may not have a negative influence on attitudes towards purchasing online. Obviously, this issue also requires further elaboration and should be addressed in future research.

In the scope of this dissertation, the overall findings of the first research have set the background for further analysis of exaggerated forms of distrust in the context of privacy-related behaviour. One of such privacy-related behaviours – willingness to disclose personal data online is explored in the following study.

2. WILLINGNESS TO DISCLOSE PERSONAL INFORMATION: HOW TO MEASURE IT?

The second article of the dissertation "Willingness to Disclose Personal Information: How to Measure It?" is published in the scientific journal "Engineering Economics". It conceptualizes the willingness to disclose personal data, assesses the ways how it is measured, and provides the modified scale of willingness to disclose personal data.

The aim and scope of the research. Willingness or unwillingness to disclose personal information has been a widely studied phenomenon as personal data is becoming increasingly important for many industries including marketing. Most of these studies treat the willingness to disclose personal information as a homogeneous construct. In many cases, it is measured by providing a number of personal information items and asking about the willingness to share them. Although recently there have been studies that find possible multidimensionality of the construct, most of them do not further elaborate on this possibility. Thus, the aim of this study is to modify the willingness to disclose personal data (WTD) construct and test its possible multidimensionality. Additionally, we aim to test the hypotheses on different types of relations between the disposition to value privacy, perceived regulatory effectiveness, privacy awareness, and various types/dimensions of the WTD construct.

Theory and hypotheses. Some authors have measured the willingness to disclose personal information in general, leaving for respondents to decide which specific data types and items might be requested (Kehr et al., 2015; Li, 2014; Wang et al., 2016), while other researchers have referenced only data categories, such as financial information, personal health information and other (Bansal et al., 2016). Malhotra et al. (2004) have used a rather simple and convenient 4-item scale to measure a general disposition to disclose personal information. However, one of the most common approaches tends to list specific data types/items and ask the respondents to evaluate their disclosure intention on an item-by-item basis (Gupta et al., 2010; Heirman et al., 2013; Malheiros et al., 2013; Norberg et al., 2007; Robinson, 2017; Treiblmaier & Chong, 2011; Walrave & Heirman, 2012). This approach goes back to the measurements used by Phelps et al. (2000) and Sheehan and Hoy (2000). Some of these authors treat the scale as a single dimension measure of willingness to disclose personal information (Robinson, 2017; Gupta et al., 2010), while others find various dimensions and different behaviours of consumers related to them (Phelps, 2000, Heirman et al., 2013).

This is justified by an increasing number of instances when personal data can be disclosed on the internet and a growing number of data types as well as multiple ways of data transfer. Therefore, the question of whether the willingness to disclose personal data is a homogeneous construct is challenged. It seems quite possible that the willingness to disclose personal data varies depending on the types of data to be disclosed and, consequently, various instances of the willingness should be studied individually.

We expect to find 3 dimensions of the willingness to disclose personal information: first – linked with the personal data that helps to identify a person and includes data items most frequently provided by an individual while browsing or purchasing online (name, address, e-mail, etc.); second – related to the information about an individual's social networking (such as social account information) and the third – related with the information collected online automatically, once permission is given (such as browsing history, location tracking, etc.). Correspondingly, this would mean three types of the willingness to disclose personal data: the willingness to disclose personal data (individual facts), the willingness to disclose personal data about social interactions, and the willingness to disclose personal data that are collected online. Thus, based on previous studies by Phelps et al. (2010), Heirman et al. (2013), Robinson (2017), we assume that the willingness to disclose personal data is not a homogeneous construct and develop the first hypothesis of the study:

H1: The scale that measures the willingness to disclose personal data has more than one dimension.

As three different types of the willingness to disclose personal data are expected to be discovered, we expect it to have a certain relation with the analysed antecedents: disposition to value privacy, perceived regulatory effectiveness and privacy awareness. The disposition to value privacy is the closest dispositional variable to the willingness to disclose personal data. Xu et al. (2008) defined the disposition to value privacy as an inherent need and trait which reflects the extent to which a person is inclined to maintain his/her personal information private *"across a broad spectrum of situations and persons"*, thus it reflects the individual's need to preserve his/her personal space, the importance put on his or her privacy and personal information. Xu et al. (2008) identified the disposition to value privacy as a "*cultural and personality characteristic*" and argues that the information disclosure decision depends on this trait. It has the most direct influence on the willingness to disclose personal information of all types because of its nature. Additionally,

it may moderate the influences of other factors. Therefore, the hypothesis follows:

H2: The disposition to value privacy will have a direct negative influence on all three dimensions of the willingness to disclose personal data.

The perceived regulatory effectiveness is linked with the situations where somebody perceives disclosing his/her personal information and relates this to the regulations of various forms of legislation, with an expectation that this information is protected (Miltgen & Smith, 2015). The considered types of data most commonly include individual characteristics and behaviours. Therefore, the perceived regulatory effectiveness is supposed to directly influence the willingness to disclose contact and profile information and online data but will not necessarily be related to the disclosure of social networking information. The following hypothesis was formulated:

H3: The perceived regulatory effectiveness will have a direct positive influence on the willingness to disclose personal data that include individual facts.

The awareness of privacy practices (privacy awareness) is a dispositional construct that reflects how an individual is aware of company practices, regulatory policies, and privacy-related matters in the society (Xu et al., 2008). Individuals who are highly aware of the issues 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 awareness of privacy practices has been found to be closely related to an individual's disposition to value privacy: it has been modelled as an antecedent of a disposition to value privacy and has been found to enhance this disposition in the e-commerce context. However, interestingly, it did not affect a disposition to value privacy in the social networking context (Xu et al., 2008). Privacy awareness is mainly linked with the disclosure of information that reflects the individual demographic characteristics of a person. Therefore, it should only directly influence the willingness to disclose personal data that include individual facts:

H4: Privacy awareness will have a direct positive influence on the willingness to disclose personal data that include individual facts.

Methodology. The quantitative research method is used to investigate the relationships between the variables. Data is collected via the internet survey and contained 439 respondents. All the items were measured on a 1-7 Likert scale. A 3-item scale of disposition to value privacy was originally developed by Xu et al. (2008). They found Cronbach's to be α=0.88. Later it

was adapted by Xu et al. (2011), Li (2014). The perceived regulatory effectiveness scale (3 items, α=0.83) was taken from Lwin et al. (2007) with a minor change that includes GDPR as an example. The privacy awareness scale (3 items) was taken from Xu et al. (2008). Later it was also used by Xu et al. (2011) and showed good reliability (α=0.865). The willingness to disclose personal data was measured by a scale adapted from Gupta et al. (2010) and Heirman et al. (2013) also used by Robinson (2017). It (with 14 items) showed good reliability in earlier studies (α = 0.87) and was the most relevant recent scale of this type (Robinson, 2017). In this study, the original list of items was reduced from 17 to 9 by removing those that were linked with entirely technical issues that would not be understood by the general population. However, the scale was amended with 5 items of personal data that are collected online automatically (on user consent). Kaiser-Meyer-Olkin's measure of sampling adequacy was 0.877, Bartlett's test of sphericity was significant (0.000), approx. Chi-square 7401.378 and df=496. The extracted factors explained 57.860 of the total variances.

Results. The first hypothesis H1 (The scale that measures the willingness to disclose personal data has more than one dimension) was tested based on exploratory factor analysis and subsequent confirmatory factor analysis. The average factor loadings (0.735, 0.683, 0.763) confirm the convergent validity, the correlations between factors (below 0.8) – discriminant validity. Additionally, these three variables have high reliability on their scales (Cronbach's α above 0.85). All this indicates that the three types of willingness can be measured as three separate variables and allows for confirmation of H1.

Hypothesis H2 (the disposition to value privacy will have a direct negative influence on all the three dimensions of the willingness to disclose personal data) is tested based on all the three causal models by checking the significance of the relation between the disposition to value privacy and corresponding types of WTD. In all the cases p=0.000; WTD_PD_IND β=-0.394; WTD_PD_SOC β=-0.273; WTD_OD β=-0.458. Therefore, H2 is confirmed.

Hypothesis H3 (the perceived regulatory effectiveness will have a direct positive influence on the willingness to disclose personal data that includes individual facts) is tested based on the causal model with the dependent variable. In this case β=0.097; p=0.045. H3 is confirmed.

Hypothesis H4 (privacy awareness will have a direct positive influence on the willingness to disclose personal data that includes individual facts, the perceived regulatory effectiveness will have a direct positive

influence on the willingness to disclose personal data that includes individual facts) is tested based on the causal model with the dependent variable. In this case β=0.158; p=0.004. H4 is confirmed.

Discussion and conclusions. The findings of the current survey support previous research carried out by Heirman et al. (2013). Factor analysis shows that there is more than one dimension in the willingness to disclose personal information construct. However, Heirman et al. (2013) distinguish 4 groups of personal data (although it is not based on any statistical model): identity data, geographical information, contact data, and profile data. We find slightly different dimensions based on factorial analysis, namely personal contact and profile information, social networking data and internet usage, and purchasing online information. Obviously, the consumers perceive personal data as a heterogeneous phenomenon with all the consequences of this fact.

The factor analysis not only shows the multidimensionality of the WTD construct. T-test analysis reveals that there is a significant difference between the average value of the three separate dimensions of willingness to disclose personal information. Test results (in both cases sig. <0.001) show that consumers are significantly more willing to disclose contact data and internet usage/purchasing information compared to social networking data. This supports the idea of differences in the perception of different types of personal information. It could be hypothesized that consumers perceive social networking data as more sensitive and intimate, therefore are consequently less willing to share it with others.

Further multidimensionality of the WTD construct is supported by a different pattern of relationship between the antecedents and WTD. The disposition to value privacy has a negative relation with all the three dimensions of WTD, while the perceived regulatory effectiveness does not have any influence on the case of social networking data (compared to a positive relationship in the other two cases), and the level of privacy awareness has a positive relationship with a willingness to disclose personal data only in the case of personal contact data disclosure (compared to no relationship in other two cases). Again, it could be hypothesized that consumers do not think that social networks could be effectively regulated by national or EU laws and, therefore, even better regulatory perception does not have a positive effect on the willingness to disclose this type of data. A positive relationship between privacy awareness (i.e., interest in privacy issues) and the willingness to disclose personal contact information shows that probably more educated consumers understand that this type of data is less sensitive compared to other types.

In the cases when the perceived regulatory effectiveness and privacy awareness have no direct impact on WTD, these variables influence WTD indirectly, via the mediation of the disposition to value privacy. Additionally, these two factors may have both direct and indirect effects on WTD. However, the most important observation is not the strength of these influences, but the existence of three different causal models when three types of WTD are considered. This additionally suggests that these three types of WTD may be assessed and analysed separately since they represent different aspects of willingness to disclose personal data. The final items of the WTD scale and its factor loadings are presented in Table 1.

Table 1. *Factor Loadings of Willingness to Disclose Personal Data (WTD)*

	Factor		
	1	2	**3**
Full name		0.794	
Address		0.625	
Mobile phone		0.739	
E-mail		0.797	
Birthday date		0.459	
LinkedIn account			0.759
Facebook account			0.653
Skype account			0.877
Internet browsing history and habits	0.754		
Geolocation data	0.635		
Online purchasing history and habits	0.926		
Information on searched goods	0.819		
IP address	0.543		
Means of the loadings	**0.735**	**0.683**	**0.763**

The main outcome of the study is the development of the modified WTD measurement tool and distinguishing its multidimensionality. This allows investigating the impact of exaggerated forms of distrust on the willingness to disclose personal data, which is the main objective of the following study.

3. FROM SOCIAL NETWORKING TO WILLINGNESS TO DISCLOSE PERSONAL DATA WHEN SHOPPING ONLINE: MODELLING IN THE CONTEXT OF SOCIAL EXCHANGE THEORY

The third study of the dissertation "From social networking to willingness to disclose personal data when shopping online: Modelling in the context of social exchange theory" is published in the scientific journal "Journal of Business Research". It applies the WTD measurement tool, which was modified in the second study of this dissertation and employs a novel approach toward the analysis of the willingness to disclose personal data.

The aims and scope of the research. Personal data disclosure online is frequently analysed by employing a cost-benefit analysis, which is applicable when personal information is treated as a commodity (Smith et al., 2011). This approach, known as privacy calculus, states that consumers disclose their personal information in exchange for benefits (Barth & de Jong, 2017; Robinson, 2017). However, the privacy calculus approach has been criticized for its overestimation of the rationality argument (Kehr et al., 2015; Wakefield, 2013) and is therefore hardly applicable when social networking is considered since the benefits of networking are not necessarily rational. This suggests that data disclosure on social networks is grounded on something other than just rationality (Zhang & Fu, 2020). Thus, the study approaches the willingness to disclose personal data in online environment from the position of Social Exchange Theory (SET), positioning social networking and online buying as the two types of social exchange. Since data disclosure in social networking and online buying is largely predicted by trust/distrust factors, the key antecedents of the current study include trust and paranoia (an extreme version of distrust). Perceptions regarding personal control over data disclosure and the effectiveness of legal regulations are two important mediators in modelling the relationship with willingness to disclose data (Lwin et al., 2007; Kehr et al., 2015, Miltgen & Smith, 2015). Based on a structural equation modelling, the study investigates the impact of involvement in social media on the willingness of consumers to disclose personal data in online purchasing.

Literature analysis and hypotheses. Based on SET, continuous non-formalized interactions of a reciprocal nature build trust between interacting parties, such as peers on social networks (Sherchan et al., 2013). Higher involvement in social networking requires more frequent disclosure of personal data, generates a higher level of trust among the participants

(Sherchan et al., 2013), and produces an overall higher level of engagement in a broader digital ecosystem, including online buying. This leads to the proposal that higher involvement in social networking positively influences the willingness to disclose personal data in a negotiated exchange, represented by e-buying.

H1: Involvement in social media positively influences the willingness to disclose personal data in e-commerce.

In negotiated interactions between a person and an institution, an individual may perceive an imbalance in the control over disclosed data (Sharma & Crossler, 2014). Understanding the terms and conditions of personal control over data disclosure allows the consumer to believe that somebody (legal systems, organizations) is efficient enough to warrant its proper use (Weil et al., 2005; Gefen & Pavlou, 2006). If a person perceives the regulations to be effective, the willingness to disclose personal information will increase. On the other hand, this does not offset all potential uncertainties, especially if the legal regulations or privacy policies are presented improperly (Meier, Schäwel & Krämer, 2020). It is typical that a person perceives a certain degree of lack of control over the process and over the provided data in online purchasing (Wang et al., 2016). Therefore, disclosure of data is linked with hesitations and uncertainties due to the perception that a person loses control over the data (Smith et al., 2011; Hong & Thong, 2013; Wang et al., 2016; Morimoto, 2020). Naturally, this perception reduces the willingness to disclose data. These arguments lead to the prediction that perceived regulatory effectiveness impacts the willingness to disclose personal data positively, while the perceived lack of control – negatively.

H2: Perceived regulatory effectiveness positively influences the willingness to disclose personal data in e-commerce.

H3: Perceived lack of control negatively influences the willingness to disclose personal data in e-commerce.

Control over the process of exchange can be shared not only with other participants of the exchange but also with the third parties regulating it. The legal systems and relevant institutions regulating privacy policies in online buying and selling take part in the control over the process (Gefen & Pavlou, 2006). This increases the perception that personal control over the exchange, which includes personal data disclosure, is rather limited.

H4: Perceived regulatory effectiveness positively influences the perceived lack of control.

To model how involvement in social media, perceived regulatory effectiveness, and perceived lack of control impact the willingness to disclose personal data, the influence of trust/distrust antecedents have to be predicted.

Trust is a key element of any type of a social exchange and stands at the very core of the concept of SET, which emphasizes the importance of trust as a predictor of social interactions that is developed in the process of social interactions (Molm et al., 2000). Therefore, the concept of trust needs to be understood in at least two different ways.

First, dispositional trust (propensity to trust something) is a human trait that is present in everyone to a certain degree (Frazier et al., 2013). This is a typical antecedent for the perceptions and activities regarding interactions with other people or their groups, institutions, regulatory systems, etc. (Bansal et al., 2016). Another form of trust – situational trust – expressed regarding concrete objects (most typical cases in marketing – types of stores, products, specific brands) occurs in specific situations or within a specific context (Heirman et al., 2013). Both types of trust typically encourage online behaviours, while privacy violations reduce trust and negatively impact future online activities (Martin, 2018).

Furthermore, both types of trust are well recognizable in the involvement in social networking: networking is triggered by the propensity to trust, and situational trust can be gradually developed during reciprocal exchanges in the process of interactions with social partners, as well as with social networking platforms (Molm et al., 2000; Sherchan et al., 2013). Since the level of trust in social networking predetermines the involvement in social media activities, the positive relation between the trust (propensity to trust) and involvement in social media may be predicted. Though the positive relationship between trust and involvement in social media seems rather clear, it remains an important aspect of research on privacy concerns and consumer trust in social media (Appel et al., 2020). Therefore, the hypothesis proposes:

H5: Trust positively influences involvement in social media.

The propensity to trust (trust trait) also predetermines the trust in institutions/regulatory systems and helps develop positive perceptions of them (Szymczak et al., 2016; Zhang et al., 2019). Therefore, trust should positively influence the perception of privacy regulation effectiveness.

H6: Trust positively influences perceived regulatory effectiveness.

However, it is inappropriate to assume that the consequences of trust on online behaviour are opposite to those of distrust (Chang & Fang, 2013). Instead, a separate assessment of the impact of distrust has to be made. This

is achievable with the use of the factor of paranoia, which is understood as an extreme form of distrust (Kramer, 2008).

Excluding clinical contexts, paranoia is a rather general irrational personal state grounded in the distrust of others (Gromann et al., 2013). Its impact on the analysed variables is largely unknown due to the limited scope of prior research. However, there are some insights that suggest initial ideas for analysis and allow for a prediction to be made about its relationships with the factors included in this study.

The relation between paranoia and social media use is rather unclear. Since paranoia means distrust of others, it should negatively influence one's social interactions (Jack & Egan, 2018). On the other hand, social media is the source of the clash of conflicting ideas, including ones that support paranoid thinking. Many studies have attempted to demonstrate the impact of social media use on risk for mental health symptoms and poor well-being (Naslund et al., 2020). However, a specific relationship with paranoia has not been detected (Bird et al., 2017; Berry et al., 2018). One of the arguments states that the relationship and causality were assessed in a wrong way, i. e., social media use was not a reason, but a consequence of paranoia (Bird et al., 2019). This confirms the directionality that is foreseen in the current study; however, it does not help in predicting whether the relationship is positive or negative.

The very concept of paranoia suggests that a person who is prone to paranoid thinking has a fear of missing out, and social media use provides rewarding experiences (Fuster et al., 2017). Paranoia should thus encourage social media use, which is an assumption supported by a rather limited scope of research that specifically analyses the impact of paranoia on social media involvement as it was enclosed in the second study of this dissertation. Therefore, we predict a positive influence of paranoia on the involvement in social media:

H7: Paranoia positively influences involvement in social media.

On the other hand, paranoid thinking generates feelings of personal vulnerability and exaggerated socially evaluative concerns (Meisel et al., 2018). Paranoid thinking is full of concerns about all kinds of possible imperfections in everything. There is fragmented evidence that paranoia is positively associated with the lack of personal control, but it is also strongly suggested to gain a better understanding of its impact on the various types of control (Imhoff & Lamberty, 2018). Therefore, we hypothesize:

H8: Paranoia positively influences perceived lack of control.

It is understood that paranoid individuals fail to correspond to any group in the wider society that shares coordinated aims and actions (Raihani

& Bell, 2019). Therefore, paranoid thinking gravitates toward ignoring and neglecting systems, rules, and organizational efforts with a dysregulated response (Saalfeld et al., 2018) and is prominently associated with low trust in the government (Imhoff & Lamberty, 2018). This leads to the neglect of the effectiveness of external regulations:

H9: Paranoia negatively influences perceived regulatory effectiveness.

Methodology. The analysis was carried out based on 480 respondents. All variables were measured using scales successfully deployed in former studies. Trust (TR) was assessed on a four-item "Propensity to Trust" scale (Frazier et al., 2013). Paranoia (PAR) was measured with the original paranoia trait scale (Fenigstein & Vanable, 1992), which was shortened to six items; shorter versions of this scale were successfully used in the first study of this dissertation. Involvement in Social Media (ISM) was measured following the Social Media Use Integration Scale (SMUIS) developed by Jenkins-Guarnieri et al. (2013). Measured with 10 items, it considers engaged social media use, emotional attachment to social media use, and the social habits of users. This allowed us to address important aspects of involvement in social media with a construct that stays unidimensional (Jenkins-Guarnieri et al., 2013). The Willingness to Disclose (WTD) personal data was assessed with the scale suggested by Gupta et al. (2010) and Heirman et al. (2013), later used by Robinson (2017). To avoid the effects of rapid dynamics in the types of data disclosed online, the list was reduced to items that are relatively stable and represent personal demographics and contact information (seven items). The Perceived Regulatory Effectiveness (PRE) three-item scale was adopted from Lwin et al. (2007) with a minor modification – GDPR, as an example of one type of legal regulation was included in one item. A three-item scale of Perceived Lack of Control (PLC) was taken from Wang et al. (2016). In all instances, a 1 to 7 Likert scale (1 = totally disagree and 7 = totally agree) was used. The scales were assessed using exploratory factor analysis, subsequent confirmatory factor analysis, and tests of reliability and validity. The exploratory factor analysis (Promax rotation, Maximum Likelihood extraction) was used for the initial assessment of the scales. The KMO was adequate (0.797) and Bartlett's Test of Sphericity showed approx. Chi-Square of 5727.640, with $df = 276$, $p < 0.001$. The model had a good fit, Chi-Square = 432.978, $df = 147$, $p < 0.001$, with extracted six factors that explained 59.93% of variation with cumulative initial Eigenvalues of 69.56%. A subsequent confirmatory factor analysis showed an acceptable fit of the model (CMIN/DF = 1.525; TLI = 0.947; CFI = 0.978; RMSEA = 0.033 (Byrne, 2010). This was achieved by reducing the ISM scale to six

items, PAR to three items, and WTD to five items. The reliability and validity of the obtained scales were assessed by measuring the composite reliability (above 0.70, Bagozzi & Yi, 2012). As recommended by the Fornell-Larcker criteria (Fornell & Larcker, 1981), all the standardized factor loadings exceeded 0.50; the average variance extracted (AVE) exceeded 0.50, and squared AVE values for each construct were greater than the correlation values of that construct. All these criteria were met, which allowed us to perform further analysis.

Results. As is typical in exploratory models that suggest using a new theoretical approach (SET), attention was paid primarily to the direct relationships between the factors. Therefore, these relationships are predicted in the formulations of the hypotheses. Based on them, the total and indirect (mediated) effects can be measured. The causal model (Fig. 2) tests the relationships that are predicted in the research model and confirms its structure. First, structural equation modelling assumes a correlation between the antecedents. In this model, this relationship confirms the correctness of the modelling assumption that propensity to trust and paranoia represent trust and distrust since their relationship is strongly negative (correlation −0.353; $p < 0.001$).

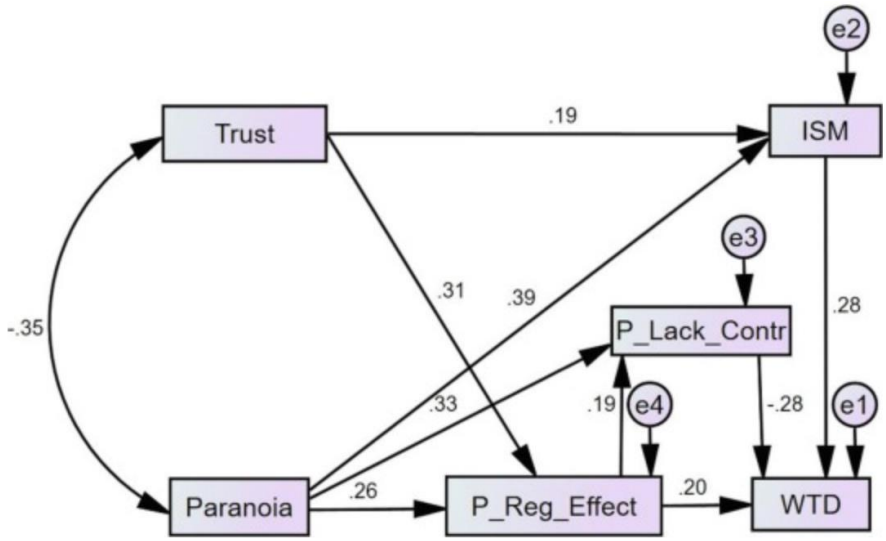

Figure 2. *Structural Model of Study 3*

All predicted direct relationships between variables are significant at the level of $p < 0.001$. Additionally, all standardized regression weights are

substantial, ranging from 0.19 to 0.39, which means a relatively high explanatory power of each individual direct relationship. However, this also allows for an analysis of all indirect and total effects, which additionally contribute to the understanding of how the willingness to disclose personal data is influenced by the analysed factors.

As it was modelled, trust and paranoia do not have direct effects on willingness to disclose personal data in e-shopping. The standardized total effect of trust is $\beta = 0.101$; $p < 0.001$; and the standardized total effect of paranoia is $\beta = 0.060$; $p < 0.001$. This confirms that the factor of trust/distrust is important in modelling willingness to disclose personal data based on SET. However, the positive total effect of paranoia is unexpected and largely predetermined by its positive (opposite to what was predicted) influence of paranoia on perceived regulatory effectiveness. This is discussed further in the text.

The influence of perceived regulatory effectiveness on willingness to disclose personal data is twofold: both direct and mediated, which means the presence of partial mediation. The standardized total effect is $\beta = 0.149$; $p < 0.001$; this is generated by the standardized direct effect of $\beta = 0.201$ ($p < 0.001$) and the standardized indirect effect of $\beta = -0.052$ ($p < 0.001$). The negative indirect effect is predetermined by the strong negative influence of the mediator (perceived lack of control) on the willingness to disclose data ($\beta = -0.277$ ($p < 0.001$).

An analysis of all direct relationships allows for the hypotheses to be tested (Table 1).

Table 2. *Tests of Hypotheses (Standardized Regression Weights)*

Hypothesized impacts				**Estimate**	**p**	**Result**
H1	**WTD**	←	**ISM**	0.271	0.000	Accepted
H2	**WTD**	←	**PRE**	0.166	0.000	Accepted
H3	**WTD**	←	**PLC**	-0.308	0.000	Accepted
H4	**PLC**	←	**PRE**	0.187	0.000	Accepted
H5	**ISM**	←	**TR**	0.204	0.000	Accepted
H6	**PRE**	←	**TR**	0.264	0.000	Accepted
H7	**ISM**	←	**PAR**	0.442	0.000	Accepted
H8	**PLC**	←	**PAR**	0.249	0.000	Accepted
H9	**PRE**	←	**PAR**	0.231	0.000	Rejected

Discussion and conclusions. This study's main contribution to the scope of knowledge about the willingness to disclose data online lies in the suggested use of SET as the background for the analysis and findings. The study revealed that reciprocal exchange (involvement in social media) strongly impacts the willingness to disclose personal data in negotiated exchange settings (buying online). This means that trust-generating reciprocal exchange increases the trust in another type of exchange and increases the willingness to disclose personal data there. Therefore, willingness develops throughout the entire digital ecosystem (Morgan-Thomas et al., 2020), and these findings extend previous knowledge in this area (Yang, 2019). Involvement in social media has no impact on willingness with the mediation of the perceived lack of control, which confirms that it influences willingness to disclose personal data only directly.

On the other side, willingness to disclose personal data was positively impacted by perceived regulatory effectiveness, as was expected based on former observations of the importance of legal assurance (Yamagishi & Yamagishi, 1994). Also, as was expected, willingness to disclose personal data was negatively impacted by the perceived lack of control, which represents uncertainties that are present in personal data disclosure situations and supports the earlier observations of Bansal et al. (2016) on the link between uncertainty avoidance and disclosure of personal data.

Both involvement in social media and perceived regulatory effectiveness had a strong impact from trust. This allows concluding that trust is an important antecedent of willingness to disclose personal data in buying online but impacts it indirectly via reciprocal interactions in social media and via the perception of the assurance of regulatory systems.

The dispositional antecedent that represents distrust (paranoia) was expected to positively influence involvement in social media and perceived lack of control, but negatively influence perceived regulatory effectiveness. The first two hypotheses have been confirmed; however, the relationship between paranoia and perceived regulatory effectiveness was significant but positive. This means that the assumptions used for grounding the hypothesis – paranoid people fail to coordinate their actions with wider groups and ignore rules and regulations (Saalfeld et al., 2018; Imhoff & Lamberty, 2018; Raihani & Bell, 2019) were not sufficient to predict the relationship. At the same time, the relationship between the two factors was significant, which confirms the correctness of the overall modelling, though it seems that this under-researched relationship should be grounded differently.

Paranoia includes not just the aspect of distrust, but also ideas about being harassed, threatened, harmed, persecuted, or mistreated by other people (Colby, 1981). This might mean that a person that exhibits paranoid thinking distrusts other people and looks for support against them in the regulations of legal bodies. Higher levels of paranoia might trigger a higher willingness to perceive that legal regulations might help in safeguarding against the negative intentions of "malevolent others". If this logic is correct, it would justify the positive relationship between paranoia and perceived regulatory effectiveness. However, this requires strong evidence from future studies.

Thus, the results of the study set the background for the final research whose main aim was to investigate a different form of exaggerated distrust in the willingness to disclose personal data online.

4. INFLUENCE OF TRUST AND CONSPIRACY BELIEFS ON THE DISCLOSURE OF PERSONAL DATA ONLINE

The fourth paper "Influence of Trust and Conspiracy Beliefs on the Disclosure of Personal Data Online" is published in the scientific journal "Journal of Business Economics and Management". The paper follows the same research path as in the previous study by exploring the role of conspiracy beliefs, as the form of exaggerated distrust, in the context of the willingness to disclose personal data.

The aims and scope of the research. The issue of trust-based personal data disclosure online remains of high importance both in social networking and online purchasing. Additionally, social networking is linked with a controversial factor of conspiracy beliefs that recently received attention because of the Covid-19 pandemic. Conspiracy beliefs trigger activities online but generate hesitations regarding rational ideas, requests, and procedures. Therefore, it is unclear how they impact rational requests for data disclosure in online shopping. The study aims to investigate how the influence of trust and conspiracy beliefs on self-disclosure in social networking and on willingness to disclose personal data in online purchasing can be modelled based on SET. The modelling of interactions employing SET is based on the third study of this dissertation. The model that is developed in the current study reflects a case of personal data disclosure and thus presents a novelty aspect among the applications of SET.

Literature analysis and hypotheses. Trust is an important antecedent of various behavioural intentions, and it is especially salient in social exchange relationships (Bernerth & Walker, 2009). Trust is also an essential factor for modelling numerous internet-based activities, including online transactions (Zhang et al., 2020). It is observed that online trust highly depends on past experiences with online activities (Chen et al., 2015; Dinev et al., 2006; Murphy, 2003) and develops over repeated interactions (Alarcon et al., 2018). When it comes to disclosure of personal data as a social exchange, trust plays the role that is of special importance, since it both creates and is created by the reciprocity of social exchange (Molm et al., 2000). When it regards transactions that require information, trust also is one of the major factors that encourages individuals to disclose information about themselves (Koohikamali et al., 2017). However, trust impacts the willingness to disclose information in online purchasing (negotiated exchange) not just directly. Since trust develops in the process of reciprocal social exchanges that are present in social networking, the growing involvement in social media

increases the level of personal disclosure in social networking. Additionally, self-disclosure is a result of trust-based perceptions about the safety of self-disclosure, which means that perceptions about the effectiveness of regulations mediate the impact of trust on self-disclosure. Thus, the total effects of trust on self-disclosure include its direct and all indirect impacts:
H1: Total effect of trust on self-disclosure in social networking is positive.

On the other hand, SET suggests that online selling also includes elements of reciprocity (Swoboda & Winters, 2021). Therefore, the above-mentioned effects of trust are also present in the process of data disclosure in online shopping. This is supported by the conceptual statement of SET developers that trust is important in both types of social exchange (Emerson, 1981). Again, this is applicable to the exchange of information: it is found that dispositional trust is one of the main predictors of the willingness to disclose personal data in online purchasing (Meinert et al., 2006; Keith et al., 2015). This is not limited to just the direct impact of trust on the willingness to exchange data. The impact of trust is often mediated by additional factors, two of them being extremely important. First, having limited relative power against an online store, an individual tends to rely on the additional assurance from third parties. Most typically, the role of a third party is played by legal systems, procedures, and institutions that look after the privacy issues in online activities as it was discovered in the first study of this dissertation. A positive perception on the effectiveness of regulations increases the relative power of individuals in their social exchange with online stores and contributes to willingness to disclose personal data online. For instance, the introduction of General Data Protection Regulation (GDPR) in 2018 increased buyers' sense of perceived security, third-party assurance, and perceived openness (Zhang et al., 2020). Therefore, the impact of trust on willingness to disclose personal data online is mediated by perceived regulatory effectiveness. Second, as it was disclosed in the first study of the dissertation, the willingness to disclose personal data in online purchasing is also positively impacted by other online activity: social networking. Social networking or the overall involvement in social media might seem not closely linked with activities in online shopping; however, SET helps to explain this relationship. The first study of the dissertation provides evidence that involvement in social media (reciprocal exchange) impacts the willingness to disclose data in online shopping (negotiated exchange). This even more strongly justifies both the direct and indirect impact of trust on willingness to disclose personal data in online shopping. Specifically, it means that the impact of trust on willingness to disclose personal data in online purchasing is mediated by factors that

represent activities in social networking and are reciprocal by their nature. Therefore, trust is expected to exert both direct and indirect positive impacts on willingness to disclose personal data in online purchasing:

H2: Total effect of trust on willingness to disclose personal data in online purchasing is positive.

Conspiracy beliefs refer to personal allegations that powerful groups or authorities are implementing misdemeanours or other unethical behaviours toward society and represent a form of distrust (van Prooijen & de Vries, 2016). Beliefs in conspiracies have been attracting the attention of researchers already for some time; however, the worldwide pandemic generated additional growth of interest in this phenomenon (Pellegrini et al., 2021). The nature of this factor suggests that people with a higher level of conspiracy beliefs should be cautious about disclosing their personal information. At the same time, people who believe in conspiracy theories tend to be involved in social networking to find support and confirmation for their beliefs (Allington et al., 2020; Goreis & Kothgassner, 2020). It is relevant to expect that conspiracy beliefs play a more and more important role in social networking and positively impact involvement in social media that is influenced by numerous factors of both dispositional and situational nature (Chung et al., 2019). This is additionally justified by the fact that some reasons for the involvement in social media might be triggered by rather unexpected personal characteristics or by the search for information on rather controversial ideas, including conspiracy theories (Allington et al., 2020). Additionally, involvement in social networks offers opportunities to interact with others sharing similar ideas regarding conspiracies (Allington et al., 2020). Therefore, conspiracy beliefs are expected to have a direct positive impact on involvement in social media. One of the reasons for involvement in social media includes the desire to preserve the social image and enhance it in the eyes of significant others (Douglas et al., 2019). Being noticed and 'visible' seems to be even more important to people who tend to represent original ideas, lifestyles, and beliefs (Bazarova & Choi, 2014). Therefore, conspiracy beliefs not just motivate to be active in social networking, but also stimulate conspiracy believers to self-disclose themselves to similar others in a more exaggerated way than typically. This justifies the proposition that conspiracy beliefs impact self-disclosure in social networking both directly and via the mediation of the involvement in social networking. We predict that the total effect of conspiracy beliefs on self-disclosure in social networking is positive:

H3: Total effect of conspiracy beliefs on self-disclosure in social networking is positive.

The link between conspiracy beliefs and willingness to disclose personal data in online purchasing is still largely unknown and represents a research gap. However, individuals with conspiracy beliefs typically are cynical about most regulations and express rather negative attitudes towards all kinds of authorities in general (Goreis & Voracek, 2019). Therefore, any regulated activity or request should be perceived by them negatively, and conspiracy beliefs should reduce the willingness to disclose personal data in all of them. Since the interaction between an individual and an online store is largely regulated, conspiracy beliefs should negatively impact the willingness to disclose personal data in online purchasing. The direct negative impact of conspiracy beliefs on the willingness to disclose personal data in purchasing lacks empirical evidence but is somehow predictable based on indirect considerations and logical arguments. However, the question of how conspiracy beliefs influence the willingness to disclose data in online purchasing is complicated by the fact that the willingness is also impacted by the effects of social networking. Since it is predictable that conspiracy beliefs impact activities in social networking positively, these may exert the further positive indirect effect of conspiracy beliefs on the willingness to disclose data in online purchasing. This positive indirect effect would conflict with the negative direct influence of conspiracy beliefs, and the direction of the total effect on the willingness to disclose data in online shopping appears unknown. The lack of empirical evidence does not make it possible to know whether the direct negative or indirect positive effect is to be stronger. We propose that the total effect of conspiracy beliefs will be negative, despite the existing indirect positive effects:

H4: Total effect of conspiracy beliefs on willingness to disclose personal data in online purchasing is negative.

Methodology. The study aims to assess the total effects of trust and conspiracy beliefs on self-disclosure in social media and on willingness to disclose personal data in online purchasing. The modelling is based on social exchange theory and includes two mediators: involvement in social media and perceived regulatory effectiveness.

Data were collected via the representative online survey and contained 1000 respondents. The survey is based on the questionnaire which included scales that have been successfully used in former studies. All items were measured on a 1-7 Likert scale. More specifically, the perceived regulatory effectiveness scale (3 items, α=0.83) was adapted from Lwin et al. (2007), with a minor alteration that included GDPR; the scale with this adaptation was successfully used in the first study of this dissertation. Trust

was assessed on a 4-item 'Propensity to Trust' scale (Frazier et al., 2013). The involvement in social media was measured with a 10-item scale (SMUIS) developed by Jenkins-Guarnieri et al. (2013) that includes engaged social media usage, emotional attachment to using social media, and social habits of users. Self-disclosure was measured with a 6-item scale, recently used by Jacobson et al. (2020). Willingness to disclose personal data (WTD) was assessed with the scale suggested by Gupta et al. (2010) and Heirman et al. (2013). Conspiracy beliefs were measured using the Brotherton et al. (2013) generic conspiracist beliefs scale. The scale was reduced to 7 items; two items were modified to include the two most recent conspiracy beliefs (vaccinations and 5G issues). Exploratory factor analysis (maximum likelihood; Promax rotation with Kaiser normalization) showed good sampling adequacy KMO= 0.897, Bartlett's test of sphericity was significant (0.000), approx. Chi-square 1555.330, df=345. The extracted factors explained 61.804 of the total variances (cumulative Eigenvalues 68.527). There were only 23 (4.0%) non-redundant residuals, which confirmed the adequacy. All loadings were above 0.5 (validity), at least 0.2 difference of variables in factors, and no more than 0.7 correlation between factors (the largest was 0.521), which refers to acceptable discriminant validity. A subsequent confirmatory factor analysis showed a good model fit: CMIN/DF=2.992; TLI rho2=0.948; CFI=954; RMSEA=0.045 (Byrne, 2010). Further validity check showed that in all instances average variance extracted (AVE) was >0.5, composite reliability (CR) >0.7, the root of AVE greater than correlations. A common latent bias test came back positive (difference in chi-square=518.8, difference in df=32, p=0.000), therefore the data imputation was performed with consideration of the common latent factor.

Results. The fit of the structural model (CMIN/DF=2.593; TLI=0.982; CFI=0.998; RMSEA=0.040) allowed testing the hypotheses (Figure 3).

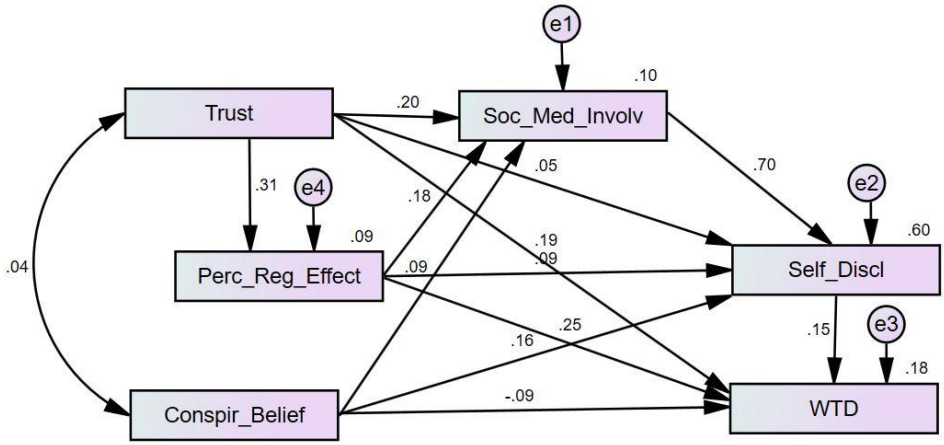

Figure 3. *Structural Model of Study 4*

The hypotheses were concentrating on the total effects of trust and conspiracy beliefs on self-disclosure in social networks and on willingness to disclose personal data in purchasing online. For this, the standardized total effects have been assessed. The total effects of trust on self-disclosure in social media were strong and positive, thus H1 was confirmed. Trust influenced self-disclosure in three different ways: directly, via the mediation of involvement in social media, and via the mediation of perceived regulatory effectiveness. Direct and indirect effects were positive and significant; however, the direct effect was weaker than the indirect one (β= 0.047 and β=0.204, respectively).

The total effect of trust on willingness to disclose data in online shopping was strong β= 0.304; the hypothesis H2 was confirmed. This influence was composed of the direct effect β= 0.191 and the indirect effect of β= 0.113, which is a sum of effects in four paths.

Hypothesis H3 predicted a positive total effect of conspiracy beliefs on self-disclosure in social networking. It was confirmed that the total effect is β= 0.242. It is made up of the direct effect of β= 0.160 and the indirect effect with the mediation of involvement in social media (β= 0.062). The most contradictory was the H4 hypothesis since it included aggregation of the direct negative and indirect positive effects of conspiracy beliefs on willingness to disclose data in online shopping. The analysis showed that the direct effect was negative β= -0.088 and relatively stronger than the indirect positive effect (β= 0.034), which resulted in a negative total effect of β= -0.054). Therefore, H4 was confirmed.

Discussion and conclusions. The study suggests several conclusions and managerial implications. First, the study confirms that the influence of trust factors on willingness to disclose personal data online can be successfully grounded on SET. This adds to the theoretical knowledge about SET applications in marketing research. Second, the results allow concluding that trust is a very important antecedent that positively influences both the data disclosure in social networking and the willingness to disclose personal data online. This is in line with former studies and with the conceptual framework of SET. Third, the study leads to a conclusion that conspiracy beliefs encourage involvement in social media and, consequently, the self-disclosure in social networking. However, in the case of the willingness to disclose personal data in online shopping, the positive effect that is mediated by self-disclosure in social networking is weaker than the negative direct effect of conspiracy beliefs. Therefore, the conclusion is that conspiracy beliefs negatively influence the willingness to disclose personal data in online shopping.

The study extends the model which was developed previously and investigates the impact of conspiracy belief (as a form of exaggerated distrust) on the willingness to disclose personal data in both reciprocal and negotiated contexts. Thus, the application of Social Exchange Theory regarding explaining the willingness to disclose personal data is supported.

CONCLUSIONS

The results of the four individual studies, conducted in the framework of this dissertation, allow making several conclusions.

First, it was confirmed that trust and distrust coexist as separate variables. More importantly, it was disclosed that distrust can be categorized into rational and irrational (i. e., exaggerated) forms. In addition, a set of conducted studies in the framework of this dissertation suggest that paranoia, cyber fear, and conspiracy beliefs are among these exaggerated forms of distrust. Moreover, it was disclosed that paranoia as an exaggerated form of distrust plays an important role in shaping the overall online consumer behaviour. These relationships were explored in the first study of the dissertation as it was found that paranoia plays a mediating role between social media use, cyber fear, computer competence, and online consumer behaviour (attitudes towards purchasing online and intention to purchase online).

Second, based on extensive theoretical analysis, the distinction between willingness and intention has been delineated. Willingness has been conceptualized as a factor of attitudinal nature, having elements of both dispositional and situational nature. The intention was defined as a clearly situational variable, predicting the behaviour in a specific context. Both seem to be predictors of actual disclosure behaviours, but the difference in this regard is a subject of further research. In addition, it was confirmed that the willingness to disclose personal data is a three-dimensional factor. These dimensions include individual facts, social networking data, and online purchasing data. In addition, it was found that customers perceive personal data differently and consider social networking data as more sensitive and intimate, thus they are less willing to share it with others. Finally, we suggest the existence of three different causal models when three types of WTD are considered. This allows us to additionally state that these three types of WTD may be assessed and analysed separately since they represent different aspects of willingness to disclose personal data. These findings are presented in the second study of the dissertation.

Third, the most noticeable novelty of the study was the use of social exchange theory to ground willingness to disclose personal data. This is done within the third and fourth studies of the dissertation. The potential of this theory in studies on privacy-related behaviour has been largely underutilized, and this gap was to some extent filled up within the set of studies of this dissertation. Based on the social exchange theory, data disclosure is an act of social exchange where one party (an individual) provides information in

exchange for various benefits. The theory allows considering the perceptions about the benefits, perceptions about the relative power of exchange participants, and many more. The concept of reciprocal and negotiated types of exchange was used to explain data disclosure in social media and online stores. This approach provides an explanation of the differences in willingness to disclose personal data in two instances and to find the relationship between them.

Fourth, as for the impact of different forms of exaggerated distrust, it was found that paranoia does not have a direct effect on willingness to disclose personal data, but instead, it has an indirect positive relationship (largely influenced by the positive influence on perceived regulatory effectiveness). A similar research approach is used in the last study of the dissertation, which investigates the impact of conspiracy beliefs on WTD. In contrast to the third study, a negative relationship was found, leading to the conclusion that different exaggerated forms of distrust play a distinctive impact on the willingness to disclose personal data, due to these factors being different in their nature.

Fifth, the study revealed that reciprocal exchange (involvement in social media) strongly impacts the willingness to disclose personal data in negotiated exchange settings (buying online). This means that trust-generating reciprocal exchange increases the trust in another type of exchange and increases the willingness to disclose personal data there. Therefore, willingness to disclose personal data develops throughout the entire digital ecosystem.

PRACTICAL IMPLICATIONS

The results of four articles covered in this dissertation suggest particular managerial recommendations:

1. Having observed a positive impact of perceived regulatory effectiveness on willingness to disclose personal data, the obvious suggestion for businesses would be to unambiguously support the presence of an effective regulatory system (national or international). Regulatory systems have to be reflected in policies of e-stores, and these policies need to be presented to the buyers in a short and clear manner (Meier et al., 2020). This is an important pre-requisite for the perception about the effectiveness of a regulatory system, which is a critical factor in willingness to disclose personal data.

2. Another important factor is perception about control over disclosed data. The perception about lack of control is partially offset by the effectiveness of legal regulations. However, it signals that businesses should use all available means to inform buyers about how they could control disclosed information, and in this way reduce the perception of lack of control. Providing clear information regarding personal data handling and inviting users to make decisions about how their information should be used would strongly increase overall willingness to share personal data.

3. Also, it seems that communication on social media is very suitable in terms of developing trust. Intensive use of social networks strongly increases willingness to disclose personal data outside of the networking context. Therefore, the suggestion for business is to integrate marketing activities with social media and invite users to connect to e-stores using social media accounts as often as possible.

4. Since a buyer's willingness to disclose their personal data is subject to their perceptions about regulation effectiveness and control, the population needs to be made aware to the highest possible level about their rights regarding privacy, as well as the mechanisms that regulate and control the use and sanction the misuse of personal data. That is why public policy should be strongly oriented toward educating consumers about regulatory systems.

5. The observed negative effects of conspiracy beliefs on willingness to disclose personal data in online shopping could be at least partially neutralized through social networking that represents a two-way communication and stands for reciprocal social exchange. This suggests that businesses may consider a closer integration between the sites of social networking and online shopping, since the trust in social networking positively impacts the data disclosure in shopping. Additionally, active

support to regulatory systems as well as active promotion of social networking that prompts self-disclosure of consumers should be an aim of organizations that want to encourage disclosure of consumer data.

RECOMMENDATIONS FOR FUTURE RESEARCH

The results of this dissertation generate the following recommendations for future scientific research:

1. To conduct exploratory research and test the model with both types of exaggerated distrust (paranoia and conspiracy beliefs) on the willingness to disclose personal data based on SET theory;
2. To investigate the impact of other existing forms of exaggerated distrust on the willingness to disclose personal data online that have not been analysed within the framework of this dissertation;
3. To further investigate the observed rather contradictory relationship between paranoia and attitudes towards purchasing online;
4. To conduct the research attempting to determine additional dimensions of the willingness to disclose personal information measurement;
5. To expand the research model by including additional dispositional variables, such as consumer scepticism, price sensitivity, and risk aversion, which could have possible implications in better explaining the consumer privacy-related behaviour online.

REFERENCES

1. Aghdam, N. H., Ashtiani, M., & Azgomi, M. A. (2020). An uncertainty-aware computational trust model considering the co-existence of trust and distrust in social networks. *Information Sciences, 513,* 465–503.
2. 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.
3. Alarcon, G. M., Lyons, J. B., Christensen, J. C., Bowers, M. A., Klosterman, S. L., & Capiola, A. (2018). The role of propensity to trust and the five factor model across the trust process. *Journal of Research in Personality, 75,* 69–82.
4. Allington, D., Duffy, B., Wessely, S., Dhavan, N., & Rubin, J. (2020). Health-protective behaviour, social media usage and conspiracy belief during the COVID-19 public health emergency. *Psychological Medicine, First View,* 1–7.
5. Appel, G., Grewal, L., Hadi, R., & Stephen, A. T. (2020). The future of social media in marketing. *Journal of the Academy of Marketing Science, 48*(1), 79–95.
6. Bagozzi, R. P. (1975). Social Exchange in Marketing. *Journal of the Academy of Marketing Science, 3*(2), 314–327.
7. Bagozzi, R. P., & Yi, Y. (2012). Specification, evaluation, and interpretation of structural equation models. *Journal of the Academy of Marketing Science, 40*(1), 8–34.
8. Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management, 53*(1), 1–21.
9. Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics, 34*(7), 1038–1058.
10. Bazarova, N. N., & Choi, Y. H. (2014). Self-disclosure in social media: Extending the functional approach to disclosure motivations and characteristics on social network sites. *Journal of Communication, 64*(4), 635–657.
11. Benamati, J. S., & Serva, M. A. (2007). Trust and distrust in online banking: Their role in developing countries. *Information technology for development, 13*(2), 161–175.

12. Bernerth, J., & Walker, H. J. (2009). Propensity to trust and the impact on social exchange. An empirical investigation. *Journal of Leadership & Organizational Studies, 15*(3), 217–226.
13. Berry, N., Emsley, R., Lobban, F., & Bucci, S. (2018). Social media and its relationship with mood, self-esteem and paranoia in psychosis. *Acta Psychiatrica Scandinavica, 138*(6), 558–570.
14. Bird, J. C., Evans, R., Waite, F., Loe, B. S., & Freeman, D. (2019). Adolescent paranoia: Prevalence, structure, and causal mechanisms. *Schizophrenia bulletin,* 45(5), 1134–1142.
15. Bird, J. C., Waite, F., Rowsell, E., Fergusson, E. C., & Freeman, D. (2017). Cognitive, affective, and social factors maintaining paranoia in adolescents with mental health problems: A longitudinal study. *Psychiatry research, 257,* 34–39.
16. Brotherton, R., French, C. C., & Pickering, A. D. (2013). Measuring belief in conspiracy theories: The generic conspiracist beliefs scale. *Frontiers in Psychology, 4,* 1–15.
17. Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science andTechnology, 58*(2), 157–165.
18. Chang, Y. S., & Fang, S. R. (2013). Antecedents and distinctions between online trust and distrust: Predicting high-and low-risk internet behaviors. *Journal of Electronic Commerce Research, 14*(2), 149.
19. Chen, Y., Yan, X., Fan, W., & Gordon, M. (2015). The joint moderating role of trust propensity and gender on consumer's online shopping behaviour. *Computers in Human Behavior, 43,* 272–283.
20. Cheng, J., Romero, D. M., Meeder, B., & Kleinberg, J. (2011). *Predicting reciprocity in social networks*. 2011 IEEE Third Int'l Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third Int'l Conference on Social Computing.
21. Chung, K. L., Morshidi, I., Yoong, L. C., & Thian, K. N. (2019). The role of the dark tetrad and impulsivity in social media addiction: Findings from Malaysia. *Personality and Individual Differences, 143,* 62–67.
22. Colby, K. M. (1981). Modeling a paranoid mind. *Behavioral and Brain Sciences, 4*(4), 515–534.
23. Dai, B. (2007). *The impact of online shopping experience on risk perceptions and online purchase intentions: the moderating role of product category and gender* [Doctoral dissertation, Auburn University].

24. Deutsch, M. (1973). *The resolution of conflict: Constructive and destructive processes*. Yale University Press.
25. Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for e-Commerce Transactions. *Information Systems Research 17*(1), 61–80.
26. Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce - A study of Italy and the United States. *European Journal of Information Systems*, *15*, 389–402.
27. Douglas, K. M., Uscinski, J. E., Sutton, R. M., Cichocka, A., Nefes, T., Ang, C. S., & Deravi, F. (2019). Understanding conspiracy theories. *Political Psychology*, *40*, 3–35.
28. Emerson, R. M. (1981). Social Exchange Theory. In M. Rosenberg, & R. H. Turner (Eds.), *Social Psychology: Sociological Perspectives* (pp. 30–65). Basic Books.
29. Fenigstein, A., & Vanable, P. A. (1992). Paranoia and self-consciousness. *Journal of Personality and Social Psychology*, *62*(1), 129–138.
30. Frazier, M. L., Johnson, P. D., & Fainshmidt, S. (2013). Development and validation of a propensity to trust scale. *Journal of Trust Research*, *3*(2), 76–97.
31. Freeman, D. (2007). Suspicious minds: The psychology of persecutory delusions. *Clinical Psychology Review*, *27*(4), 425–457.
32. Fuster, H., Chamarro, A., & Oberst, U. (2017). Fear of missing out, online social networking and mobile phone addiction: A latent profile approach. *Aloma*, *35*(1), 23–31.
33. Gefen, D., & Pavlou, P. (2006). An inverted-U theory of trust: The moderating role of perceived regulatory effectiveness of online marketplaces. *Information Systems Research, article* in advance, 1–20.
34. Goreis, A., & Voracek, M. (2019). A Systematic Review and Meta-Analysis of Psychological Research on Conspiracy Beliefs: Field Characteristics, Measurement Instruments, and Associations with Personality Traits. *Frontiers in Psychology*, *10*, 1–13.
35. Gromann, P. M., Heslenfeld, D. J., Fett, A.-K., Joyce, D. W., Shergill, S. S., & Krabbendam, L. (2013). Trust versus paranoia: Abnormal response to social reward in psychotic illness. *Brain*, *136*(6), 1968–1975.
36. Gupta, B., Iyer, L. S., & Weisskirch, R. S. (2010). Facilitating Global E-Commerce: A Comparison of Consumers Willingness to Disclose Personal Information Online in the US and in India. *Journal of Electronic Commerce Research*, *11*(1).

37. Heirman, W., Walrave, M., Ponnet, K., & Van Gool, E. (2013). Predicting adolescents' willingness to disclose personal information to a commercial website: Testing the applicability of a trust-based model. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 7*(3).
38. Hong, W., & Thong, J. Y. L. (2013). Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies. *MIS Quarterly, 37*(1), 275–298.
39. Huang, D. L., Rau, P. L. P., & Salvendy, G. (2010). Perception of information security. *Behaviour & Information Technology, 29*(3), 221–232.
40. Imhoff, R., & Lamberty, P. (2018). How paranoid are conspiracy believers? Toward a more fine-grained understanding of the connect and disconnect between paranoia and belief in conspiracy theories. *European Journal of Social Psychology, 48*(7), 909–926.
41. Jack, A. H., & Egan, V. (2018). Childhood bullying, paranoid thinking and the misappraisal of social threat: Trouble at school. *School Mental Health: A Multidisciplinary Research and Practice Journal, 10*(1), 26–34.
42. Jacobson, J., Gruzd, A., & Hernández-García, Á. (2020). Social media marketing: Who is watching the watchers? *Journal of Retailing and Consumer Services, 53*, 1–12.
43. Jenkins-Guarnieri, M. A., Wright, S. L., & Johnson, B. (2013). Development and validation of a social media use integration scale. *Psychology of Popular Media Culture, 2*(1), 38.
44. 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.
45. Keith, M. J., Babb, J. S., Lowry, P. B., Furner, C. P., & Abdullat, A. (2015). The role of mobile-computing self-efficacy in consumer information disclosure. *Information Systems Journal, 25*(6), 637–667.
46. Kim, J. B. (2012). An empirical study on consumer first purchase intention in online shopping: integrating initial trust and TAM. *Electronic Commerce Research, 12*(2), 125–150.
47. Kim, Y. A., & Ahmad, M. A. (2013). Trust, distrust and lack of confidence of users in online social media-sharing communities. *Knowledge-Based Systems, 37*, 438–450.

48. Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64,* 122–134.
49. Koohikamali, M., Peak, D. A. & Prybutok, V. (2017). Beyond self-disclosure: disclosure of information about others in social network sites. *Computers in Human Behaviour, 69,* 29–42.
50. Kramer, R. M. (2008). Organizational paranoia: Origins and dysfunctional consequences of exaggerated distrust and suspicion in the workplace. In *21st Century Handbook of Organizations: A Reference Handbook* (pp. 231–238). Sage Publications: Los Angeles, GA, USA.
51. Levi-Strauss, C. (1969). *The Elementary Structures of Kinship* (rev. ed.). Beacon.
52. Li, Y. (2014). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision Support Systems, 57,* 343–354.
53. 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.
54. Malheiros, M., Preibusch, S., & Sasse, M. A. (2013, June). *"Fairly truthful": The impact of perceived effort, fairness, relevance, and sensitivity on personal data disclosure.* In International Conference on Trust and Trustworthy Computing (pp. 250–266). Springer, Berlin, Heidelberg.
55. 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.
56. Martin, K. (2018). The penalty for privacy violations: How privacy violations impact trust online. *Journal of Business Research, 82,* 103–116.
57. Mason, O. J., Stevenson, C., & Freedman, F. (2014). Ever-present threats from information technology: the Cyber-Paranoia and Fear Scale. *Frontiers in Psychology, 5,* 1298.
58. Masur, P. K. (2019). The theory of situational privacy and self-disclosure. In Situational Privacy and Self-Disclosure, (pp. 131–182). Cham: Springer. https://doi.org/10.1007/978-3-319-78884-5
59. McKnight, D. H., & Chervany, N. L. (2001). Trust and distrust definitions: One bite at a time. *Trust in Cyber-societies* (pp. 27-54). Springer, Berlin, Heidelberg.

60. Meier, Y., Scha¨wel, J., & Kr¨amer, N. C. (2020). The shorter the better? Effects of privacy policy length on online privacy decision-making. *Media and Communication, 8*(2), 291–301.
61. Meinert, D. B., Peterson, D. K., Criswell, J. R., & Crossland, M. D. (2006). Privacy policy statements and consumer willingness to provide personal information. *Journal of Electronic Commerce in Organizations, 4*(1), 1–17.
62. Meisel, S. F., Garety, P. A., Stahl, D., & Valmaggia, L. R. (2018). Interpersonal processes in paranoia: A systematic review. *Psychological Medicine, 48*(14), 2299–2312.
63. Miltgen, C. L., & Smith, H. (2015). Exploring information privacy regulation, risks, trust, and behavior. *Information & Management, 52*(6), 741–759.
64. Molm, L., Takahashi, N., & Peterson, G. (2000). Risk and trust in social exchange: An experimental test of a classical proposition. *American Journal of Sociology, 105*(5), 1396–1427.
65. Moody, G. D., Galletta, D. F., & Lowry, P. B. (2014). When trust and distrust collide online: The engenderment and role of consumer ambivalence in online consumer behavior. *Electronic Commerce Research and Applications, 13*(4), 266-282.
66. Morahan-Martin, J., & Schumacher, P. (2007). Attitudinal and experiential predictors of technological expertise. *Computers in Human Behavior, 23*(5), 2230–2239.
67. Morgan-Thomas, A., Dessart, L., & Veloutsou, C. (2020). Digital ecosystem and consumer engagement: A socio-technical perspective. *Journal of Business Research, 121,* 713–723.
68. Morimoto, M. (2020). Privacy concerns about personalized advertising across multiple social media platforms in Japan: The relationship with information control and persuasion knowledge. *International Journal of Advertising,* 1–21.
69. Murphy, G. B. (2003). Propensity to trust, purchase experience, and trusting beliefs of unfamiliar e-commerce ventures. *New England Journal of Entrepreneurship, 6*(2), 53–64.
70. Naslund, J. A., Bondre, A., Torous, J., & Aschbrenner, K. A. (2020). SocialMedia and Mental Health: Benefits, Risks, and Opportunities for Research and Practice. *Journal of Technology in Behavioral Science, 5*(3), 245–257.
71. Nimrod, G. (2018). Technophobia among older Internet users. *Educational Gerontology, 44*(2-3), 148–162.

72. Nikkhah, H. R., Sabherwal, R., & Sarabadani, J. (2021). Mobile cloud computing apps and information disclosure: the moderating roles of dispositional and behaviour-based traits. *Behaviour & Information Technology,* 1–17.
73. Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs, 41*(1), 100–126.
74. Omrani, N., & Souli ́e, N. (2018). Individual, contextual and macro antecedents of online privacy concern: The case of data collection in Europe. *SSRN Electronic Journal.* Advance online publication.
75. Pellegrini, V., Giacomantonio, M., De Cristofaro, V., Salvati, M., Brasini, M., Carlo, E., ... & Leone, L. (2021). Is Covid-19 a natural event? Covid-19 pandemic and conspiracy beliefs. *Personality and Individual Differences*, 111011.
76. 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.
77. Raihani, N. J., & Bell, V. (2019). An evolutionary perspective on paranoia. *Nature Human Behaviour, 3*(2), 114–121.
78. Robinson, 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.
79. Saalfeld, V., Ramadan, Z., Bell, V., & Raihani, N. J. (2018). Experimentally induced social threat increases paranoid thinking. *Royal Society Open Science, 5*(8), 1–12.
80. Sharma, S., & Crossler, R. E. (2014). Disclosing too much? Situational factors affecting information disclosure in social commerce environment. *Electronic Commerce Research and Applications, 13*(5), 305–319.
81. Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing, 19*(1), 62–73.
82. Sherchan, W., Nepal, S., & Paris, C. (2013). A survey of trust in social networks. *ACM Computing Surveys, 45*(4), 47.
83. Simione, L., Vagni, M., Gnagnarella, C., Bersani, G., & Pajardi, D. (2021). Mistrust and beliefs in conspiracy theories differently mediate the effects of psychological factors on propensity for COVID-19 vaccine. *Frontiers in Psychology, 12.*
84. Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly, 35*(4), 989–1015.

85. Swoboda, B., & Winters, A. (2021). Effects of the most useful offline-online and online-offline channel integration services for consumers. *Decision Support Systems*, *145*, 113522.
86. Szymczak, H., Kücükbalaban, P., Lemanski, S., Knuth, D., & Schmidt, S. (2016). Trusting Facebook in crisis situations: The role of general use and general trust toward Facebook. *Cyberpsychology, Behavior, and Social Networking*, *19*(1), 23–27.
87. Treiblmaier, H., & Chong, S. (2011). Trust and perceived risk of personal information as antecedents of online information disclosure. *Journal of Global Information Management, 19*(4), 76–94.
88. Varey, R. J. (2015). Social Exchange (Theory). In C. L. Cooper, N. Lee & A.M. Farrell (Eds.), *Wiley Encyclopedia of Management.*
89. van Prooijen, J.-W., & de Vries, R. E. (2016). Organizational conspiracy beliefs: Implications for leadership styles and employee outcomes. *Journal of Business Psychology, 31*, 479–491.
90. van Scoy, L. J., Snyder, B., Miller, E. L., Toyobo, O., Grewel, A., Ha, G., Gillespie S., Patel M., Reilly J., Zgierska A. E., & Lennon, R. P. (2021). Public anxiety and distrust due to perceived politicization and media sensationalism during early COVID-19 media messaging. *Journal of Communication in Healthcare, 14*(3), 193-205
91. van Slyke, C., Shim, J. T., Johnson, R., & Jiang, J. J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems*, *7*(6), 16.
92. Wakefield, R. (2013). The influence of user affect in online information disclosure. *The Journal of Strategic Information Systems*, *22*(2), 157–174.
93. Walrave, M., & Heirman, W. (2012). Adolescents, Online Marketing and Privacy: Predicting Adolescents' Willingness to Disclose Personal Information for Marketing Purposes. *Children & Society, 38.*
94. Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management, 36*(4), 531–542.
95. Weil, D., Fung, A., Graham, M., & Fagotto, E. (2005). The effectiveness of regulatory disclosure policies. *Journal of Policy Analysis and Management, 25*(1), 155–181.
96. Wieringa, J., Kannan, P. K., Ma, X., Reutterer, T., Risselada, H., & Skiera, B. (2019). Data analytics in a privacy-concerned world. *Journal of Business Research, 122,* 915–925.

97. Xu, H., Dinev, T., Smith, H., & Hart, Paul J. (2008). *Examining the formation of individual's privacy concerns: Toward an integrative view*. ICIS 2008 Proceedings - Twenty Ninth International Conference on Information Systems.
98. Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems, 12*(12), 798–824.
99. Yamagishi, T., & Yamagishi, M. (1994). Trust and commitment in the United States and Japan. *Motivation and Emotion, 18*, 129–166.
100. Yang, X. (2019). How perceived social distance and trust influence reciprocity expectations and eWOM sharing intention in social commerce. *Industrial Management & Data Systems, 119*(4), 867–880.
101. Yoon, S. J. (2002). The antecedents and consequences of trust in online-purchase decisions. *Journal of Interactive Marketing*, *16*(2), 47–63.
102. Zarrad, H., & Debabi, M. (2012). Online purchasing intention: Factors and effects. *International Business and Management*, *4*(1), 37–47.
103. Zhang, J. Hassandoust, F., & Williams, J.E. (2020). Online customer trust in the context of the general data protection regulation (GDPR). *Pacific Asia Journal of the Association for Information Systems, 12*(1), 86–122.
104. Zhang, R., & Fu, J. S. (2020). Privacy management and self-disclosure on social network sites: The moderating effects of stress and gender. *Journal of Computer-Mediated Communication, 25*(3), 236–251.
105. Zhang, X. P., Cai, Y. L., & Zhao, L. (2019). *Analysis implications of general trust model on consumer's trust in CBEC sellers.* Proceedings of the 2nd International Workshop on Advances in Social Sciences (IWASS 2019).

INFORMATION ABOUT DOCTORAL STUDENT

Ignas Zimaitis is a junior assistant at the Faculty of Economics and Business Administration in Vilnius University and the assistant editor at the journal Organizations and Markets in Emerging Economies. Ignas is a member of The European Marketing Academy. His research interests include online consumer behaviour, paranoid consumer behaviour, and the implications of gamification in e-commerce. Ignas has publications in Journal of Business Research, Journal of Marketing Education, Engineering Economics, Journal of Business Economics and Management, and Sustainability. His conference papers were presented at EMAC regional and AMS conferences. He teaches Fundamentals of Marketing, Marketing, International E-marketing and E-commerce courses at the Faculty of Economics and Business Administration in Vilnius University.

INFORMACIJA APIE DOKTORANTĄ

Ignas Zimaitis yra Vilniaus universiteto Ekonomikos ir verslo administravimo fakulteto jaunesnysis asistentas ir žurnalo „Organizations and Markets in Emerging Economies" redaktoriaus asistentas. Ignas yra Europos rinkodaros akademijos („The European Marketing Academy") narys. Jo mokslinių interesų sritys - vartotojų elgsena internete, paranojiška vartotojų elgsena ir žaidybinių elementų naudojimas elektroninėje komercijoje. Ignas yra paskelbęs publikacijų žurnaluose „Journal of Business Research", „Journal of Marketing Education", „Engineering Economics", „Journal of Business Economics and Management" ir „Sustainability". Jo konferencijų pranešimai buvo pristatyti EMAC regioninėse ir AMS konferencijose. Ignas dėsto rinkodaros pagrindų, rinkodaros, tarptautinės el. rinkodaros ir el. komercijos kursus Vilniaus universiteto Ekonomikos ir verslo administravimo fakultete.

SANTRAUKA

Įmonių valdomi vartotojų asmens duomenys joms turi išskirtinę vertę, kadangi teisingas jų panaudijimas leidžia teikti individualiai pritaikytus rinkodaros pasiūlymus, kurti geresnę naršymo tinklapyje patirtį ir pan. (Zhang ir kt., 2020). Pasak Barth ir Jong (2017), klientai paprastai suasmenintus rinkodaros pasiūlymus suvokia kaip naudingus, tačiau daugeliu atvejų tokių pasiūlymų vertę vis dėlto nusveria tam tikri nuogąstavimai dėl atskleidžiamos asmeninės informacijos saugumo, todėl klientai iš esmės nėra linkę atskleisti savo duomenis pirkdami internetu (Wieringa ir kt., 2019). Nenoro atskleisti asmens duomenis internete priežastys sulaukia labai didelio mokslininkų dėmesio - šis reiškinys dažnai analizuojamas pasitelkiant privatumo skaičiavimo (angl. privacy calculus) teoriją, kurioje teigiama, kad klientai atskleidžia asmens duomenis mainais į gaunamą naudą (Robinson, 2017). Taikant privatumo skaičiavimo teoriją, vartotojų informacija traktuojama kaip prekė (Smith ir kt., 2011). Nors ši teorija labai dažnai naudojama su privatumu susijusiuose vartotojų sprendimų priėmimo tyrimuose, toks požiūris susilaukia nemažai kritikos dėl vartotojų racionalumo pervertinimo (Kehr ir kt., 2015). Kiti autoriai teigia, kad su privatumu susiję sprendimai grindžiami ne tik kaštų ir naudos analize, bet daugiausia yra situaciniai ir priklauso nuo informacijos atskleidimo tikslo ir konteksto (Omrani ir Souli'e, 2018; Masur, 2019). Be to, plačiai pripažįstama, kad su nenoru atskleisti asmens duomenis internete susiję ir įvairūs dispoziciniai veiksniai (Nikhhah, 2018), kurie taip pat nepatenka į privatumo skaičiavimo teorijos taikymo sritį.

Tarp tokių dispozicinių veiksnių, susijusių su privatumo elgsena, pasitikėjimas vaidina esminį vaidmenį (Kolokakis, 2018; Zhang ir kt., 2020). Nors pasitikėjimas kartais traktuojamas kaip kontinuumas, kai kurie mokslininkai teigia, kad žemiausias pasitikėjimo matavimo taškas nereiškia nepasitikėjimo (McKnight ir Chervany, 2001; Kim ir Ahmad, 2013, Aghdam ir kt., 2021). Šiam teiginiui pritaria Dinev ir Hart (2006) tvirtinantys, kad pasitikėjimas ir nepasitikėjimas egzistuoja kaip atskiri konstruktai, o pastarasis laikomas veiksniu, kur kas labiau veikiančiu vartotojų ketinimus (Moody ir kt., 2014). Kita vertus, nepasitikėjimas taip pat gali įgauti įvairias formas, nes yra teigiama, kad jį galima skirstyti į racionalų ir iracionalių (Deutsch, 1973). Racionalus nepasitikėjimas apibūdinamas kaip lankstus ir galintis keistis priklausomai nuo konkrečios situacijos; neracionalus – priešingai (Deutsch, 1973). Nors nepasitikėjimas plačiai analizuojamas vartotojų elgsenos kontekste, jo neracionalių (perdėtų) formų poveikis yra nepakankamai ištirtas.

Su perdėtu nepasitikėjimu susiję keli konstruktai, pavyzdžiui, technofobija (Nimrod, 2018), kibernetinė baimė (Mason ir kt., 2014) ir socialinis nerimas (Van Scoy ir kt., 2021), tačiau šioje disertacijoje dėmesys skiriamas kitiems perdėto nepasitikėjimo tipams - paranojai (Kramer, 2008) ir tikėjimu sąmokslo teorijomis (Simione ir kt., 2021). Šios dvi perdėto nepasitikėjimo formos pasirinktos dėl jų išskirtinumo – paranoja labiau siejama su neracionaliu nepasitikėjimu individais (Colby, 1981), o tikėjimas sąmokslo teorijomis - organizacijomis (van Prooijen ir de Vries, 2016). Tokiu požiūriu vadovaujamasi, nes jis leidžia ištirti šių dviejų skirtingų perdėto nepasitikėjimo formų poveikį norui atskleisti asmens duomenis skirtingomis aplinkybėmis, priklausomai nuo formalaus reglamentavimo lygio (lyginant elgseną socialiniuose tinkluose ir perkant internetu), kuris anksčiau mokslinėje literatūroje nebuvo analizuotas.

Apibendrinant atitinkamus šios srities mokslinius tyrimus, galima daryti išvadą, kad mokslinėje literatūroje yra didelių spragų, susijusių su noru atskleisti asmens duomenis internete. Pirma, anksčiau nėra buvę bandymų tirti su privatumu susijusią elgseną įvairiuose kontekstuose, priklausomai nuo jų išorinio formalaus reglamentavimo. Antra, nepakankamai ištirtas perdėtų nepasitikėjimo formų poveikis norui atskleisti asmens duomenis internete. Galiausiai, su privatumu susijusio elgesio tyrimuose taikomi keli teoriniai požiūriai, tačiau juose pernelyg pabrėžiamas racionalumo aspektas. Taigi tokios įžvalgos leidžia suformuluoti šios disertacijos **mokslinę problemą kaip klausimą**: koks yra perdėto nepasitikėjimo poveikis norui atskleisti asmens duomenis internete?

Šioje disertacijoje siūlomas naujas požiūris į privatumo elgsenos tyrimus, pasitelkiant socialinių mainų teoriją (angl. social exchange theory). Ši teorija stebėtinai retai pasitelkiama rinkodaros tyrimuose, nors pati rinkodaros esmė slypi santykiuose ir įvairiose socialinių mainų formose (Bagozzi, 1975; Varey, 2015). Socialinių mainų teorija individų ar įmonių sąveiką vertina kaip socialinių mainų, besiskiriančių savo formomis ir objektais, kuriais keičiamasi, seriją. Informacija (įskaitant asmens duomenis) yra vienas iš objektų, kuriais keičiamasi su kitais. Socialinių mainų teorija apima dvi dimensijas - abipusius ir derybinius socialinių mainų tipus (Lévi-Straus, 1969; Emerson, 1981). Derybinis mainų tipas pasireiškia, kai dalyvaujančios šalys iš anksto susitaria dėl mainų sąlygų ir jos iš esmės yra formalizuotos. Paprastai deramasi dėl mainų naudos ir kaštų, taip pat apsvarstomi reikalingi papildomi aspektai, pavyzdžiui, laikas ir pan. Pirkimo internetu situacijose paprastai vyksta tokia sąveika, todėl tai priskiriama derybinių socialinių mainų kategorijai (Molm ir kt., 2000). Abipusiai mainai

grindžiami abipuse mainų dalyvių sąveika, tikintis, kad partneris atsakys tuo pačiu (Cheng ir kt., 2011). Dėl mainų sąlygų nebūtinai iš anksto susitariama, jos nebūna formalizuojamos, todėl šio tipo mainai daugiausia grindžiami abipusiu pasitikėjimu (Molm ir kt., 2000). Veikla socialiniuose tinkluose yra geras abipusio keitimosi asmenine informacija su kitais pavyzdys (Yang, 2019). Keistis informacija socialiniuose tinkluose nebūtinai skatina racionalūs ar ekonominiai motyvai - žmonės dalijasi informacija socializacijos tikslais, siekdami pripažinimo, palaikymo ir kitos nematerialios naudos (Szymczak ir kt., 2016). Tuo remiantis, šioje disertacijoje socialinių mainų teorijos rėmuose tiriamas dviejų perdėto nepasitikėjimo formų (paranojos ir tikėjimo sąmokslo teorijomis) poveikis norui atskleisti asmens duomenis.

Taigi, disertacijos tikslas - nustatyti, kaip perdėtas nepasitikėjimas veikia norą atskleisti asmens duomenis internete.

Disertacijos tikslui pasiekti keliami šie uždaviniai:

1. Konceptualizuoti nepasitikėjimo fenomeną ir identifikuoti esamas perdėtas jo formas.
2. Įvertinti perdėto nepasitikėjimo poveikį bendrai vartotojų elgsenai internete.
3. Įvertinti, kokiais būdais galima konceptualizuoti ir išmatuoti norą atskleisti asmens duomenis.
4. Pagrįsti socialinių mainų teorijos taikymą, tiriant paranojos ir tikėjimo sąmokslo teorijomis, kaip perdėto nepasitikėjimo formų, poveikį norui atskleisti asmens duomenis internete.
5. Įvertinti paranojos ir tikėjimo sąmokslo teorijomis poveikį norui atskleisti asmens duomenis internete abipusių ir derybinių socialinių mainų aplinkoje.

Įgyvendindamas šiuos uždavinius, disertacijos autorius siekia apginti šiuos tyrimo teiginius:

1. Pasitikėjimas ir nepasitikėjimas egzistuoja kaip du skirtingi kontinuumai, o nepasitikėjimas gali būti skirstomas į racionalias ir perdėtas formas.
2. Paranoja (kaip perdėto nepasitikėjimo forma) atlieka svarbų vaidmenį formuojant bendrą vartotojų elgseną internete.
3. Noras atskleisti asmens duomenis yra daugialypis veiksnys - jį sudaro trijų rūšių asmens duomenų atskleidimas: individualūs faktai apie asmenį, socialinių tinklų duomenys ir pirkimo internetu duomenys.
4. Noras atskleisti asmens duomenis gali būti analizuojamas remiantis socialinių mainų teorija. Tiksliau, perdėtas nepasitikėjimas (paranoja ir

tikėjimas sąmokslo teorijomis) turi įtakos duomenų atskleidimo elgsenai tiek abipusių, tiek derybinių socialinių mainų kontekstuose.

Disertacijos tyrimai. Disertacija grindžiama keturiais straipsniais, publikuotais žurnaluose, kurie yra indeksuojami „Clarivate Web of Science Core Collection“ duomenų bazėje:

1 tyrimas. Pirmasis straipsnis „Social Media Use and Paranoia: Factors That Matter in Online Shopping“ publikuotas moksliniame žurnale „Sustainability“. Straipsnio bendraautoriai - doc. dr. Mindaugas Degutis ir prof. dr. Sigitas Urbonavičius. Disertacijos autoriaus indėlis rengiant šį straipsnį apima literatūros analizę, metodikos kūrimą, duomenų rinkimą ir pirmojo rankraščio projekto rengimą.

Tyrimas grindžiamas žvalgomuoju kiekybiniu tyrimu, kuriuo siekiama konceptualizuoti nepasitikėjimo reiškinį ir aptarti pasitikėjimo ir nepasitikėjimo kaip kontinuumo egzistavimą. Jame užpildoma esama teorinė spraga, analizuojant paranoją ir kibernetinę baimę kaip perdėtas nepasitikėjimo rūšis socialinių tinklų naudojimo, požiūrio į apsipirkimą internetu bei ketinimo pirkti internetu kontekste. Pagrindinė tyrimo prielaida yra ta, kad paranoja, kaip perdėto nepasitikėjimo forma, yra požiūrio į pirkimą internetu antecedentas. Tai patvirtinama atlikus empirinį tyrimą, pagrįstą struktūrinių lygčių modeliavimu: atlikus duomenų analizę paaiškėjo, kad paranoja yra svarbus požiūrio į pirkimą internetu antecedentas ir medijuoja ryšį tarp kompiuterinių žinių, kibernetinės baimės, socialinių tinklų naudojimo ir požiūrio į pirkimą internetu. Kadangi abu priklausomi kintamieji (požiūris į pirkimą internetu ir ketinimas pirkti internetu) neišvengiamai susiję su asmens duomenų atskleidimu, tyrimo rezultatai sudaro prielaidas tolesnei analizei, susijusiai su perdėto nepasitikėjimo formų galima įtaka labai specifiniam elgsenos internete aspektui - norui atskleisti asmens duomenis.

2 tyrimas. Antrasis straipsnis „Willingness to Disclose Personal Information: How to Measure It?“ publikuotas moksliniame žurnale „Engineering Economics“. Straipsnio bendraautoriai - doc. dr. Mindaugas Degutis, prof. dr. Sigitas Urbonavičius, doc. dr. Vatroslav Škare ir Dalia Laurutytė. Disertacijos autoriaus indėlis į šį straipsnį apima tyrimo metodikos parengimą, duomenų rinkimą, duomenų analizę ir rankraščio peržiūrą. Straipsnis turėjo du tikslus: pirma, konceptualizuoti noro atskleisti asmens duomenis internete fenomeną; antra, išsiaiškinti metodologinius klausimus, susijusius su noro atskleisti asmens duomenis matavimu. Vykdant pirmąjį uždavinį reikėjo atkreipti dėmesį į noro atskleisti asmens duomenis sąvoką ir suformuluoti jo savitumą, atskiriant jį nuo ketinimo atskleisti asmens duomenis. Antruoju uždaviniu siekta išsiaiškinti duomenų rūšis ir jų rinkimo

būdus bei aiškiai atskirti asmens atskleidžiamus duomenis, kuriuos renka kita keitimosi informacija dalis, ir elementus, susijusius su leidimais naudoti pateiktus duomenis. Šiam tikslui pasiekti buvo taikomas kiekybinis tyrimo metodas - siekiant išskirti noro atskleisti asmens duomenis konstrukto dimensijas, buvo atlikta faktorinė analizė, o struktūrinių lygčių modeliavimo metodas taikytas siekiant ištirti sąsajas tarp polinkio vertinti privatumą, suvokiamo reguliavimo veiksmingumo, privatumo suvokimo ir įvairių noro atskleisti asmens duomenis konstrukto dimensijų. Tyrimo rezultatai rodo, kad suvokiamas reguliavimo veiksmingumas ir privatumo suvokimas neturi tiesioginio poveikio norui atskleisti asmens duomenis – šie kintamieji daro įtaką netiesiogiai, medijuojant polinkio vertinti privatumą veiksniui. Visgi pagrindinė antrojo tyrimo išvada yra ta, kad noras atskleisti asmens duomenis yra susijęs su trijų rūšių duomenimis: noru atskleisti asmens duomenis, tokius kaip individualūs faktai apie asmenį, socialinių tinklų duomenis ir pirkimo internetu duomenis. Tokios išvados leido naudoti pakoreguotą noro atskleisti asmens duomenis matavimo instrumentą tolimesniuose tyrimuose, kuriuose nagrinėjama perdėto nepasitikėjimo formų įtaka norui atskleisti asmens duomenis internete.

3 tyrimas. Trečiasis straipsnis „From Social Networking to Willingness to Disclose Personal Data When Shopping Online: Modeling in The Context of Social Exchange Theory“ paskelbtas moksliniame žurnale „Journal of Business Research“. Straipsnio bendraautoriai - prof. dr. Sigitas Urbonavičius, doc. dr. Mindaugas Degutis, Vaida Kaduškevičiūtė ir doc. dr. Vatroslav Škare. Disertacijos autoriaus indėlį į šį straipsnį apima pirmojo literatūros analizės projekto parengimas, matavimo skalių parinkimas ir kritinė rankraščio peržiūra. Tyrimas grindžiamas kiekybiniu tyrimu, atliekant struktūrinių lygčių modeliavimą, siekiant nustatyti ryšius tarp išdėstytų veiksnių. Tyrime į norą atskleisti asmens duomenis internetinėje aplinkoje žvelgiama iš socialinių mainų teorijos pozicijos, naudojimąsi socialiniais tinklais ir pirkimą internetu traktuojant kaip dvi socialinių mainų rūšis. Kadangi duomenų atskleidimą socialiniuose tinkluose ir perkant internetu daugiausia lemia pasitikėjimo ir nepasitikėjimo veiksniai, pagrindiniai šio tyrimo antecedentai yra pasitikėjimas ir paranoja (kraštutinė nepasitikėjimo versija). Modeliuojant ryšį su noru atskleisti duomenis, kaip moderuojantys veiksniai pasirinkti suvokimas apie asmeninę duomenų atskleidimo kontrolę ir suvokiamas teisinio reguliavimo veiksmingumas.

Tyrimas atskleidė, kad abipusiai mainai (dalyvavimas socialinėje žiniasklaidoje) stipriai veikia norą atskleisti asmens duomenis derybinių mainų aplinkoje (perkant internetu). Tai reiškia, kad pasitikėjimą keliantys

abipusiai mainai didina pasitikėjimą derybiniais mainais pagrįstuose santykiuose ir didina norą juose atskleisti asmens duomenis. Todėl noras atskleisti asmens duomenis formuojasi visoje skaitmeninėje ekosistemoje.

Be to, nustatyta, kad pasitikėjimas veikia tiek socialinių tinklų naudojimosi intensyvumą, tiek suvokiamą reguliavimo veiksmingumą. Tai leidžia daryti išvadą, kad pasitikėjimas yra svarbus antecedentas, lemiantis norą atskleisti asmens duomenis perkant internetu, tačiau jis veikia netiesiogiai.

Be to, nors tikėtasi, kad paranoja, kaip perdėto nepasitikėjimo forma, teigiamai paveiks dalyvavimą socialiniuose tinkluose ir suvokiamą kontrolės stoką, tačiau neigiamai paveiks suvokiamą reguliavimo veiksmingumą, buvo patvirtintos tik pirmosios dvi prielaidos. Tuo tarpu ryšys tarp paranojos ir suvokiamo reguliavimo veiksmingumo buvo reikšmingas, bet teigiamas. Todėl galima teigti, kad tiek pasitikėjimas, tiek perdėta nepasitikėjimas daro teigiamą poveikį norui atskleisti asmens duomenis tarpusavio santykiuose (asmens duomenų atskleidimas socialiniuose tinkluose); taip pat duomenų atskleidimas socialiniuose tinkluose turi teigiamą poveikį norui atskleisti asmens duomenis perkant internetu. Taigi, tyrimo rezultatai sudarė prielaidas baigiamajam tyrimui, kurio pagrindinis tikslas buvo ištirti tikėjimo sąmokslo teorijomis, kaip perdėto nepasitikėjimo formos, įtaką norui atskleisti asmens duomenis internete.

4 tyrimas. Ketvirtasis straipsnis „Influence of Trust and Conspiracy Beliefs on the Disclosure of Personal Data Online“ paskelbtas moksliniame žurnale „Journal of Business Economics and Management“. Straipsnio bendraautoriai - prof. dr. Sigitas Urbonavičius, doc. dr. Mindaugas Degutis ir Vaida Kaduškevičiūtė. Disertacijos autoriaus indėlis rengiant šį straipsnį apima literatūros analizę, metodikos ir išvadų parengimą. Straipsnyje tęsiamas tas pats tyrimo kelias, kuris buvo nubrėžtas trečiajame šios disertacijos tyrime, ir toliau tiriamas perdėto nepasitikėjimo formų poveikis norui atskleisti asmens duomenis. Tyrimu siekiama išsiaiškinti, kaip, remiantis socialinių mainų teorija, galima modeliuoti pasitikėjimo ir tikėjimo sąmokslo teorijomis įtaką duomenų atskleidimui socialiniuose tinkluose ir norui atskleisti asmens duomenis perkant internetu. Siekiant įvertinti bendrą pasitikėjimo ir tikėjimo sąmokslo teorijomis poveikį duomenų atskleidimui socialiniuose tinkluose ir norui atskleisti asmens duomenis perkant internetu buvo pasitelktas struktūrinių lygčių modeliavimas. Be to, modeliuojant šių faktorių sąveiką, buvo nagrinėjama įsitraukimo į socialinius tinklus bei suvokiamo reguliavimo veiksmingumo, kaip medijuojančių ryšių, įtaka. Tyrimas patvirtino, kad pasitikėjimo-nepasitikėjimo veiksnių įtaką norui atskleisti asmens duomenis

internete galima sėkmingai pagrįsti socialinių mainų teorija. Tai papildo teorines žinias apie socialinių mainų teorijos taikymą rinkodaros tyrimuose. Be to, rezultatai leidžia daryti išvadą, kad pasitikėjimas yra labai svarbus antecedentas, darantis teigiamą įtaką tiek duomenų atskleidimui socialiniuose tinkluose, tiek norui atskleisti asmens duomenis internete. Tai atitinka ankstesnius tyrimus ir socialinių mainų teorijos koncepciją. Be to, tyrimas leidžia daryti išvadą, kad tikėjimas sąmokslo teorijomis skatina įsitraukimą į socialinius tinklus, taigi ir asmens duomenų atskleidimą socialiniuose tinkluose. Tuo pačiu, nepaisant to, kad nustatytas tiesioginis neigiamas tikėjimo sąmokslo teorijomis poveikis norui atskleisti asmeninius duomenis, bendras poveikis (medijuojamas savęs atskleidimo socialiniuose tinkluose ir dalyvavimo socialinėje žiniasklaidoje) yra teigiamas. Todėl galima daryti išvadą, kad tikėjimas sąmokslo teorijomis norą atskleisti asmens duomenis internete veikia šiek tiek kitaip nei paranoja, kurios įtaka nagrinėta trečiajame tyrime.

Apibendrinant galima teigti, kad ketvirtasis tyrimas išplečia modelį, kuris buvo sukurtas trečiajame disertacijos straipsnyje, ir tiria tikėjimo sąmokslo teorijomis (kaip perdėto nepasitikėjimo formos) poveikį norui atskleisti asmens duomenis tiek abipusiškumu, tiek derybiniais mainais pagrįstų santykių kontekste, taip patvirtinamas socialinių mainų teorijos taikymas aiškinant norą atskleisti asmens duomenis internete.

Išvados. Atliktų keturių atskirų tyrimų rezultatai leidžia daryti keletą išvadų. Pirma, buvo patvirtinta, kad pasitikėjimas ir nepasitikėjimas egzistuoja kaip atskiri, unikalūs kintamieji. Dar svarbiau, atskleista, kad nepasitikėjimą galima skirstyti į racionalias ir neracionalias (t. y. perdėtas) formas. Atlikti tyrimai šioje disertacijoje rodo, kad paranoja, kibernetinė baimė ir tikėjimas sąmokslo teorijomis yra vienos iš šių perdėtų nepasitikėjimo formų. Be to, buvo atskleista, kad paranoja, kaip perdėta nepasitikėjimo forma, atlieka svarbų vaidmenį formuojant bendrą vartotojų elgseną internete. Šie ryšiai buvo ištirti pirmajame disertacijos tyrime, nes nustatyta, kad paranoja atlieka medijuojantį vaidmenį tarp naudojimo socialiniais tinklais, kibernetinės baimės, kompiuterinių žinių ir vartotojų elgsenos internete (požiūrio į pirkimą internetu ir ketinimo pirkti internetu).

Antrajame tyrime, remiantis išsamia teorine analize, buvo nubrėžtas skirtumas tarp noro ir ketinimo atskleisti asmens duomens. Noras konceptualizuotas kaip požiūrio veiksnys, turintis tiek dispozicinio, tiek situacinio pobūdžio elementų. Tuo tarpu ketinimas buvo apibrėžtas kaip aiškiai situacinis kintamasis, numatantis elgesį konkrečiame kontekste, nepaisant to, kad abu šie veiksniai prognozuoja faktinį elgesį atskleidžiant

asmeninę informaciją. Be to, patvirtinta, kad noras atskleisti asmens duomenis yra trijų dimensijų veiksnys. Šios dimensijos apima individualius faktus, socialinių tinklų duomenis ir pirkimo internetu duomenis. Be to, nustatyta, kad vartotojai skirtingai suvokia asmeninius duomenis ir socialinių tinklų duomenis laiko jautresniais ir intymesniais, todėl mažiau linkę jais dalytis su kitais.

Trečia, vienas iš svarbiausių disertacijos rezultatų – patvirtintas galimas socialinių mainų teorijos taikymas, siekiant paaiškinti norą atskleisti asmens duomenis internete. Tai atlikta trečiajame ir ketvirtajame disertacijos tyrimuose. Socialinių mainų teorijos potencialas su privatumu susijusio elgesio tyrimuose iš esmės buvo nepakankamai išnaudotas, ir ši spraga buvo iš dalies užpildyta šios disertacijos tyrimuose. Remiantis socialinių mainų teorija tvirtinama, kad duomenų atskleidimas yra socialinių mainų veiksmas, kai viena šalis (asmuo) teikia informaciją mainais į įvairią naudą. Teorija leidžia atsižvelgti į vartotojų turimą suvokimą apie naudą, suvokimą apie santykinę mainų dalyvių galią ir kt. Siekiant paaiškinti duomenų atskleidimą socialinėje žiniasklaidoje ir internetinėse parduotuvėse, naudotasi abipusių ir derybinių mainų koncepcija. Šis požiūris leido paaiškinti noro atskleisti asmens duomenis skirtumus abiem atvejais, nagrinėjant duomenų atskleidimą naudojantis socialiniais tinklais bei perkant internetu, ir rasti jų tarpusavio ryšį.

Ketvirta, vertinant įvairių perdėto nepasitikėjimo formų poveikį, nustatyta, kad paranoja nedaro įtakos norui atskleisti asmens duomenis tiesiogiai, o turi netiesioginį teigiamą ryšį (daugiausia per teigiamą įtaką suvokiamam teisinio reguliavimo veiksmingumui). Panašus tyrimo metodas taikomas ir paskutiniame disertacijos tyrime, kuriame nagrinėjamas tikėjimo sąmokslo teorijomis poveikis norui atskleisti asmens duomenis. Skirtingai nei trečiajame tyrime, nustatytas neigiamas tiesioginis ryšys, leidžiantis daryti išvadą, kad skirtingos perdėto nepasitikėjimo formos daro savitą poveikį norui atskleisti asmens duomenis, nes šie veiksniai yra skirtingo pobūdžio.

Penkta, tyrimas atskleidė, kad abipusiai mainai (dalyvavimas socialiniuose tinkluose) stipriai veikia norą atskleisti asmens duomenis derybinių mainų aplinkoje (perkant internetu). Tai reiškia, kad pasitikėjimą keliantys abipusiai mainai didina pasitikėjimą kitos rūšies mainais ir didina norą juose atskleisti asmens duomenis. Todėl noras atskleisti asmens duomenis vystosi visoje skaitmeninėje ekosistemoje.

Praktinės rekomendacijos. Keturių disertacijoje nagrinėjamų straipsnių rezultatai leidžia pateikti konkrečias praktines rekomendacijas:

1. Pastebėjus teigiamą suvokiamo reguliavimo efektyvumo poveikį norui atskleisti asmens duomenis, akivaizdus siūlymas įmonėms būtų vienareikšmiškai remti veiksmingos reguliavimo sistemos (nacionalinės ar tarptautinės) veikimą: reguliavimo sistemos turi atsispindėti el. parduotuvių privatumo politikoje, o ši turi būti trumpai ir aiškiai pateikta pirkėjams.
2. Kitas svarbus veiksnys – vartotojo suvokimas apie atskleidžiamų duomenų kontrolę. Suvokimą apie kontrolės trūkumą iš dalies kompensuoja teisinio reguliavimo veiksmingumas, tačiau tai signalizuoja, kad įmonės turėtų naudoti visas turimas priemones, kad informuotų pirkėjus apie tai, kaip jie galėtų kontroliuoti atskleidžiamą informaciją, ir taip sumažinti suvokimą apie kontrolės trūkumą. Pateikus aiškią informaciją apie asmens duomenų tvarkymą ir pakvietus naudotojus priimti sprendimus dėl to, kaip turėtų būti naudojama jų informacija, labai padidėtų bendras noras dalytis asmens duomenimis.
3. Disertacijos tyrimų rezultatai rodo, kad vartotojų dalyvavimas socialiniuose tinkluose yra labai reikšmingas veiksnys pasitikėjimui ugdyti. Intensyvus naudojimasis socialiniais tinklais stipriai padidina norą atskleisti asmens duomenis už tinklo konteksto ribų. Todėl verslui siūloma integruoti rinkodaros veiklą su socialiniais tinklais ir, pavyzdžiui, kviesti vartotojus jungtis prie el. parduotuvių naudojantis socialinių tinklų paskyromis.
4. Kadangi vartotojų noras atskleisti savo asmens duomenis priklauso nuo jų suvokimo apie reguliavimo veiksmingumą ir kontrolę, vartotojai turi būti kuo geriau informuojami apie jų teises, susijusias su privatumu, taip pat apie mechanizmus, reguliuojančius ir kontroliuojančius asmens duomenų naudojimą ir sankcijas už netinkamą jų naudojimą. Todėl viešoji politika turėtų būti stipriai orientuota į vartotojų švietimą apie reguliavimo sistemas.
5. Dėl pastebėto neigiamo tiesioginio tikėjimo sąmokslo teorijomis poveikio norui atskleisti asmens duomenis apsiperkant internetu galima būtų bent iš dalies neutralizuoti naudojantis socialiniais tinklais, kurie yra pagrįsti abipuse komunikacija. Tai rodo, kad įmonės gali apsvarstyti galimybę glaudžiau integruoti socialinių tinklų svetaines ir apsipirkimą internetu, nes pasitikėjimas socialiniais tinklais teigiamai veikia duomenų atskleidimą apsiperkant. Be to, aktyvi parama reguliavimo sistemoms, taip pat aktyvus socialinių tinklų, skatinančių vartotojų saviraišką, propagavimas turėtų būti organizacijų, norinčių skatinti vartotojų duomenų atskleidimą, tikslas.

Rekomendacijos ateities tyrimams. Disertacijos rezultatai leidžia pateikti šias rekomendacijas būsimiems moksliniams tyrimams:

1. Atlikti žvalgomąjį tyrimą ir patikrinti kaip veikia modelis, kuriame kartu būtų nagrinėjama abiejų perdėto nepasitikėjimo formų (paranojos ir tikėjimo sąmokslo teorijomis) įtaka ketinimui atskleisti asmens duomenis internete.
2. Ištirti kitų perdėto nepasitikėjimo formų, kurios nebuvo analizuotos šios disertacijos rėmuose, poveikį norui atskleisti asmens duomenis internete.
3. Toliau tirti pastebėtą gana prieštaringą ryšį tarp paranojos ir požiūrio į pirkimą internetu.
4. Atlikti tyrimą, kuriuo būtų bandoma nustatyti papildomas noro atskleisti asmeninę informaciją matavimo dimensijas.
5. Išplėsti tyrimo modelį, įtraukiant papildomus dispozicinius kintamuosius, tokius kaip vartotojų skepticizmas, jautrumas kainai ir vengimas rizikuoti, kurie galėtų geriau paaiškinant su privatumu susijusią vartotojų elgseną internete.

LITERATŪROS SĄRAŠAS

1. Aghdam, N. H., Ashtiani, M., & Azgomi, M. A. (2020). An uncertainty-aware computational trust model considering the co-existence of trust and distrust in social networks. *Information Sciences, 513,* 465–503.
2. Bagozzi, R. P. (1975). Social Exchange in Marketing. *Journal of the Academy of Marketing Science, 3*(2), 314–327.
3. Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics, 34*(7), 1038–1058.
4. Cheng, J., Romero, D. M., Meeder, B., & Kleinberg, J. (2011). *Predicting reciprocity in social networks*. 2011 IEEE Third Int'l Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third Int'l Conference on Social Computing.
5. Colby, K. M. (1981). Modeling a paranoid mind. *Behavioral and Brain Sciences, 4*(4), 515–534.
6. Deutsch, M. (1973). *The resolution of conflict: Constructive and destructive processes*. Yale University Press.
7. Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for e-Commerce Transactions. *Information Systems Research 17*(1), 61–80.
8. Emerson, R. M. (1981). Social Exchange Theory. In M. Rosenberg, & R. H. Turner (Eds.), *Social Psychology: Sociological Perspectives* (pp. 30–65). Basic Books.
9. 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.
10. Kim, Y. A., & Ahmad, M. A. (2013). Trust, distrust and lack of confidence of users in online social media-sharing communities. *Knowledge-Based Systems, 37*, 438–450.
11. Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122–134.
12. Koohikamali, M., Peak, D. A. & Prybutok, V. (2017). Beyond self-disclosure: disclosure of information about others in social network sites. *Computers in Human Behaviour, 69*, 29–42.
13. Kramer, R. M. (2008). Organizational paranoia: Origins and dysfunctional consequences of exaggerated distrust and suspicion in the

workplace. In *21st Century Handbook of Organizations: A Reference Handbook* (pp. 231–238). Sage Publications: Los Angeles, GA, USA.
14. Levi-Strauss, C. (1969). *The Elementary Structures of Kinship* (rev. ed.). Beacon.
15. Mason, O. J., Stevenson, C., & Freedman, F. (2014). Ever-present threats from information technology: the Cyber-Paranoia and Fear Scale. *Frontiers in Psychology, 5,* 1298.
16. Masur, P. K. (2019). The theory of situational privacy and self-disclosure. In Situational Privacy and Self-Disclosure, (pp. 131–182). Cham: Springer. https://doi.org/10.1007/978-3-319-78884-5
17. McKnight, D. H., & Chervany, N. L. (2001). Trust and distrust definitions: One bite at a time. *Trust in Cyber-societies* (pp. 27-54). Springer, Berlin, Heidelberg.
18. Meier, Y., Scha¨wel, J., & Kr¨amer, N. C. (2020). The shorter the better? Effects of privacy policy length on online privacy decision-making. *Media and Communication, 8*(2), 291–301.
19. Molm, L., Takahashi, N., & Peterson, G. (2000). Risk and trust in social exchange: An experimental test of a classical proposition. *American Journal of Sociology, 105*(5), 1396–1427.
20. Moody, G. D., Galletta, D. F., & Lowry, P. B. (2014). When trust and distrust collide online: The engenderment and role of consumer ambivalence in online consumer behavior. *Electronic Commerce Research and Applications, 13*(4), 266-282.
21. Nimrod, G. (2018). Technophobia among older Internet users. *Educational Gerontology, 44*(2-3), 148–162.
22. Nikkhah, H. R., Sabherwal, R., & Sarabadani, J. (2021). Mobile cloud computing apps and information disclosure: the moderating roles of dispositional and behaviour-based traits. *Behaviour & Information Technology,* 1–17.
23. Omrani, N., & Souli´e, N. (2018). Individual, contextual and macro antecedents of online privacy concern: The case of data collection in Europe. *SSRN Electronic Journal.* Advance online publication.
24. Robinson, 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.
25. Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly, 35*(4), 989–1015.
26. Szymczak, H., Kücükbalaban, P., Lemanski, S., Knuth, D., & Schmidt, S. (2016). Trusting Facebook in crisis situations: The role of general use

and general trust toward Facebook. *Cyberpsychology, Behavior, and Social Networking, 19*(1), 23–27.

27. Varey, R. J. (2015). Social Exchange (Theory). In C. L. Cooper, N. Lee & A.M. Farrell (Eds.), *Wiley Encyclopedia of Management.*
28. van Prooijen, J.-W., & de Vries, R. E. (2016). Organizational conspiracy beliefs: Implications for leadership styles and employee outcomes. *Journal of Business Psychology, 31*, 479–491.
29. van Scoy, L. J., Snyder, B., Miller, E. L., Toyobo, O., Grewel, A., Ha, G., Gillespie S., Patel M., Reilly J., Zgierska A. E., & Lennon, R. P. (2021). Public anxiety and distrust due to perceived politicization and media sensationalism during early COVID-19 media messaging. *Journal of Communication in Healthcare, 14*(3), 193-205
30. Wieringa, J., Kannan, P. K., Ma, X., Reutterer, T., Risselada, H., & Skiera, B. (2019). Data analytics in a privacy-concerned world. *Journal of Business Research, 122*, 915–925.
31. Yang, X. (2019). How perceived social distance and trust influence reciprocity expectations and eWOM sharing intention in social commerce. *Industrial Management & Data Systems, 119*(4), 867–880.
32. Zhang, J. Hassandoust, F., & Williams, J.E. (2020). Online customer trust in the context of the general data protection regulation (GDPR). *Pacific Asia Journal of the Association for Information Systems, 12*(1), 86-122.

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to my academic supervisor and the co-author of the published studies Prof. Dr. Sigitas Urbonavičius, as the completion of this thesis could not have been possible without his inspiration, expertise, advice and patience. I also could not have undertaken this journey without the other co-authors of the published studies; thus, I am extremely grateful to Assoc. Prof. Dr. Mindaugas Degutis, Assoc. Prof. Dr. Vatroslav Škare, Vaida Kaduškevičiūtė and Dalia Laurutytė for all the ups and downs we had.

I am also very grateful to the Research Council of Lithuania for financial support, the anonymous reviewers of the published articles for valuable remarks, the administration of our faculty for their helpfulness and assistance, and all the members of the Marketing department for continuous encouragement.

Lastly, all of this would have been impossible without the support of my family and friends. A special thanks go my parents, my lovely wife Eglė, my daughter Agota and my companion Django. Finally, just a few words to my brother Andrius: it took me a while to catch up, huh?

PRESENTATIONS AND CONFERENCE PROCEEDINGS

1. Urbonavicius, S., & Zimaitis, I. The mediating role of paranoia on online consumer behaviour. 9th EMAC Regional Conference, Prague, Czech Republic, 12–14 September 2018.
2. Zimaitis, I., Degutis, M., Urbonavicius, S., & Kaduskeviciute, V. Impact of age on the willingness to disclose personal data in e-shopping. 11th EMAC Regional Conference, Zagreb, Croatia, 16-19 September 2020.
3. Urbonavicius, S., Laurutyte, D., Zimaitis, I., Kaduskeviciute, V., & Skare, V. Dispositional willingness to provide personal data online: antecedents and the mechanism. EMAC 2020 Annual Conference proceedings.
4. Skare, V., Urbonavicius, S., Degutis, M., Zimaitis, I., & Kaduskeviciute, V. Conspiracy beliefs and the disclosure of personal data online. 2021 International Conference on Technology and Entrepreneurship, Kaunas, Lithuania, 24-27 August 2021.
5. Zimaitis, I., Urbonavicius, S., & Kaduskeviciute, V. Modelling the willingness to disclose personal data in registration to online store on the basis of social exchange theory. 12th EMAC Regional Conference, Warsaw, Poland, 23-24 September 2021.

COPIES OF PUBLICATIONS

1. Zimaitis, I., Degutis, M., & Urbonavicius, S. (2020). Social Media Use and Paranoia: Factors That Matter in Online Shopping. *Sustainability, 12*(3), 904.

2. Degutis, M., Urbonavicius, S., Zimaitis, I., Vatroslav, S., & Laurutyte, D. (2020). Willingness to Disclose Personal Information: How to Measure It? *Engineering Economics, 31*(4), 487–494.

3. Urbonavicius, S., Degutis, M., Zimaitis, I., Kaduskeviciute, V., & Skare, V. (2021). From social networking to willingness to disclose personal data when shopping online: Modelling in the context of social exchange theory. *Journal of Business Research, 136*, 76-85.

4. Zimaitis, I., Urbonavičius S., Degutis, M., & Kaduškevičiute, V. (2022). Influence of Trust and Conspiracy Beliefs on the Disclosure of Personal Data Online. *Journal of Business Economics and Management, 23*(3), 551-568.

sustainability

MDPI

Article

Social Media Use and Paranoia: Factors That Matter in Online Shopping

Ignas Zimaitis *, Mindaugas Degutis and Sigitas Urbonavicius

Marketing Department, Faculty of Economics and Business Administration, Vilnius university, Vilnius LT-10222, Lithuania; mindaugas.degutis@evaf.vu.lt (M.D.); sigitas.urbonavicius@evaf.vu.lt (S.U.)

* Correspondence: ignas.zimaitis@evaf.vu.lt

Received: 19 December 2019; Accepted: 22 January 2020; Published: 26 January 2020

Abstract: The paper aims to explore the ways social media use is linked with paranoia, and how they influence buyers' attitudes and intentions in online shopping, thus shaping overall consumer behaviour. The theoretical analysis suggests that paranoia, being influenced by social media use, plays a noticeable role in the process of online shopping. The main assumption is that paranoia is an antecedent of the attitude towards online purchasing and mediates effects of other factors towards it. This is confirmed with SEM modelling on the basis of empirical data: the analysis provides evidence that paranoia is an important antecedent of the attitude towards purchasing online and mediates relationships between computer competence, cyber-fear, social media use and the attitude towards online shopping. Additionally, a contradictory relation between paranoia and online purchasing intention is observed. Overall, these findings disclose a new important factor in online shopping and outline several new directions for future research.

Keywords: social media; paranoia; online purchasing; computer competence; cyber-fear

1. Introduction

The development of digital technologies made social media use and online purchasing of products and services a daily routine for most of the people worldwide [1]. There is numerous evidence that engagement into social networks is linked with attitudes towards online purchasing or online purchasing behaviour [2,3]. One of the ways that could be considered in order to better understand the mechanism of the relation between participation in social networks and in online purchasing is to include a factor that has been somehow neglected in many previous studies–paranoia.

Paranoia is defined as "persecutory delusions, false beliefs whose propositional content clusters around ideas of being harassed, threatened, harmed, subjugated, persecuted, accused, mistreated, wronged, tormented, disparaged, vilified, and so on, by malevolent others, either specific individuals or groups" [4]. The mechanism of paranoia itself is frequently linked with the concept of distrust [5,6], which is conceptualized as a psychological state that is related to the lack of trustworthiness for others, caused by negative expectations and beliefs [7]. Emphasis is laid on the fact that distrust can be categorized into rational and irrational [8]. Rational distrust is described as being flexible and able to change depending on specific situations. Meanwhile, irrational distrust implies being inflexible and incapable to respond to the changing circumstances [8]. This specific type of distrust is associated with paranoid cognition and paranoid behaviour. A hierarchical structure of paranoia categorizes paranoia in terms of the level of intensity from the mildest, most common types, to most severe, less noticeable among the general population members [9]. This idea is supported by the statement that paranoid behaviour is not necessarily associated with the delusional distrust since it has developed as misperception and misjudgement [6] and is a common human experience [10]. Despite the fact that paranoia has been associated with a clinically diagnosable syndrome [11], recent developments

of paranoia studies have extended the scope of its research beyond clinical psychology. It is stated that a mild form of paranoia is a personality trait that can be observed among people without any medical indications [11,12]. This was supported by other scholars, confirming the existence of paranoia in non-clinical samples [9,13,14]. Therefore, paranoia should not be perceived as a mental disorder only, but also as "a part of a normally functioning human psychology" [15]. Based on the idea that paranoia does not exist on a dichotomous basis [16], we aim to explore paranoia as a continuum which is present to the general population.

Taking into consideration the fact that trust and distrust are widely accepted as being among the most important factors, influencing the online purchasing behaviour [17–20], with this exploratory study we aim to fulfil the existing research gap, by analysing paranoia as the extreme type of irrational distrust in the context of social media use and online shopping intentions. More specifically, we predict the presence of paranoia effect in online behaviours that are perceived by non-professional users as being complex, include unclear and sometimes hardly understandable functionalities and the lack of human interactions during the purchasing process. These types of situations are known as triggering uncertainties and distrust [21], but studies almost never reach towards an even more irrational factor—paranoia. People who intensively use social media or have higher general expertise in computer use may be less sensitive to these situations, thus factors of social media use and computer expertise may interact with paranoia and afterwards have not yet known effects in online shopping behaviour (specifically on attitude and intentions). These interactions are analysed together with the presence of cyber-fear, which is a factor of a similar nature with paranoia and privacy concern that is a typical negative antecedent of online behaviours [22]. Since the current knowledge on paranoia effects in online shopping remains very limited and fragmented, thus its analysis with the potential implications in explaining online consumer behaviour seems to be very promising both for scholars and for managers.

2. Theory and Hypotheses

2.1. Paranoia in Online Purchasing

Purchasing online is associated with a number of factors that are positively influencing purchase intentions, many of them are linked with various aspects of trust that acquire specific forms in online contexts. Consumer purchasing intention online can be directly influenced by the trust that is evoked by a website brand [18]. The trust of the platform is one of the three factors (others being satisfaction and awareness) that are the most important in predicting the consumer intention to purchase online [17]. On the other hand, there are factors that influence online purchasing intentions negatively, typically generating some form of distrust [23]. These factors pose a set of obstacles that reduce the use of electronic commerce. Trust and distrust coexist as separate constructs, however, distrust generally plays a much more important role in consumer intentions [20]. This is especially correct when different levels of risk (risk-linked factors) are present in online behaviours: trust has a stronger effect on low-risk behaviours, while distrust has a stronger negative impact on higher risk behaviours [19].

Discussing the more extreme form of distrust—paranoia—it has to be specified that this phenomenon is not only directed towards the other individuals but also towards the social groups and organizations [4], and, possibly, processes. Online processes and activities, as they include complex interactions between humans and IT systems, may evoke uncertainties and ambiguity, which may trigger irrational distrust in a form which could be considered as paranoid thinking. This is supported by evidence of the existing positive relationship between internet use frequency and general trait paranoia [22]. The possible implications of paranoia on consumer behaviour online are also supported by the suggestion, that paranoid thinking is associated with the subliminal advertising phenomena—while customers tend to have a specific set of fears towards the advertising itself, their thinking that someone is potentially playing with their minds, evoke the irrational response, consumer paranoia [24]. This can be explained through the nature of paranoia, which is considered to be a natural

reaction towards the uprising social threats [15]. In such circumstances, paranoia may play a particular role in specific internet-based activities, such as online shopping, as electronic purchasing is almost always associated with specific fears and risks which customers are perceiving [25]. Finally, this allows an assumption to be made that paranoia, a factor that represents a set of irrational risks and extreme forms of distrust, may be one of the antecedents of the attitude towards e-purchasing, able to influence the attitude negatively:

H1: Paranoia has a direct negative influence on attitude towards purchasing online.

If paranoia is an antecedent of the attitude, both the theory of reasoned action and theory of planned behaviour [26,27] suggest that it should not have a direct influence on the intention. This influence has to be mediated by the attitude. Based on this solid background we cannot predict the direct relationship between an antecedent (paranoia) and the intention. Instead, this relationship has to be indirect, mediated by the attitude:

H2: Paranoia has no direct impact on intention to purchase online.

H3: Paranoia has an indirect negative impact on intention to purchase online when the relationship is mediated by an attitude towards purchasing online.

2.2. Privacy Concern and Cyber-Fear

In the context of online activities, distrust is associated with other negative factors. All they root from a broad background of the privacy concerns and related risks. The phenomenon of privacy concern in buyer behaviour is mainly linked with the awareness of privacy-related issues which include the disclosure of personal information to third parties [28]. A large number of studies agree on a strong negative influence of the privacy concern on the extent of various internet-related activities [29–31]. Purchasing online is among them—the risk of privacy loss online is negatively related to the purchasing intention [32]. The influence of the perceived threats may be so strong that individuals may feel an overall fear to perform digital activities, and this may be defined as cyber-fear [22]. The concept of cyber-fear is new and understudied. However, it has been disclosed that the technology awareness, experience of using the internet (internet use by years), frequency of internet use has a significant negative impact on cyber-paranoia [22].

The next issue in determining the role of paranoia in online shopping is finding its place among factors that measure privacy concerns and risks. These factors themselves may have a direct influence on the attitude towards purchasing online [33,34]:

H4: Cyber-fear has a direct negative impact on the attitude towards purchasing online.

H5: Privacy concern has a direct negative impact on the attitude towards purchasing online.

Cyber fear by its essence is a close factor to paranoia. Though the direction of their interaction requires further discussion, we assume that cyber fear also has an indirect influence on the attitude:

H6: Cyber-fear has an indirect negative impact on the attitude towards purchasing online when the relationship is mediated by paranoia.

2.3. Social Media Use and Computer Competence

People who use social media frequently, receive unexpected suggestions or recommendations, depending on their previous interactions, preferences and likes. These instances have obvious explanations on the basis of used programming algorithms, however, they may seem unclear and even threatening to the general population, since typical users cannot be professionally aware of the technical side of how internet-based social networks are working. Intensive use of social media increases the number of such interactions, and therefore increases the opportunity of paranoid cognition. In this case,

social media use integration shall have an indirect (mediated by paranoia) influence on the attitude towards online purchasing. However, there is no theoretical or empirical evidence that could allow predicting the valence of this relationship, since the relation between the social media use integration and paranoia is expected to be positive, while the relation between paranoia and the attitude – negative. Since the latter is stronger justified, we hypothesize as follows:

H7: Paranoia mediates a negative impact of social media use integration on the attitude towards purchasing online.

Computer competency is directly reflecting the buyer's experience and skills working with the computers [35]. In the context of online shopping, there is strong evidence that computer competence significantly enhances purchasing online [36,37]. Moreover, a positive impact of the level of internet usage on purchasing behaviour is discovered [38,39]. One of the factors representing one's involvement with computers is the extent of social media use, which is claimed to have a positive impact on the intention to purchase online [2]. The intensity of social media use may be measured using several variables (duration, frequency, etc.), but a more comprehensive assessment is achieved via measuring social media use integration, which refers to the involvement and emotional connection to the social network usage [40].

Continuing a similar logic as with the hypotheses on social media use, we state that competent users should have answers to many of unexpected occurrences during the internet-based activities. Therefore, computer competence seems not likely to have a relation (at least—positive) with paranoia. However, computer expertise allows us to know how much tracking may be done on the internet, and how badly this accumulated knowledge may be used by somebody with bad intentions [41]. As a result, the increase in computer expertise may develop a paranoid cognition. As in the case of social media use, we may predict a negative influence of computer competence on the attitude, if mediated by paranoia:

H8: Computer competence has an indirect negative impact on the attitude towards purchasing online when the relationship is mediated by paranoia.

In addition, it is expected that computer competence should have a positive influence on the attitude towards purchasing online:

H9: Computer competence has a direct positive impact on the attitude towards purchasing online.

3. Materials and Methods

3.1. Participants and Procedure

The aim of this research is to determine the role of paranoia on the relationships between social media use, cyber-fear, computer competence, privacy concern, attitude towards purchasing online and online purchase intention. The quantitative research method is used to investigate the relationships between the variables. Data is collected via the internet survey. The analysis is based on 287 respondents from Lithuania. The largest proportion of respondents consisted of 18–35 age group, making 95.8% of the total sample. Since the intention to purchase online is the dependent variable of this research, the target population of this research can be a population that is most likely to do online shopping, thus the 18–35 age group was specifically targeted since it is claimed to be the most active internet users group in Lithuania [42]. In addition, 77.8% of the respondents were graduates of higher education institutions, 65.9% of the sample were women.

3.2. Measures

To measure the trait paranoia, a 5-point, 20 items Likert type general paranoia scale, developed by Fenigstein and Vanable was used [11], which is widely accepted as a measurement tool, allowing to capture the paranoia in non-clinical samples. The cyber-fear was measured using 5-point, 11 items

Likert type cyber paranoia and fear scale, developed by Mason, Stevenson and Freedman which had been originally reported to be loading on two factors–cyber paranoia and cyber-fear [22]. In the scope of this research, the cyber-fear factor was utilized and taken into consideration. The following factor, the privacy concern was measured by 5-point 16 items Likert type attitudinal scale, evaluating the scope of general concerns about privacy on the Internet [28]. The social media use was measured by employing the social media use integration scale (10 items on a 7-point scale) to assess the involvement and emotional connection to the social networks [40]. Computer competence was measured using 4 items on a 5-point Likert type Internet and computer comfort/competency scale, which is linked with the extent of the computer and Internet skills [35]. The attitude towards purchasing online (10 items on a 5-point Likert type scale) and online purchasing intention (4 items on a 5-point Likert type scale) were taken from a similar study [43].

An exploratory factor analysis with a maximum likelihood extraction and Promax with Kaiser normalization rotation allowed the extraction of 7 factors that explained 60.5% of the variance. The KMO value was 0.815 (> 0.7) and the Bertlett's Chi-square value resulted at 5217.930 ($p = 0.00$) and demonstrated the sample adequacy and applicability for the analysis. 27 non-redundant residuals equalled to 5%, which was an acceptable result for the adequacy. All correlations between the factors were below 0.7 what suggested an acceptable discriminant validity. All the factor loadings were above 0.5 (Table 1).

Table 1. Factor Matrix.

	Factor						
Item	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Attitude_online_p_1						0.830	
Attitude_online_p_4						0.649	
Attitude_online_p_5						0.816	
Attitude_online_p_7						0.828	
Competence_1				0.721			
Competence_2				0.727			
Competence_3				0.879			
Competence_4				0.835			
Privacy concern_11		0.799					
Privacy concern_12		0.921					
Privacy concern_13		0.928					
Privacy concern_15		0.654					
Privacy concern_16		0.553					
Paranoia_3					0.739		
Paranoia_4					0.711		
Paranoia_5					0.689		
Paranoia_6					0.693		
Paranoia_7					0.680		
Cyber_fear_2							0.691
Cyber_fear_3							0.692
Cyber_fear_4							0.662
Soc_media_use_1	0.658						
Soc_media_use_2	0.671						
Soc_media_use_3	0.822						
Soc_media_use_4	0.868						
Soc_media_use_5	0.625						
Soc_media_use_6	0.785						
Onl_purch_int_1			0.782				
Onl_purch_int_2			0.837				
Onl_purch_int_3			0.935				
Onl_purch_int_4			0.891				

The CFA analysis required further modifications of the scales, since a validity and reliability check resulted in AVE measure scored 0.457 (< 0.5) on a cyber-fear scale. After the deletion of cyb_fear_1 item, all AVE measures scored > 0.5, CR scored > 0.7 and the root of AVE was greater than correlations.

The common latent bias test came back positive, showing the Chi-square unconstrained value as 584.9, the Chi-square constrained value—499.4, the df unconstrained value—406, the df fully constrained value—375. Cronbach's alpha values for each scale were > 0.7, indicating a good level of scales reliability. More specifically: attitude towards online purchasing: 0.867, computer competence: 0.865, privacy concern: 0.892, paranoia: 0.830, cyber-fear: 0.778, social media use: 0.879, online purchasing intention: 0.911.

4. Results

The hypotheses of the research were tested using the structural equation analysis, estimating the path coefficients for each relationship. The acceptable level of model fit was confirmed, measuring the following values: $\chi 2$ (278) = 584.9, CMIN=499.442, DF=375, CFI=0.974, TLI =0.968, RMSEA=0.034.

In total, 9 hypotheses were tested, seven of them were accepted. The research model with regression weights is presented in Figure 1.

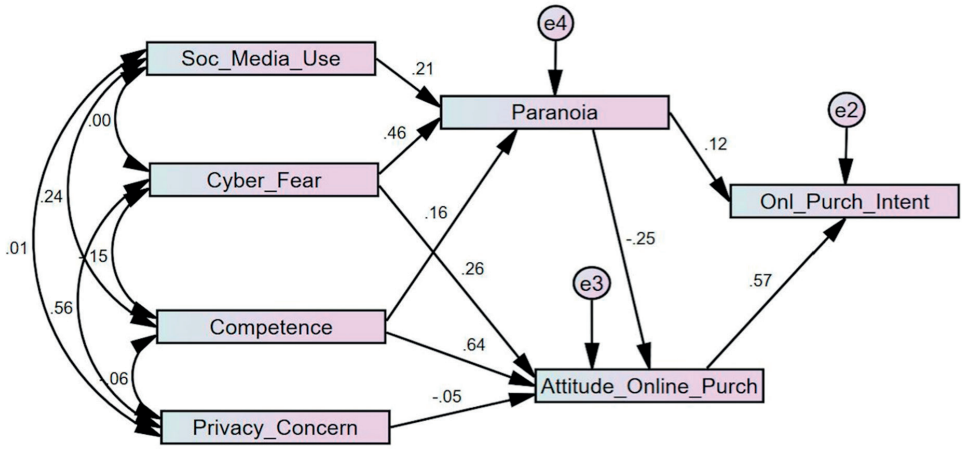

Figure 1. Research model.

H1 hypothesis states that paranoia has a direct negative influence on the attitude towards purchasing online. The regression analysis shows a significant negative relationship between paranoia and the attitude towards purchasing online (β=−0.306, p=0.000), thus H1 is accepted. The results of the direct effects are presented in Table 2.

Table 2. Regression weights.

			Regression Weights	S.E.	C.R.	p
Paranoia	←	Cyber fear	0.417	0.046	8.990	***
Paranoia	←	Social media use integration	0.089	0.022	4.010	***
Paranoia	←	Computer competence	0.211	0.071	2.973	0.003
Attitude towards purchasing online	←	Privacy concern	−0.053	0.057	−0.919	0.358
Attitude towards purchasing online	←	Computer competence	1.032	0.078	13.185	***
Attitude towards purchasing online	←	Paranoia	−0.306	0.064	−4.809	***
Attitude towards purchasing online	←	Cyber fear	0.288	0.067	4.284	***
Online purchasing intention	←	Attitude towards purchasing online	0.420	0.035	11.886	***
Online purchasing intention	←	Paranoia	0.105	0.042	2.486	0.013

H2 states that paranoia has no direct impact on online purchasing intention. However, the regression analysis shows rather contradicting results: this relation is not significant if $p < 0.01$ is used. However, it would be significant if $p < 0.05$ criteria were employed (as it is done in many studies). In this study, we use stricter criteria for significance, therefore the results ($\beta = 0.105$, $p = 0.013$) allow us to accept H2.

H3 states that paranoia has an indirect negative impact on the intention to purchase online when the relationship is mediated by the attitude towards purchasing online. An indirect effect on purchase intention, mediated by the attitude towards online purchasing is found to be negative ($\beta = -0.026$), allowing to accept H3. The results of the indirect effects are presented in Table 3.

Table 3. Standardized indirect effects.

	Social Media Use Integration	Privacy Concern	Computer Competence	Cyber Fear	Paranoia	Attitude towards Purchasing Online
Paranoia	0.000	0.000	0.000	0.000	0.000	0.000
Attitude towards purchasing online	−0.053	0.000	−0.040	−0.117	0.000	0.000
Online purchasing intention	−0.005	−0.030	0.361	0.140	−0.146	0.000

H4 states that cyber-fear has a direct negative impact on the attitude towards purchasing online. However, the results are the opposite: cyber-fear has a direct positive impact on the attitude towards purchasing online ($\beta = 0.288$, $p = 0.000$), thus H4 hypothesis is rejected.

H5 predicts that privacy concern has a direct negative impact on attitude towards purchasing online. A regression analysis shows that this relation is not significant ($\beta = -00.053$, $p = 0.358$), therefore H5 is rejected.

H6 states that cyber-fear has an indirect negative impact on the attitude towards purchasing online when the relationship is mediated by paranoia. The assessment of the standardized indirect effect confirms this assumption ($\beta = -0.117$), and H6 is accepted.

H7 hypothesis states that paranoia mediates a negative impact of social media use integration on the attitude towards purchasing online. Standardized indirect effects show the existence of a relatively small ($\beta = -0.53$) negative indirect effect, and this allows accepting H7.

H8 states that computer competence has an indirect negative impact on the attitude towards purchasing online when the relationship is mediated by paranoia. The standardized indirect effects show that due to mediation, computer competence changes the relationship valence and is negative ($\beta = -0.04$). Thus, H8 is accepted.

H9 states that computer competence has a direct positive impact on the attitude towards purchasing online. The regression analysis shows a significant positive relationship between computer competence and the attitude towards purchasing online ($\beta = 1.032$, P = 0.000), thus H9 is accepted.

5. Discussion

The purpose of this study was to examine the role of paranoia in relation to social media use in the context of the online purchasing process. Findings of the study suggest that paranoia is an important psychological antecedent on the attitude towards purchasing online, which is a new element in overall studies of online behaviour. Elaboration of this negative relationship presents the main contribution of the current study since the growing complexity of human interactions with IT systems trigger extreme forms of distrust and even paranoia. The current study might be considered as an extension of the studies on distrust, as paranoia can be considered as the irrational type of distrust [8] and the current findings are broadening the previous knowledge that distrust has a negative impact on attitudes towards purchasing online [44]. The current study extends the previous scope of knowledge regarding the antecedents of distrust/paranoia by including into the consideration two factors that represent user competence from two perspectives: from the general computer competence and from the engagement in social media use.

Another important finding of this study is the disclosure of the fact that paranoia mediates effects of other factors towards the attitude of purchasing online. These factors (social media use integration, cyber fear and computer competence) are different by their nature and their potential influence on online purchasing. However, paranoia is a mediator between them and attitude towards online purchasing. To our knowledge, this type of relationship has never been found before and presents another noticeable contribution to this study. Paranoia mediates effects from these three factors but does not play a mediating role between privacy concern and the attitude towards purchasing online. The exploratory study did not aim to elaborate deeper on this, but these findings suggest interesting directions for future studies. The relation of each factor under analysis (social media integration, cyber-fear, computer competence) with paranoia seems to be really promising, though might require additional theoretical justification and empirical testing.

We assumed that paranoia is an antecedent of the attitude towards online purchasing and has no direct influence on the intention to purchase online. However, the empirical evidence has revealed a possibility that this influence might exist. Therefore, it is necessary to test it again on a larger sample in order to conclude whether this observation is a sample-specific case, or it suggests an alternative consideration on the role of paranoia in purchasing, thus inviting to look for a different theoretical background.

Finally, a smaller and rather unexpected result has been observed in terms of the relation between cyber-fear and the attitude towards purchasing online. Since both paranoia and cyber-fear factors are associated [22], similar results were expected. However, the relation between cyber-fear and attitude towards purchasing online was positive, and therefore, rather contradictory. Such an unexpected result might be related to the nature of the cyber-fear measurement scale, which originally aims to capture the human attitudes towards the cyber-related threats that are likely to occur or are at least are much more realistic in comparison to the cyber-paranoia dimension, which has also been developed by the same authors, aiming to evaluate the "unrealistic fears concerning threats via information technologies whereby individuals perceive themselves to be open to be 'attacked,' persecuted or victimized in some way [22]. Due to this, cyber-fear might be related to the cognition of cyber-related threats, which may not have a negative influence on attitudes towards purchasing online. Obviously, this issue also requires further elaboration and should be addressed in future researches.

Though the study allowed to explore several aspects of paranoia in online purchasing, it has several limitations. First, the tested variables were rather similar by their nature and this required a significant reduction of items during EFA and CFA. Most probably, future studies will consider the possibilities of modifying the scales or using their alternatives. Second, though the sample size was sufficient for the exploratory purposes, it could have influenced several indices of the model fit and the significance levels in regressions. It is most advisable to employ larger samples in future studies. However, despite these limitations, the study has contributed to the scientific knowledge regarding the role of paranoia in online purchasing and hopefully will trigger several new studies on the issue.

Author Contributions: I.Z. has been responsible for methodology, data gathering and the first draft of the manuscript. M.D. has critically revised the manuscript. S.U. has developed the conceptualization of the paper and performed the analysis. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Alalwan, A.A. Investigating the impact of social media advertising features on customer purchase intention. *Int. J. Inf. Manag.* **2018**, *42*, 65–77. [CrossRef]
2. Hajli, M.N. A study of the impact of social media on consumers. *Int. J. Mark. Res.* **2013**, *56*, 387–404. [CrossRef]
3. Gupta, G.; Vohra, A.V. Social Media Usage Intensity: Impact Assessment on Buyers' Behavioural Traits. *FIIB Bus. Rev.* **2019**, *8*, 161–171. [CrossRef]

4. Colby, K.M. Modeling a paranoid mind. *Behav. Brain Sci.* **1981**, *4*, 515–534. [CrossRef]
5. Kramer, R.M. Paranoid Cognition in Social Systems: Thinking and Acting in the Shadow of Doubt. *Pers. Soc. Psychol. Rev.* **1998**, *2*, 251–275. [CrossRef] [PubMed]
6. Kramer, R.M. Organizational Paranoia: Origins and Dysfunctional Consequences of Exaggerated Distrust and Suspicion in the Workplace. In *21st Century Handbook of Organizations: A Reference Handbook*; Sage Publications: Los Angeles, GA, USA, 2008; pp. 231–238.
7. Deutsch, M. Trust and suspicion. *J. Confl. Resolut.* **1958**, *2*, 265–279. [CrossRef]
8. Deutsch, M. The Resolution of Conflict: Constructive and Destructive Processes. *Am. Behav. Sci.* **1973**, *17*, 248. [CrossRef]
9. Freeman, D.; Garety, P.A.; Bebbington, P.E.; Smith, B.; Rollinson, R.; Fowler, D.; Kuipers, E.; Ray, K.; Dunn, G. Psychological investigation of the structure of paranoia in a non-clinical population. *Br. J. Psychiatry* **2005**, *186*, 427–435. [CrossRef]
10. Ellett, L.; Lopes, B.; Chadwick, P. PARANOIA IN A NONCLINICAL POPULATION OF COLLEGE STUDENTS. *J. Nerv. Ment. Dis.* **2003**, *191*, 425–430. [CrossRef]
11. Fenigstein, A.; Vanable, P.A. Paranoia and self-consciousness. *J. Pers. Soc. Psychol.* **1992**, *62*, 129–138. [CrossRef]
12. Freeman, D. Suspicious minds: The psychology of persecutory delusions. *Clin. Psychol. Rev.* **2007**, *27*, 425–457. [CrossRef] [PubMed]
13. Freeman, D.; McManus, S.; Brugha, T.; Meltzer, H.; Jenkins, R.; Bebbington, P. Concomitants of paranoia in the general population. *Psychol. Med.* **2011**, *41*, 923–936. [CrossRef] [PubMed]
14. Urbonavicius, S.; Zimaitis, I. The mediating role of paranoia on online consumer behaviour. In Proceedings of the 9th EMAC Regional Conference, Prague, Czech Republic, 12–14 September 2018.
15. Raihani, N.J.; Bell, V. An evolutionary perspective on paranoia. *Nat. Hum. Behav.* **2019**, *3*, 114–121. [CrossRef] [PubMed]
16. Carvalho, C.; Pinto-Gouveia, J.; Peixoto, E.; Motta, C. Paranoia as a Continuum in the Population. *AJSSH* **2014**, *2*, 382–391.
17. Yoon, S.-J. The antecedents and consequences of trust in online-purchase decisions. *J. Interact. Mark.* **2002**, *16*, 47–63. [CrossRef]
18. Chang, H.H.; Chen, S.W. The impact of online store environment cues on purchase intention: Trust and perceived risk as a mediator. *Online Inf. Rev.* **2008**, *32*, 818–841. [CrossRef]
19. Chang, S.Y.; Fang, S.R. Antecedents and distinctions between online trust and distrust: Predicting high and low-risk internet behaviours. *J. Electron. Commer. Res.* **2013**, *14*, 149–166.
20. Moody, G.D.; Galletta, D.F.; Lowry, P.B. When trust and distrust collide online: The engenderment and role of consumer ambivalence in online consumer behavior. *Electron. Commer. Res. Appl.* **2014**, *13*, 266–282. [CrossRef]
21. Hilton, J.L.; Fein, S.; Miller, D.T. Suspicion and Dispositional Inference. *Pers. Soc. Psychol. Bull.* **1993**, *19*, 501–512. [CrossRef]
22. Mason, O.J.; Stevenson, C.; Freedman, F. Ever-present threats from information technology: The Cyber-Paranoia and Fear Scale. *Front. Psychol.* **2014**, *5*, 5. [CrossRef]
23. Benamati, J. "Skip"; Serva, M.A. Trust and distrust in online banking: Their role in developing countries. *Inf. Technol. Dev.* **2007**, *13*, 161–175. [CrossRef]
24. Broyles, S.J. Subliminal Advertising and the Perpetual Popularity of Playing to People's Paranoia. *J. Consum. Aff.* **2006**, *40*, 392–406. [CrossRef]
25. Pappas, N. Marketing strategies, perceived risks, and consumer trust in online buying behaviour. *J. Retail. Consum. Serv.* **2016**, *29*, 92–103. [CrossRef]
26. Fishbein, M.A. Behavior theory approach to the relations between beliefs about an object and the attitude toward the object. In *Readings in Attitude Theory and Measurement*; Fishbein, M., Ed.; John Wiley & Sons: New York, NY, USA, 1967; pp. 389–400.
27. Beck, L.; Ajzen, I. Predicting dishonest actions using the theory of planned behavior. *J. Res. Pers.* **1991**, *25*, 285–301. [CrossRef]
28. Buchanan, T.; Paine, C.; Joinson, A.; Reips, U.D. Development of measures of online privacy concern and protection for use on the Internet. *J. Assoc. Inf. Sci.* **2007**, *58*, 157–165. [CrossRef]

29. Akhter, S.H. Privacy concern and online transactions: The impact of internet self-efficacy and internet involvement. *J. Consum. Mark.* **2014**, *31*, 118–125. [CrossRef]
30. Slyke, C.; University of Central Florida; Shim, J.; Johnson, R.; Jiang, J. University of South Florida Concern for Information Privacy and Online Consumer Purchasing. *J. Assoc. Inf. Syst.* **2006**, *7*, 415–444.
31. Coşar, C.; Panyi, K.; Varga, A. Try Not to Be Late!-the Importance of Delivery Service in Online Shopping. *Organ. Mark. Emerg. Econ.* **2017**, *8*, 177–192.
32. Dai, B.; Forsythe, S.; Kwon, W. The impact of the online shopping experience on risk perceptions and online purchase intentions: Does product category matter? *J. Electron. Commer. Res.* **2014**, *15*, 13–24.
33. McCole, P.; Ramsey, E.; Williams, J. Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns. *J. Bus. Res.* **2010**, *63*, 1018–1024. [CrossRef]
34. Monsuwé, T.P.Y.; Dellaert, B.G.; De Ruyter, K. What drives consumers to shop online? A literature review. *Int. J. Serv. Ind. Manag.* **2004**, *15*, 102–121. [CrossRef]
35. Morahan-Martin, J.; Schumacher, P. Attitudinal and experiential predictors of technological expertise. *Comput. Hum. Behav.* **2007**, *23*, 2230–2239. [CrossRef]
36. Liao, Z.; Cheung, M.T. Internet-based e-shopping and consumer attitudes: An empirical study. *Inf. Manag.* **2001**, *38*, 299–306. [CrossRef]
37. Lu, H.-P.; Su, P.Y.-J. Factors affecting purchase intention on mobile shopping web sites. *Internet Res.* **2009**, *19*, 442–458. [CrossRef]
38. Blake, B.F.; Neuendorf, K.A.; Valdiserri, C.M. Innovativeness and variety of Internet shopping. *Internet Res.* **2003**, *13*, 156–169. [CrossRef]
39. Burroughs, R.E.; Sabherwal, R. Determinants of retail electronic purchasing: A multi-period investigation. *J. Inf. Syst. Res.* **2005**, *40*, 35–56. [CrossRef]
40. Jenkins-Guarnieri, M.A.; Wright, S.L.; Johnson, B. Development and validation of a social media use integration scale. *Psychol. Popul. Media Cult.* **2013**, *2*, 38–50. [CrossRef]
41. Huang, D.-L.; Rau, P.-L.P.; Salvendy, G. Perception of information security. *Behav. Inf. Technol.* **2010**, *29*, 221–232. [CrossRef]
42. Lietuvos Statistikos Departamentas. Available online: https://osp.stat.gov.lt/statistiniu-rodikliu-analize#/ (accessed on 2 January 2020).
43. Zarrad, H.; Debabi, M. Online Purchasing Intention: Factors and Effects. *Int. Bus. Manag.* **2012**, *4*, 37–47.
44. Kim, J.B. An empirical study on consumer first purchase intention in online shopping: Integrating initial trust and TAM. *Electron. Commer. Res.* **2012**, *12*, 125–150. [CrossRef]

Willingness to disclose personal information: how to measure it?

Mindaugas Degutis[1], Sigitas Urbonavicius[2], Ignas Zimaitis[3], Vatroslav Skare[4], Dalia Laurutyte[5]

[1]*Vilnius University*
Sauletekio Ave. 9, LT- 10222 Vilnius, Lithuania
E-mail. mindaugas.degutis@evaf.vu.lt

[2]*Vilnius University*
Sauletekio Ave. 9, LT- 10222 Vilnius, Lithuania
E-mail. sigitas.urbonavicius@evaf.vu.lt

[3]*Vilnius University*
Sauletekio Ave. 9, LT- 10222 Vilnius, Lithuania
E-mail. ignas.zimaitis@evaf.vu.lt

[4]*University of Zagreb, Faculty of Economics & Business*
Trg J.F. Kennedya 6, 10000 Zagreb, Croatia
E-mail. vskare@efzg.hr

[5]*Vilnius University*
Sauletekio Ave. 9, LT- 10222 Vilnius, Lithuania
E-mail. laurutyted@gmail.com

crossref

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

The study investigates a possibility of multidimensionality of a construct of willingness to disclose personal information (WTD). Willingness or unwillingness to disclose personal information has been a widely studied phenomenon as personal data is becoming increasingly important for many industries including marketing. Most of these studies treat the willingness to disclose personal information as a homogenous construct. In many cases it is measured by providing a number of personal information items and asking about the willingness to share them. Although recently there have been studies that find possible multidimensionality of the construct, most of them do not further elaborate this possibility. Therefore, we have adopted a scale used in many previous studies and made an attempt to test the hypotheses that would base the argument regarding the multidimensionality of this construct or even the possibility to consider several separate variables and constructs aimed at measuring the willingness to disclose personal data. This was achieved by using three antecedents of the willingness to disclose personal data – the perceived regulatory effectiveness, privacy awareness and disposition to value privacy – and comparing how they interact with different types of the willingness. This allowed to assess different relationship patterns between the antecedents and possible dimensions of the willingness to disclose personal information.

We have employed Exploratory and Confirmatory Factor Analysis to check the homogeneity of the willingness to disclose personal information and Structural Equation Modelling to test the patterns of the relations. We have found that there is more than one separate dimension of WTD which means it could not be treated as a homogenous construct. Factorial analysis distinguishes three types of the willingness linked with three types of data: the willingness to disclose personal data that includes individual facts (profile data), social networking data and online browsing/purchasing data. The conclusion of multidimensionality is also supported by the differences in relationship patterns observed between the antecedents and the willingness to disclose personal information.

Keywords: *Willingness to disclose personal information, privacy awareness, privacy perceived regulatory effectiveness, disposition to value privacy*

Introduction

Predictive marketing based on consumer personal data analytics has become a common approach for many business companies and organizations around the world during the recent decades (Omer & Levin, 2015). More and more companies, both internet and offline based, are trying to collect personal data of their consumers or visitors in order to use it for a variety of analytical and/or communicational purposes (Paine Schofield & Joinson, 2008). At the same time, consumers leave more and more personal information online (Boerman et al., 2018) hoping to increase the usability, convenience of the website or get other benefits. Many businesses use personal information for personalization of

services and messages (Boerman et al., 2017; Estrada-Jiménez, 2017), be it advertising or political microtargeting.

Therefore, information privacy has become an increasingly important topic for academic research (Rohunen et al., 2018), as it plays an important role in the online purchasing process (Cosar et al., 2017). One of the major topics of this literature stream is about understanding what causes consumer willingness to disclose (WTD) personal information (Miltgen & Smith, 2015). One type of antecedents is related with personal dispositions of consumers (e.g. their values (Anic et al., 2018), personality traits (Bansal et al., 2016), privacy attitudes and privacy experiences such as prior experience with privacy invasion (Malhotra et al., 2004; Xu et al., 2011), as well as cultural backgrounds (Gupta, Iyer, & Weisskirch, 2010; Robinson, 2017). Another type of antecedents under analysis is related to socio-demographic characteristics (Weinberger et al, 2017), internet usage and habits (Akhter, 2014; Park, 2013). All these factors are based on personal characteristics of users. One more type of antecedents includes factors that could be named as situational factors, i.e. factors such as industry or company-specific variables, e.g. a general trust in the company or its reputation (Lwin et al., 2007; Xu et al., 2011). Situation-specific factors also include the perceived sensitivity, volume and relevance of information requested (Mothersbaugh et al., 2012), familiarity with the website and/or vendor, and incentives such as rewards offered for data disclosure. So, generally, privacy-related constructs (including but not limited to the antecedents of disclosure behaviour) can be dispositional, that is, belong to or be impacted by an individual's pre-existing attitudes, beliefs, tendencies, knowledge and skills, or situational - driven by context-dependent and "*situation-specific privacy constructs*" and their perceptions, e.g. related to a specific online company (Kehr et al., 2015).

Even though the antecedents of willingness to disclose personal information have received a prominent attention from scholars, the consequent construct of the willingness to disclose personal information has not been yet extensively studied. There are several different scales used to measure the construct of the willingness to disclose personal information.

Some authors have measured the willingness to disclose personal information in general, leaving for respondents to decide which specific data types and items might be requested (Kehr et al., 2015; H. Li et al., 2011; Y. Li, 2014; Schoenbachler & Gordon, 2002; Wakefield, 2013; T. Wang et al., 2016) while other researchers have referenced only data categories, such as financial information, personal health information and other (Bansal et al., 2016; Z. Wang & Liu, 2014). Malhotra et al. (2004) have used a rather simple and convenient 4 item scale to measure a general disposition to disclose personal information. However, one of the most common approaches tends to list specific data types/items and ask the respondents to evaluate their disclosure intention on an item-by-item basis (Gupta et al., 2010; Heirman et al., 2013; Malheiros et al., 2013; Norberg et al., 2007; Robinson, 2017; Treiblmaier & Chong, 2011; Walrave & Heirman, 2012). This approach goes back to the measurements used by Phelps et al. (2000) and Sheehan and Hoy (2000). Some of these authors treat the scale as a single dimension measure of willingness to disclose personal information (Robinson, 2017; Gupta et al., 2010), while others find various dimensions and different behaviours of consumers related to them (Phelps, 2000, Heirman et al., 2013). This is justified by an increasing number of instances when personal data can be disclosed on the internet and a growing number of data types as well as multiple ways of data transfer. Therefore, the question of whether the willingness to disclose personal data is a homogenous construct is challenged. It seems quite possible that the willingness to disclose personal data varies depending on the types of data to be disclosed and, consequently, various instances of the willingness should be studied individually.

The aim of this study is to test the possible multidimensionality of the willingness to disclose personal data (WTD) construct. Additionally, we aim to test the hypotheses on different types of relations between the tested antecedents and various types/dimensions of the WTD construct.

Theoretical background

One of the first examples measuring the willingness to disclose personal information in the modern commerce context was a study by Phelps et al. (2000). The researchers used a 16 item scale and asked respondents to evaluate their willingness to disclose each 16 types of data on a 4-point scale (from 'always willing' to 'never willing'). Phelps et al. categorized 16 items into four groups: demographic characteristics, lifestyle, media usage habits and financial information. Nevertheless, this grouping was neither based on any type of statistical or other analytics, nor it was used for the subsequent analysis aimed to disclose their relations with antecedents or consequents. Therefore, although naming four groups of personal information, Phelps et al. (2000) treated the concept and the construct of willingness to disclose data as a one-dimensional variable.

Gupta et al. (2010) examined consumer willingness to disclose personal data in the US and India, adapted (shortened to 13 items) the scale used by Phelps et al. (2000) and deployed a 5-item scale to measure the willingness (from "not at all willing" to "very willing"). These researchers also treated the construct of the willingness to disclose personal information as a homogenous unit.

The scales used by Gupta and Phelps were adapted by Robinson (2017) in his comparative study of Estonian and US consumers. He used a 7-item scale and expanded the list of items to 17, including the ones related to the internet and e-commerce. In his analysis, he also used 6 sub-indices: Contact Information, Payment Information, Life History Information, Work-Related Information, Online Account Information, Financial/Medical History Info. He has concluded that there are some differences between Estonia and the US regarding the terms of the willingness to disclose different types of personal data (Robinson, 2017). These categories may be considered as sub-dimensions of the willingness, but the author did not elaborate on the possibility that there might be

more than one separate type of willingness and separate constructs for the measurement of willingness to disclose personal data.

This step was done by Heirman et al. (2013) who studied the willingness to disclose personal data to an internet site. These researchers proposed 4 separate sub-constructs of WTD, namely: identity data, geographical information, contact data and profile data. They used a 7-item scale to measure the willingness to provide each item of personal data and, after conducting factor analysis, confirmed the existence of 4 dimensions of willingness to disclose data. They have also proved that there are differences in how an antecedent variable (namely, trust) influences various dimensions of the willingness to disclose personal data.

In this study, we have attempted to modify the existing WTD scale towards modern realities and situations when an individual may express a certain degree of the willingness to disclose personal data. Simultaneously, we avoid situations where an individual has no choice in disclosing certain types of data such as the necessity to provide a credit card or other banking information in order to perform a transaction. This leads to three types of personal data that are disclosed in a variety of instances: (a) personal data that discloses the basic demographic and contact information; (b) personal data that discloses social interactions of a person (account of social networks, communication engines) and (c) personal data that disclosed online behaviours and is collected automatically, based on a single-time permission (such as browsing history, location tracking). The first two types of data are provided by a person, but differ in terms of whether the data are linked with the parameters of an individual versus his/her social interactions; the third type differs by the form of its collection (automatic) and represents behavioural patterns. Consequently, these items may help to assess the three different types of willingness to disclose personal data.

The willingness to disclose personal data may be considered both as a dispositional (attitudinal) and situational variable. In this study, the dispositional aspect is considered, thus the three forms of willingness have to be related with the antecedents that are also dispositional by their nature. The three dispositional antecedents – the privacy awareness, disposition to value privacy and perceived regulatory effectiveness (Xu et al., 2008) – have been widely studied in the context of privacy concerns and willingness to disclose personal data and are included in the current study.

Individuals might demonstrate different inclinations towards certain privacy behaviours and various levels of disposition to value privacy which can be related to a disposition to value privacy as an inherent need and trait which reflects the extent to which a person is inclined to maintain their personal information in private as much as possible *"across a broad spectrum of situations and persons"* (Xu et al., 2008). The disposition to value privacy positively impacts online privacy concern and the perceived intrusive information gathering; a person who attributes higher value to his/her informational privacy is more likely to have a higher degree of serious concerns regarding personal data disclosure. The concerns of people with a high disposition to value privacy include issues not about the content of information, but also about how the personal data is collected, how it might be processed, i.e. some types of information gathering might be perceived as inappropriate and intrusive (Smith et al., 2011; Xu et al., 2008).

The disposition to value privacy is closely linked with one's awareness of privacy practices (privacy awareness). This dispositional factor reflects how an individual is aware of company practices, regulatory policies and privacy-related matters in the society (Xu et al., 2008). The awareness of privacy practices has been studied as an antecedent of disposition to value privacy and has been found to decrease the willingness to disclose personal information (Olivero and Lunt, 2004).

Privacy has been generally considered as a natural right of individuals, both in theory and under national and international law (Smith et al., 2011). Therefore, the regulatory aspect of a person's privacy offline and online is important on societal and individual decision-making levels. The empirical findings support the importance of an individual's perceptions regarding privacy regulation as a higher perceived effectiveness was found to decrease privacy concern (Miltgen & Smith, 2015) and to reduce the need for privacy protection behaviour (Lwin et al., 2007; Miltgen & Smith, 2015). If consumers feel protected enough at a societal level, this reduces the need to put in individual efforts for privacy protection; people feel secure enough about the private data they provide (Miltgen and Smith, 2015).

Hypotheses

Based on previous studies by Phelps et al (2010), Heirman et al. (2013), Robinson (2017) we assume that the willingness to disclose personal data is not a homogenous construct. We hypothesize that:

H1. The scale that measures the willingness to disclose personal data has more than one dimension.

We expect to find 3 dimensions of the willingness to disclose personal information: first – linked with the personal data that helps to identify a person and includes data items most frequently provided by an individual while browsing or purchasing online (name, address, e-mail, etc.); second – related to the information about an individual's social networking (such as social account information) and the third – related with the information collected online automatically, once a permission is given (such as browsing history, location tracking, etc.). Correspondingly, this would mean three types of the willingness to disclose personal data: the willingness to disclose personal data (individual facts, WTD_PD_IND), the willingness to disclose personal data about social interactions (WTD_PD_SOC) and the willingness to disclose personal data that is collected online (WTD_OD). All the three types of willingness are supposed to have certain relations with the analysed antecedents: disposition to value privacy, perceived regulatory effectiveness and privacy awareness.

The disposition to value privacy is the closest dispositional variable to the willingness to disclose personal

data. Xu et al. (2008) defined the disposition to value privacy as an inherent need and trait which reflects the extent to which a person is inclined to maintain his personal information private *"across a broad spectrum of situations and persons"*, thus it reflects the individual's need to preserve his personal space, the importance put on his or her privacy and personal information. Xu et al. (2008) identified the disposition to value privacy as a "*cultural and personality characteristic*" and argues that the information disclosure decision depends on this trait. It has the most direct influence on the willingness to disclose personal information of all types because of its nature. Additionally, it may moderate the influences of other factors. Therefore, the hypothesis follows:

H2. The disposition to value privacy will have a direct negative influence on all the three dimensions of the willingness to disclose personal data.

The perceived regulatory effectiveness is linked with the situations where somebody perceives disclosing his/her personal information and relates this the regulations of various forms of legislation, with an expectation that this information is protected (Miltgen and Smith, 2015). The considered types of data most commonly include individual characteristics and behaviours. Therefore, the perceived regulatory effectiveness is supposed to directly influence the willingness to disclose contact and profile information and online data but will not necessarily be related to the disclosure of social networking information. The following hypothesis formulated:

H3. The perceived regulatory effectiveness will have a direct positive influence on the willingness to disclose personal data that include individual facts.

The awareness of privacy practices (privacy awareness) is a dispositional construct that reflects how an individual is aware of company practices, regulatory policies and privacy-related matters in the society (Xu et al., 2008). The individuals who are highly aware of the issues 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 awareness of privacy practices has been found to be closely related with an individual's disposition to value privacy: it has been modelled as an antecedent of a disposition to value privacy and has been found to enhance this disposition in the e-commerce context. However, interestingly, it did not affect a disposition to value privacy in the social networking context (Xu et al., 2008). The privacy awareness is mainly linked with the disclosure of the information that reflects the individual demographic characteristics of a person. Therefore, it should only directly influence the willingness WTD_PD_IND:

H4. Privacy awareness will have a direct positive influence on the willingness to disclose personal data that include individual facts.

Measurement scales and survey

The survey data were collected in Lithuania by using CAWI survey and a self-administered questionnaire. The study included the scales that were developed and used in previous academic studies and that were demonstrating satisfactory reliability and validity. All the items were measured on a 1-7 Likert scale. A 3-item scale of disposition to value privacy was originally developed by Xu et al. (2008). They found Cronbach's to be α=0.88. Later it was adapted by Xu et al. (2011), Li (2014). The perceived regulatory effectiveness scale (3 items, α=0.83) was taken from Lwin et al. (2007) with a minor change that includes GDPR as an example. The privacy awareness scale (3 items) was taken from Xu et al. (2008). Later it was also used by Xu et al. (2011) and showed a good reliability (α=0.865). The willingness to disclose personal data was measured by a scale adopted from Gupta et al (2010) and Heirman et al. (2013) also used by Robinson (2017). It (with 14 items) showed a good reliability in earlier studies (α = 0.87) and was the most relevant recent scale of this type (Robinson, 2017). In this study, the original list of items was reduced from 17 to 9 by removing those that were linked with entirely technical issues that would not be understood by general population. However, the scale was amended with 5 items of personal data that are collected online automatically (on user consent).

The survey sample consisted of 439 respondents ranging from 18 to 69 years of age; the age group of 18-22 represented 32.1% of the respondents, those spanning 23-35 covered 33.0%; those 36 or older represented the remaining 34.9%. 25.1% of the respondents were male and 74.9% female. There were 54.9% of the respondents with bachelor degree or lower education qualifications and 45.1% with master or higher.

One item was removed from the willingness to disclose the personal data scale because of the high skewness (2.532) and kurtosis (5.799). All other items were included into the exploratory 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. The extracted factors explained 57.860 of the total variance. The dependent variable *willingness to disclose the personal data* appeared in three factors (see Table 1).

Table 1

Factor loadings of Willingness to disclose personal data (WTD)

	Factor		
	1	2	3
Full name		0.794	
Address		0.625	
Mobile phone		0.739	
E-mail		0.797	
Birthday date		0.459	
LinkedIn account			0.759
Facebook account			0.653
Skype account			0.877
Internet browsing history and habits	0.754		
Geolocation data	0.635		
Online purchasing history and habits	0.926		
Information on searched goods	0.819		
IP address	0.543		
Means of the loadings:	**0.735**	**0.683**	**0.763**

The first extracted factor – the willingness to provide online data (WTD_OD) - included the data that are linked with online activities but does not have to be provided by a person. It is required just to give a permission to track/record this type of the data, while the further processes are going automatically without a direct intervention of the internet user. The reliability of this scale was 0.854. Two other factors represent personal data about the internet user. However, factor number 2 – the willingness to disclose personal data (individual facts, WTD_PD_IND) – includes the identification and demographic data of an individual, while factor number 3 the willingness to disclose personal data about social interactions (WTD_PD_SOC). The reliabilities of these scales were: 0.851 and 0.853, respectively. The reliability of scales that measured antecedents was also satisfactory: disposition to value privacy α = 0.835; perceived regulatory effectiveness α = 0. 746; privacy awareness α = 0.829; online privacy concern α = 0.901;

A subsequent confirmatory factor analysis has been performed three times, with the same three same antecedents and each dependent variable separately. All the three models were robust and showed good fit: a model with a dependent variable WTD_PD_IND – CMIN/DF=1.242; TLI rho^2=0.991; CFI=0.993; RMSEA=0.023; a model with a dependent variable WTD_PD_SOC – CMIN/DF=1.242; TLI rho^2=0.991; CFI=0.993; RMSEA=0.023; a model with a dependent variable WTD_OD – CMIN/DF=1.350; TLI rho^2=0.988; CFI=0.991; RMSEA=0.028.

On this basis, three causal models have been developed. In all the three instances, the presence of the common latent factor has been discovered, therefore the variables have been imputed considering its presence. All the three models demonstrated satisfactory fit: a model with a dependent variable WTD_PD_IND – CMIN/DF=3.472; TLI rho^2=0.941; CFI=0.990; RMSEA=0.075; a model with a dependent variable WTD_PD_SOC – CMIN/DF=1.041; TLI rho^2=0.999; CFI=1.000; RMSEA=0.010; a model with a dependent variable WTD_OD – CMIN/DF=2.862; TLI rho^2=0.965; CFI=0.994; RMSEA=0.065. This allowed to test the hypotheses.

Testing of the hypotheses

The first hypothesis H1 (The scale that measures the willingness to disclose personal data has more than one dimension) was tested on the basis of an exploratory factor analysis (Table 1) and a subsequent confirmatory factor analysis. The average factor loadings (0.735, 0.683, 0.763) confirm the convergent validity, the correlations between factors (below 0.8) – discriminant validity (Table 2).

Table 2

Correlation among factors

	WTD_PD_IND	WTD_PD_SOC	WTD_OD
WTD_PD_IND	1.000	0.523	0.509
WTD_PD_SOC	0.523	1.000	0.414
WTD_OD	0.509	0.414	1.000

Additionally, these three variables have a high reliability of their scales (Cronbach's α above 0.85). All this indicates that the three types of the willingness can be measured as three separate variables and allows to confirm H1.

Hypothesis H2 (the disposition to value privacy will have a direct negative influence on all the three dimensions of the willingness to disclose personal data) is tested on the basis of all the three causal models by checking the significance of the relation between the disposition to value privacy and corresponding types of WTD. In all the cases p=0.000; WTD_PD_IND β=-0.394; WTD_PD_SOC β=-0.273; WTD_OD β=-0.458. Therefore, H2 is confirmed.

Hypothesis H3 (the perceived regulatory effectiveness will have a direct positive influence on the willingness to disclose personal data that includes individual facts) is tested on the basis of the causal model with the dependent variable WTD_PD_IND. In this case β=0.097; p=0.045. H3 is confirmed.

Hypothesis H4 (privacy awareness will have a direct positive influence on the willingness to disclose personal data that includes individual facts, the perceived regulatory effectiveness will have a direct positive influence on the willingness to disclose personal data that includes individual facts) is tested on the basis of the causal model with the

dependent variable WTD_PD_IND. In this case β=0.158; p=0.004. H4 is confirmed.

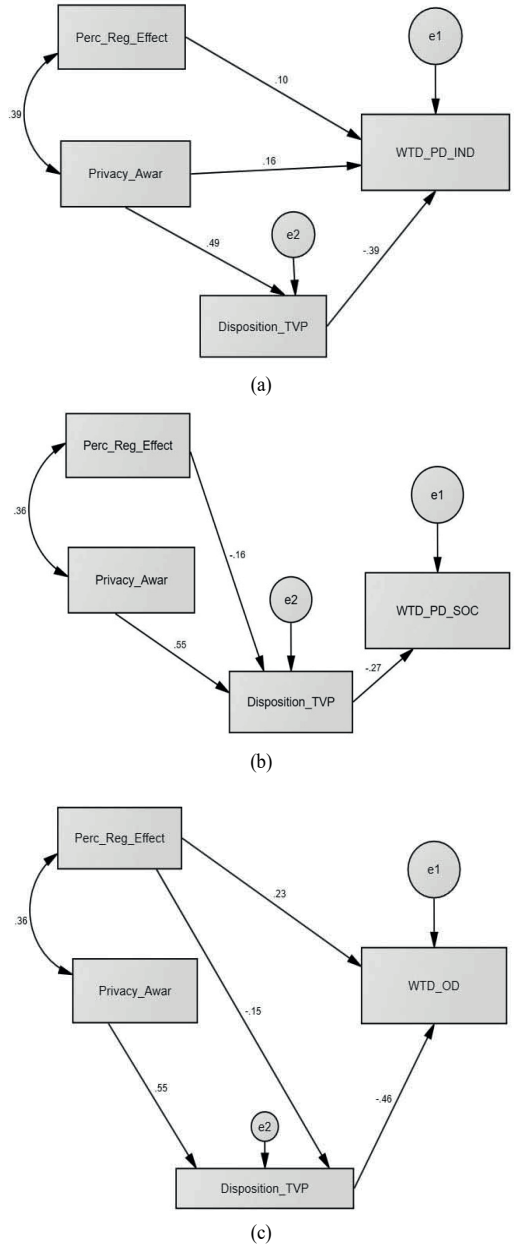

Figure 1. Causal models

Although it was not included in the hypotheses, we aimed to disclose that the three antecedents influence all the three types of WTD, but this happens in different ways. These different relation patterns are presented in three different causal models (Figure 1).

Discussion and conclusions

The findings of the current survey support a previous research carried out by Heirman et al. (2013). Factor analysis shows that there is more than one dimension in the willingness to disclose personal information construct. Heirman et al. (2013) found 4 separate dimensions while we found 3 dimensions instead of 4. Probably, the difference is due to a larger number of items used in a survey conducted by Heirman et al. (2013). As mentioned previously, Heirman et al. (2013) distinguish 4 groups of personal data (although it is not based on any statistical model): identity data, geographical information, contact data and profile data. We find slightly different dimensions based on factorial analysis, namely personal contact and profile information, social networking data and internet usage and purchasing online information. This partially reflects the dimensions found by Heirman et al. (2013). Obviously, the consumers perceive personal data as a heterogenous phenomenon with all the consequences of this fact.

Not only the factor analysis shows multidimensionality of the WTD construct. T-test analysis shows that there is a significant difference between the average value of the three separate dimensions of willingness to disclose personal information. Test results (in both cases sig. <0.001) show that consumers are significantly more willing to disclose contact data and internet usage/purchasing information compared to social networking data. This supports the idea of difference in the perception of different types of personal information. It could be hypothesized that consumers perceive social networking data as more sensitive and intimate, therefore are consequently less willing to share it with others.

Further multidimensionality of WTD construct is supported by a different pattern of relationship between the antecedents and WTD. The disposition to value privacy has a negative relation with all the three dimensions of WTD, while the perceived regulatory effectiveness does not have any influence in case of social networking data (compared to a positive relationship in other two cases) and level of privacy awareness has positive relation with willingness to disclose personal data only in case of personal contact data disclosure (compared to no relationship in other two cases). Again, it could be hypothesized that consumers do not think that social networks could be effectively regulated by national or EU laws and, therefore, even better regulatory perception does not have a positive effect on the willingness to disclose this type of data. A positive relationship between privacy awareness (i.e. interest in privacy issues) and the willingness to disclose personal contact information shows that probably more educated consumers understand that this type of data is less sensitive compared to other types.

In the cases when the perceived regulatory effectiveness and privacy awareness have no direct impact on WTD, these variables influence WTD indirectly, via mediation of the disposition to value privacy. Additionally, these two factors

may have both direct and indirect effects on WTD. However, the most important observation is not the strength of these influences, but the existence of three different causal models when three types of WTD are considered. This allows to additionally state that these three types of WTD may be assessed and analyzed separately, since they represent different aspects of willingness to disclose personal data.

The multidimensionality of WTD issue is worth further investigation, probably including more items of personal information into factorial analysis. It might provide even more than 3 or 4 possible dimensions of the construct. More than that, additional justification might help concluding that it is possible to consider not just dimensions, but separate constructs and variables. Based on an additional theoretical evidence, these could help to better understand consumers' habits of dealing with personal data.

References

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. Available from internet: https://doi.org/10.1108/JCM-06-2013-0606

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. Available from internet: https://doi.org/10.1108/OIR-10-2017-0281

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. Available from internet: https://doi.org/10.1016/j.im.2015.08.001

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius F. J. (2017). Online behavioral advertising: A literature review and research agenda. *Journal of Advertising*, *46*, 363-376. Available from internet: https://doi.org/10.1080/00913367.2017.1339368

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2018). Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data. *Communication Research*. Available from internet: https://doi.org/10.1177/0093650218800915

Coşar C., Panyi, K. & Varga, A. (2017). Try Not to Be Late! - the Importance of Delivery Service in Online Shopping, Organizations and Markets in Emerging Economies, 8(2), 177-192. Available from internet: https://doi.org/10.15388/omee.2017.8.2.14186

Estrada-Jiménez, J., Parra-Arnau, J., Rodríguez-Hoyos, A., & Forné, J. (2017). Online advertising: Analysis of privacy threats and protection approaches. *Computer Communications*, *100*, 32-51. Available from internet: https://doi.org/10.1016/j.comcom.2016.12.016

Gupta, B., Iyer, L. S., & Weisskirch, R. S. (2010). Facilitating global e-commerce: A comparison of consumers willingness to disclose personal information online in the US and in India. *Journal of electronic commerce research* 11 (1).

Heirman, W., Walrave, M., Ponnet, K., & Van Gool, E. (2013). Predicting adolescents' willingness to disclose personal information to a commercial website: Testing the applicability of a trust-based model. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 7*(3). Available from internet: https://doi.org/10.5817/CP2013-3-3

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. Available from internet: https://doi.org/10.1111/isj.12062

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. Available from internet: https://doi.org/10.1016/j.dss.2011.01.017

Li, Y. (2014). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision Support Systems*, *57*, 343–354. Available from internet: https://doi.org/10.1016/j.dss.2013.09.018

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. Available from internet: https://doi.org/10.1007/s11747-006-0003-3

Malheiros, M., Preibusch, S., & Sasse, M. A. (2013, June). "Fairly truthful": The impact of perceived effort, fairness, relevance, and sensitivity on personal data disclosure. *In International Conference on Trust and Trustworthy Computing* (pp. 250-266). Springer, Berlin, Heidelberg. Available from internet: https://doi.org/10.1007/978-3-642-38908-5_19

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. Available from internet: https://doi.org/10.1287/isre.1040.0032

Miltgen, C. L., & Smith, H. (2015). Exploring information privacy regulation, risks, trust, and behavior. *Information & Management*, *52*(6), 741–759. Available from internet: https://doi.org/10.1016/j.im.2015.06.006

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. Available from internet: https://doi.org/10.1177/1094670511424924

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of consumer affairs, 41(1), 100-126. Available from internet: https://doi.org/10.1111/j.1745-6606.2006.00070.x

Omer A., Levin D. (2015). Predictive marketing: easy ways every marketer can use customer analytics and big data. Wiley. Paine Schofield, C. B., & Joinson, A. N. (2008). Privacy, trust, and disclosure online. In A. Barak (Ed.), *Psychological aspects of cyberspace: Theory, research, applications* (pp. 13-31). Cambridge, UK: Cambridge University Press.

Olivero, N., Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: the effect of risk awareness on the relative role of trust and control, *Journal of Economic Psychology*, Vol. 25 No. 2, pp. 243-262. Available from internet: https://doi.org/10.1016/S0167-4870(02)00172-1

Park, Y. J. (2013). Digital Literacy and Privacy Behavior Online. *Communication Research*, *40*(2), 215–236. Available from internet: https://doi.org/10.1177/0093650211418338

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. Available from internet: https://www.jstor.org/stable/30000485

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. Available from internet: https://doi.org/10.1016/j.tele.2016.09.006

Robinson, S. C. (2018). Factors predicting attitude toward disclosing personal data online. *Journal of Organizational Computing and Electronic Commerce*, *28*(3), 214–233. Available from internet: https://doi.org/10.1080/10919392.2018.1482601

Rohunen, A., Markkula, J., Heikkilä, M., & Oivo, M. (2018). Explaining Diversity and Conflicts in Privacy Behavior Models. *Journal of Computer Information Systems*, 1-16. Available from internet: https://doi.org/10.1080/08874417.2018.1496804

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of public policy & marketing*, 19(1), 62-73. Available from internet: https://www.jstor.org/stable/30000488

Schoenbachler, D. D., & Gordon, G. L. (2002). Trust and customer willingness to provide information in database-driven relationship marketing. *Journal of Interactive Marketing*, *16*(3), 2–16. Available from internet: https://doi.org/10.1002/dir.10033

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, 35(4), 989-1016. Available from internet: https://doi.org/10.2307/41409970

Treiblmaier, H., & Chong, S. (2011). Trust and Perceived Risk of Personal Information as Antecedents of Online Information Disclosure. *Journal of Global Information Management*, *19*(4), 76–94. Available from internet: https://doi.org/10.4018/jgim.2011100104

Wakefield, R. (2013). The influence of user affect in online information disclosure. *The Journal of Strategic Information Systems*, *22*(2), 157–174. Available from internet: https://doi.org/10.1016/j.jsis.2013.01.003

Walrave, M., & Heirman, W. (2012). Adolescents, Online Marketing and Privacy: Predicting Adolescents' Willingness to Disclose Personal Information for Marketing Purposes. *Children & Society*, *38*. Available from internet: https://doi.org/10.1111/j.1099-0860.2011.00423.x

Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management*, *36*(4), 531–542. Available from internet: https://doi.org/10.1016/j.ijinfomgt.2016.03.003

Wang, Z., & Liu, Y. (2014). Identifying Key Factors Affecting Information Disclosure Intention in Online Shopping. *International Journal of Smart Home*, *8*(4), 47–58. Available from internet: https://doi.org/10.14257/ijsh.2014.8.4.05

Weinberger, M., Zhitomirsky-Geffet, M., & Bouhnik, D. (2017). Factors affecting users' online privacy literacy among students in Israel. *Online Information Review*, *41*(5), 655–671. Available from internet: https://doi.org/10.1108/OIR-05-2016-0127

Xu, H., Dinev, T., Smith, H., & Hart, Paul J. (2008). Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View. *ICIS 2008 Proceedings - Twenty Ninth International Conference on Information Systems*. Available from internet: https://aisel.aisnet.org/icis2008/6

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. Available from internet: https://doi.org/10.17705/1jais.00281

Journal of Business Research 136 (2021) 76–85

Contents lists available at ScienceDirect

Journal of Business Research

journal homepage: www.elsevier.com/locate/jbusres

From social networking to willingness to disclose personal data when shopping online: Modelling in the context of social exchange theory

Sigitas Urbonavicius [a,*], Mindaugas Degutis [a], Ignas Zimaitis [a], Vaida Kaduskeviciute [a], Vatroslav Skare [b]

[a] Faculty of Economics and Business Administration, Vilnius University, Sauletekio al. 9, 10222 Vilnius, Lithuania
[b] Faculty of Economics & Business, University of Zagreb, Trg J.F. Kennedya 6, 10000 Zagreb, Croatia

ARTICLE INFO

Keywords:
Willingness to disclose data
Social exchange theory
Online marketing
Trust
Paranoia

ABSTRACT

The trend toward personalized offers in online marketing requires buyers to disclose personal data. Buyers express low willingness to do this while buying online, though many are involved in social networking where sharing personal facts is routine. This study approaches this from the position of Social Exchange Theory (SET), positioning social networking and online buying as the two types of social exchange. They are influenced by trust and distrust, also considering perceptions about legal regulations of privacy and control. Based on a survey of 480 respondents, a structural equation modeling disclosed the impact of involvement in social media on the willingness of consumers to disclose personal data in online purchasing. The interaction was predicted by trust and distrust, with mediation of perceptions about the effectiveness of legal regulations. The study contributes to literature linking social networking and online purchasing in terms of data disclosure and suggesting SET for similar studies.

1. Introduction

Consumer-generated information is becoming increasingly important to businesses, and a significant part of marketing activities are based on personalized consumer data (Wieringa et al., 2019). Personal data obtained from consumers allow businesses to provide better-targeted value propositions. Therefore, businesses are highly interested in obtaining personal data from as many consumers as possible (Hong et al., 2019; Zeng et al., 2020).

From the perspective of consumers, receiving better proposals or other marketing benefits based on the personal data they provide is advantageous (Barth & Jong, 2017). However, these potential benefits are often outweighed by rational and irrational concerns, and generally, consumers are not willing to disclose their personal data (Bansal et al., 2016; Wieringa et al., 2019). The reasons for willingness or unwillingness to disclose personal data continue to receive attention from many researchers (Robinson, 2017; Zimaitis et al., 2020a).

On the other hand, the disclosure of a large scope of personal information on social networks is rather typical and occurs in various social networking formats (Jenkins-Guarnieri et al., 2013). When networking, people seem willing to disclose not just personal demographic parameters, but also numerous personal facts, experiences, and opinions. This seems somewhat inconsistent with the low levels of willingness to disclose personal data in online purchasing. Though self-disclosure on social networks has been studied extensively from the perspective of privacy calculus (Krasnova et al., 2010; Lee & Yuan, 2020), by employing the Technology Acceptance Model (Zhao et al., 2018), and through knowledge-sharing models (Kim et al., 2015), it has not been linked directly with online-buying behavior. The issue presents a noticeable research gap, which this study attempts to address by analyzing the problem of the linkage between social networking and online purchasing in terms of personal data disclosure.

However, this aim seems to be unachievable on the basis of the theoretical backgrounds that are widely used for studies on willingness to disclose personal data online. Some studies start with the concept of a cost-benefit analysis, which is applicable when personal information is treated as a commodity (Smith et al., 2011). This approach, known as privacy calculus, states that consumers disclose their personal information in exchange for benefits (Barth & Jong, 2017; Robinson, 2017). However, the privacy calculus approach has been criticized for its

* Corresponding author.
E-mail addresses: sigitas.urbonavicius@evaf.vu.lt (S. Urbonavicius), mindaugas.degutis@evaf.vu.lt (M. Degutis), ignas.zimaitis@evaf.vu.lt (I. Zimaitis), vaida.kaduskeviciute@evaf.vu.lt (V. Kaduskeviciute), vskare@efzg.hr (V. Skare).

https://doi.org/10.1016/j.jbusres.2021.07.031
Received 5 December 2020; Received in revised form 10 July 2021; Accepted 14 July 2021
Available online 24 July 2021

overestimation of the rationality argument (Kehr et al., 2015; Wakefield, 2013) and is therefore hardly applicable when social networking is considered, since the benefits of networking are not necessarily rational. This suggests that data disclosure on social networks is grounded on something other than just rationality (Zhang & Fu, 2020).

It is widely acknowledged that privacy-related decisions are mostly situational and strongly dependent on the purpose and context of the information disclosure (Malhotra et al., 2004; Bansal et al., 2016; Omrani & Soulié, 2018; Masur, 2019). The contexts of online purchasing and social networking vary from ones that are precisely formalized and regulated to others that are mainly based on reciprocity and the mutual trust of the interacting participants. Both these instances are recognizable within the scope of Social Exchange Theory (SET), which defines them as negotiated and reciprocal types of social exchange.

The negotiated social exchange occurs in legally regulated exchanges of information where the consumer is aware of how the information will be processed and what, when, and how a benefit for the information disclosure will be provided. Additionally, consumers may be aware of and assured by external regulatory systems that supervise and control how transactions, including personal data disclosure, are carried out. This typically occurs in online shopping situations where transactions are strictly formalized and handled by responsible sellers who are additionally controlled by legal systems. If these systems function as intended, the level of personal data disclosure risks and uncertainties would be low. Nevertheless, online buyers typically declare low willingness to disclose personal data (Barth & Jong, 2017; Zeng et al., 2020).

Another extreme occurs in situations where information-exchanging participants assume no formal obligations and relatively little is regulated by legal systems/institutions. The disclosure and exchange of information is mainly based on reciprocity and mutual trust, with no formal guarantees regarding the handling and use of disclosed information. This is evident in social networking, where various types of personal information are disclosed to generate/maintain a rather emotional socialization process (Zhang & Fu, 2020).

This study focuses mainly on personal data disclosure in online buying representing negotiated exchanges (King, 2018; Morgan-Thomas et al., 2020). SET helps to predict that involvement in trust-based reciprocal exchanges may stimulate overall engagement in a digital ecosystem and increase willingness to disclose data in a negotiated exchange (Yang, 2019). This can ultimately contribute to the conceptual grounding and empirical evidence of this relationship, and address the research gap in the relationship between social networking and online purchasing in terms of personal data disclosure.

Since data disclosure in social networking and online buying are largely predicted by trust/distrust factors, the key antecedents of the current study include trust and paranoia (an extreme version of distrust). Perceptions regarding personal control over data disclosure and the effectiveness of legal regulations (such as the General Data Protection Regulation [GDPR]) are two important mediators in modeling the relationship with willingness to disclose data (Lwin et al., 2007; Kehr et al., 2015; Miltgen & Smith, 2015; Zimaitis et al., 2020a). More specifically, trust is understood as an important antecedent of reciprocal relationships (Yang, 2019) and the perceptions of regulatory bodies and systems (Davidovic & Harring, 2020). Paranoia was found to be related to privacy concerns and levels of trust (Gromann et al., 2013; Imhoff & Lamberty, 2018), as well overall involvement in social networking (Zimaitis et al., 2020b), and therefore also provides an important contribution to the modeling of personal data disclosure.

This study concentrates on negotiated exchanges with well-predefined situations in which data is being disclosed (in the process of searching for and purchasing products online). This allows for the omission of other situational factors and to focus on the key dispositional factors (Urbonavičius, 2020). This approach allows for the modeling of interactions on the basis of SET and an analysis of the survey data from a new perspective. The study contributes to the existing literature in three ways. First, using SET as a theoretical background for a study on data disclosure opens new opportunities to conceptualize various situations of personal data disclosure. This specific study formulates the disclosure of personal data in online buying as a case of negotiated exchange, while in social networking – as reciprocal exchange. Second, the study empirically confirms the relationship between the two types of social exchange, demonstrating the influence of reciprocal exchanges on negotiated exchanges and, particularly, on the willingness of individuals to disclose personal data in online buying. In other words, it shows how involvement in social media is linked to the willingness to disclose personal data in a seemingly unrelated situation, i.e. – in online purchasing. This research contribution has implications for further studies, encouraging broader applications of SET in business and, specifically, in marketing settings. Also, the developed model takes perceptions about the legal regulations of privacy into consideration, which are crucial for making them efficient. This allows for the empirical findings to be linked with legal privacy regulations (including the still widely discussed GDPR), as well as for the development of managerial implications and policy-making insights regarding online privacy. The findings, conclusions and recommendations are based on a robust model and strong empirical evidence.

2. Theoretical background

This study employs SET as a background for analyzing consumer perceptions of personal information disclosure. Rooted in the conceptual writings of the sociologists George C. Homans (1961), Phillip Blau (1964), and Richard Emerson (1976), SET applies theoretical principles of microeconomics to analyze social behavior. The justification for using SET in marketing is based on the belief that the roots of marketing are intrinsically found in social exchange theory (Bagozzi, 1975). Varey (2015) argued that, "…originating in the nexus of economics, psychology, sociology, and anthropology, and the concept of contract, social exchange thinking has become embedded in the marketing discipline, so much so that recent textbooks reproducing the convention do not mention it explicitly at all." (p. 1) SET is used extensively to explain business-to-business marketing issues (Lambe et al., 2001), loyalty in the service industry (Sierra & McQuitty, 2005), and privacy-related consumer behaviors and attitudes (Metzger, 2004; King, 2018).

Long ago, social exchange theorists classified information as one of the exchanged resources (Foa & Foa, 1974). Cheshire (2007) argued that information can be a valuable resource of exchange as it is, "much like any other good, since it can be transferred and it has value." (p. 83). Therefore, disclosure of personal information in online purchasing is one of the processes of social exchange. Exchange participants expect to gain benefits, and the exchange is typically recurrent by nature and structured by the interdependence and power relations of the exchange partners.

Early SET thinkers defined the distinction between negotiated and reciprocal exchanges (Lévi-Strauss, 1969; Emerson, 1981). The negotiated exchange assumes that exchange partners know the terms of an exchange, which are agreed upon in advance. The parties are aware of the benefits they acquire as well as the costs related to the exchange. Also, timing and other settings are defined a priori. The majority of social exchanges that include economic activities are negotiated ones (Molm et al., 2000). The reciprocal exchange is based on individual expectations that other participants will reciprocate in exchange for the delivered resources. The extent, forms and other aspects of reciprocity are not granted in advance; exchange relations are developed during the process of trust-based, sequential, mutual exchange transactions (Molm et al., 2000). When it comes to sharing personal information, social media involvement is a good example of a situation with a reciprocal exchange of personal information (Yang, 2019). People share personal information on social media in exchange for social support, recognition, and other benefits they expect from their exchange partners (Szymczak et al., 2016). No one is formally obliged to reciprocate to a certain extent or based on a time constraint.

The majority of personal information exchange situations in e-commerce (purchasing, browsing online) are examples of the negotiated exchange. Marketers collect personal information in exchange for the offered benefits: access, convenience, or monetary compensation in the form of discounts or bonuses (Malgieri & Custers, 2018) and the process is formalized by terms of agreement or permissions to use personal data. Additionally, exchange terms are typically backed by international, national, or local legal assurance systems. Therefore, willingness to disclose personal data largely depends on the perceptions of formal assurances (Hong et al., 2019), trust (Bansal et al., 2016), and uncertainties (Mothersbaugh et al., 2012).

Uncertainties and concerns are inherent attributes of any exchange relation (Molm et al., 2000); however, they do vary depending on the type of exchange relation. Reciprocal exchange relations are more exposed to uncertainty because partners are never sure if the other side will reciprocate, or if they will get a benefit in exchange for the provided personal information. Uncertainty and lack of control could be less important in negotiated exchange relations where participants know the terms and benefits they will receive in advance. Ideally, once an agreement is reached, uncertainty should be eliminated from this type of exchange (Molm et al., 2000). However, even in negotiated situations not everything is precisely defined: the terms may not be strictly binding (Heckathorn, 1985), time lags between the promise and the delivery may create opportunities for defection (Coleman, 1990), and the value of the obtained resources may be unclear (Kollock, 1994). Therefore, perception of the lack of control remains the immanent characteristic of the negotiated exchange.

As Molm et al. (2000) state, "trust is more likely to develop in reciprocal exchanges than in negotiated exchanges." (p. 1403). In cases of negotiated exchange, trust is largely expressed in a form of *assurance* (Yamagishi & Yamagishi, 1994). Negotiated (binding) exchange relations rely heavily on assurance structures: legal and normative authorities that define, supervise, and impose sanctions for violating the terms of agreement. A good example of an assurance scheme regarding online data disclosure is the GDPR, which has been in effect in the EU since 2018. The presence of an assurance system is intended to lower the reliance on mutual trust and reinforce the willingness to disclose personal data in online purchasing. The element of trust is still present; however, it is mainly directed towards the perception of the regulatory effectiveness of the assurance schemes.

Reciprocal exchange relations do not require assurance systems; therefore, they might seem riskier. However, this may be offset by trust that is present or developed during the exchange process (Molm et al., 2000; King, 2018). The participants of an exchange process either come to the relationship with a certain level of trust in others (high personal propensity to trust others) or develop it during the mutual exchange of resources, as in the process of social networking. Therefore, the relation of trust and willingness to participate in a reciprocal exchange is twofold. People who have a higher propensity to trust others are more likely to engage in a reciprocal exchange. Additionally, trust develops if the exchange participants reciprocate, and at each stage, their willingness to share resources increases. This allows us to propose that involvement in reciprocal exchanges impacts the willingness to disclose personal information in general, including instances of negotiated exchange.

Trust and distrust asymmetrically affect behaviors with different risk levels (Chang & Fang, 2013). Therefore, modeling of the willingness to disclose personal data would be incomplete without considering paranoia, which represents an extreme form of distrust (Kramer, 2008). Paranoia is described as, "persecutory delusions, false beliefs whose propositional content clusters around the ideas of being harassed, threatened, harmed, subjugated, persecuted, accused, mistreated … by the malevolent others," (Colby, 1981, p. 518) and is defined as a common human trait, not a clinical condition (Ellett et al., 2003, Della Libera, et al., 2020). This means that in addition to the aspect of general distrust, paranoia also includes the feeling of potential threat posed by other people, thus expanding the trust-distrust continuum toward a more radical approach with regard to social interactions. The relation between paranoia and online activities has not yet been widely studied; however, existing studies suggest that paranoia is positively related to internet use and involvement in social media (Mason et al., 2014; Urbonavičius & Zimaitis, 2018; Zimaitis et al., 2020b). The availability of large amounts of information on the internet contributes to the development and spread of conspiracy theories, which fuel paranoia (Parish & Parker, 2001; Fenster, 2008). Paranoid people look for support and confirmation of their feelings on social media, which leads to higher involvement in social media and the exchange of personal information with others.

This study employs SET to address a research gap in the knowledge of interaction between social networking and willingness to disclose personal data in online purchasing. This approach stands apart from the most typical theoretical backgrounds that have been used for modeling data disclosure: the commodity view of privacy (Kehr, et al, 2015), Privacy Calculus (Dinev, & Hart, 2006; Wang, et al, 2016) and privacy paradox (Norberg, et al, 2007; Barth & Jong, 2017). However, it includes the elements of the above-mentioned approaches: it considers personal data a valuable asset for an exchange and links disclosure with behaviors (social networking). At the same time, SET allows major emphasis to be put on the trust/distrust that have been less directly addressed in studies using other theoretical approaches.

3. Model and hypotheses

Research on e-behaviors often take the trust factor into consideration; however, the distrust factor is seldom included in studies (Chang & Fang, 2013). The use of SET allowed this study to develop a model that integrates both trust and distrust factors, and link them to two online activities: social networking and online purchasing. The dependent variable in the model is the willingness to disclose personal data in online shopping, which represents the case of negotiated exchange. This negotiated exchange is impacted by the trust-generating experiences of reciprocal exchange, represented by involvement in social media. This is based on evidence that increased involvement in social media requires more frequent disclosure of personal data, and the accumulated experience in disclosing information impacts the willingness to disclose personal data in other settings, including online buying. The model also includes the impact of perceived regulatory effectiveness (assurance systems) and perceived lack of control (uncertainty) on the willingness to disclose personal data in exchange for benefits in online purchasing (Smith et al., 2011). These two factors serve as mediators between trust and the extreme form of distrust (paranoia), and willingness to disclose personal data in online purchasing. The analysis of their known and/or predicted interactions allows a research model (Fig. 1) and hypotheses to be developed.

The exploratory nature of the study requires an assessment of each outlined direct relationship, since the interactions between the variables under research are largely unknown. However, they can be predicted either on the basis of the existing (though limited) scope of knowledge or grounded by the SET postulates of the nature of the factors themselves.

Based on SET, continuous non-formalized interactions of a reciprocal nature build trust between interacting parties, such as peers on social networks (Sherchan et al., 2013). Higher involvement in social networking requires more frequent disclosure of personal data, generates a higher level of trust among the participants (Sherchan et al., 2013), and produces an overall higher level of engagement in a broader digital ecosystem, including online buying. This leads to the proposal that higher involvement in social networking positively influences the willingness to disclose personal data in a negotiated exchange, represented by e-buying.

H1. Involvement in social media positively influences the willingness to disclose personal data in e-commerce.

In negotiated interactions between a person and an institution (a

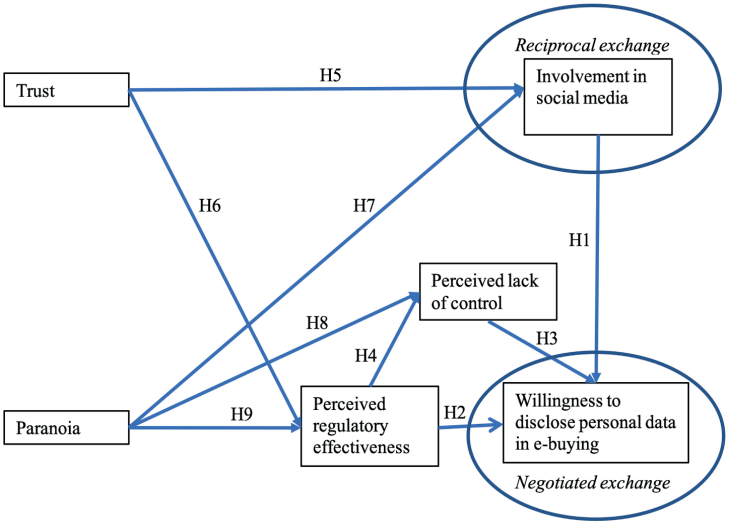

Fig. 1. Research Model.

marketer), an individual may perceive an imbalance in the control over disclosed data (Sharma & Crossler, 2014). Understanding the terms and conditions of personal control over data disclosure allows the consumer to believe that somebody (legal systems, organizations) is efficient enough to warrant its proper use (Weil et al., 2005; Gefen & Pavlou, 2006). If a person perceives the regulations to be effective, the willingness to disclose personal information will increase. On the other hand, this does not offset all potential uncertainties, especially if the legal regulations or privacy policies are presented improperly (Meier, Schäwel & Krämer, 2020). It is typical that a person perceives a certain degree of lack of control over the process and over the provided data in online purchasing (Wang et al, 2016; Zimaitis et al., 2020a). Therefore, disclosure of data is linked with hesitations and uncertainties due to the perception that a person loses control over the data (Smith et al., 2011; Hong & Thong, 2013; Wang et al., 2016; Morimoto, 2020). Naturally, this perception reduces the willingness to disclose data. These arguments lead to the prediction that perceived regulatory effectiveness impacts the willingness to disclose personal data positively, while the perceived lack of control – negatively.

H2. Perceived regulatory effectiveness positively influences the willingness to disclose personal data in e-commerce.

H3. Perceived lack of control negatively influences the willingness to disclose personal data in e-commerce.

Control over the process of exchange can be shared not only with other participants of the exchange, but also with the third parties regulating it. The legal systems and relevant institutions regulating privacy policies in online buying and selling take part of the control over the process (Gefen & Pavlou, 2006). This increases the perception that personal control over the exchange, which includes personal data disclosure, is rather limited. If the regulation is perceived as being effective, the feeling of lack of personal control becomes even stronger.

H4. Perceived regulatory effectiveness positively influences the perceived lack of control.

To model how involvement in social media, perceived regulatory effectiveness, and perceived lack of control impact the willingness to disclose personal data, the influence of trust/distrust antecedents have to be predicted.

Trust is a key element of any type of a social exchange and stands at the very core of the concept of SET, which emphasizes the importance of trust as a predictor of social interactions and as a result that is developed in the process of social interactions. (Molm et al., 2000). Therefore, the concept of trust needs to be understood in at least two different ways.

First, dispositional trust (propensity to trust something) is a human trait that is present in everyone to a certain degree (Frazier et al., 2013). This is a typical antecedent for the perceptions and activities regarding interactions with other people or their groups, institutions, regulatory systems, etc. (Bansal et al., 2016). Another form of trust – situational trust – expressed with regard to concrete objects (most typical cases in marketing – types of stores, products, specific brands) that occurs in specific situations or within a specific context (Heirman et al., 2013). Both types of trust typically encourage online behaviors, while privacy violations reduce trust and negatively impact future online activities (Martin, 2018).

Furthermore, both types of trust are well recognizable in the involvement in social networking: networking is triggered by the propensity to trust, and situational trust can be gradually developed during reciprocal exchanges in the process of interactions with social partners, as well as with social networking platforms (Molm et al., 2000; Sherchan et al., 2013). Since the level of trust in social networking predetermines the involvement in social media activities, the positive relation between the trust (propensity to trust) and involvement in social media may be predicted. Though the positive relationship between trust and involvement in social media seems rather clear, it remains an important aspect of research on privacy concerns and consumer trust in social media (Appel et al., 2020). Therefore, the hypothesis states:

H5. Trust positively influences involvement in social media.

The propensity to trust (trust trait) also predetermines the trust in institutions/regulatory systems and helps develop positive perceptions of them (Szymczak et al., 2016; Zhang et al., 2019; Zhao et al., 2018). Therefore, trust should positively influence the perception of privacy regulation effectiveness.

H6. Trust positively influences perceived regulatory effectiveness.

However, it is inappropriate to assume that the consequences of trust on online behaviors are opposite to those of distrust (Chang & Fang, 2013). Instead, a separate assessment of the impact of distrust has to be made. This is achievable with the use of the factor of paranoia, which is understood as an extreme form of distrust (Kramer, 2008).

Excluding clinical contexts, paranoia is a rather general irrational personal state grounded in the distrust of others (Gromann et al., 2013). Its impact on the analyzed variables is largely unknown due to the

limited scope of prior research. However, there are some insights that suggest initial ideas for analysis and allow for a prediction to be made about its relationships with the factors included in this study.

The relation between paranoia and social media use is rather unclear. Since paranoia means distrust of others, it should negatively influence one's social interactions (Jack & Egan, 2018). On the other hand, social media is the source of the clash of conflicting ideas, including ones that support paranoid thinking. A large number of studies have attempted to demonstrate the impact of social media use on risk for mental health symptoms and poor wellbeing (Naslund et al., 2020). However, a specific relationship with paranoia has been not been detected (Bird et al., 2017; Berry et al., 2018). One of the arguments states that the relationship and causality were assessed in a wrong way; i.e. social media use was not a reason, but a consequence of paranoia (Bird et al., 2019). This confirms the directionality that is foreseen in the current study; however, it does not help in predicting whether the relationship is positive or negative.

The very concept of paranoia suggests that a person who is prone to paranoid thinking has a fear of missing out, and social media use provides rewarding experiences (Fuster et al., 2017). Paranoia should thus encourage social media use, which is an assumption supported by a rather limited scope of research that specifically analyzes the impact of paranoia on social media involvement (Zimaitis et al., 2020b). Therefore, we predict a positive influence of paranoia on the involvement in social media.

H7. Paranoia positively influences involvement in social media.

On the other hand, paranoid thinking generates feelings of personal vulnerability and exaggerated socially evaluative concerns (Meisel et al., 2018). Paranoid thinking is full of concerns about all kinds of possible imperfections in everything. There is fragmented evidence that paranoia is positively associated with the lack of personal control, but it is also strongly suggested to gain a better understanding of its impact on the various types of control (Imhoff & Lamberty, 2018). Therefore, we hypothesize:

H8. Paranoia positively influences perceived lack of control.

It is understood that paranoid individuals fail to correspond to any group in wider society who share coordinated aims and actions (Raihani & Bell, 2019). Therefore, paranoid thinking gravitates towards ignoring and neglecting systems, rules and organizational efforts with an dysregulated response (Saalfeld et al., 2018) and is prominently associated with low trust in the government (Imhoff & Lamberty, 2018). This leads to the neglection of effectiveness of external regulations:

H9. Paranoia negatively influences perceived regulatory effectiveness.

4. Measures and data

Data was collected through an online survey during the period of December 13, 2019 and February 2, 2020. All variables were measured using scales successfully deployed in former studies. Trust (TR) was assessed on a four-item "Propensity to Trust" scale (Frazier et al., 2013). Paranoia (PAR) was measured with the original paranoia trait scale (Fenigstein & Vanable, 1992), which was shortened to six items; shorter versions of this scale were successfully used by Urbonavičius & Zimaitis (2018) and Zimaitis et al. (2020b). Involvement in Social Media (ISM) was measured following the Social Media Use Integration Scale (SMUIS) developed by Jenkins-Guarnieri et al. (2013). Measured with 10 items, it takes into account engaged social media use, emotional attachment to social media use, and the social habits of users. This allowed us to address important aspects of involvement in social media with a construct that stays unidimensional (Jenkins-Guarnieri et al., 2013; Zimaitis et al, 2020a; Zimaitis et al., 2020b). The Willingness To Disclose (WTD) personal data was assessed with the scale suggested by Gupta et al. (2010) and Heirman et al. (2013), later used by Robinson (2017) and Degutis et al. (2020). To avoid the effects of rapid dynamics in the types of data disclosed online, the list was reduced to items that are relatively stable and represent personal demographics and contact information (seven items). The Perceived Regulatory Effectiveness (PRE) three-item scale was adopted from Lwin et al. (2007) with a minor modification – GDPR, as an example of one type of legal regulation, was included into one item. A three-item scale of Perceived Lack of Control (PLC) was taken from Wang et al. (2016). In all instances, a 1 to 7 Likert scale (1 = *totally disagree* and 7 = *totally agree*) was used. Detailed information regarding the scales is provided in Appendix 1.

The data was collected in Lithuania using an online self-administered survey. Lithuania was chosen due to the fact that it is among the leaders in the infrastructure of Wi-Fi and broadband use[1] as well as in overall development of digital infrastructure for individuals and businesses (Castelo-Branco et al., 2019). Additionally, as an EU country, Lithuania has implemented the GDPR, one of the world's strictest regulations regarding personal data collection and processing.

The analysis was carried out based on 480 respondents. The sample included 25.6% male and 74.4 % female respondents in three age groups: 16–29 (33.5%); 30–49 (29.2%); 50 and over (37.3%). Of them, 43.1% were from the capital city, 22.5% from other larger cities, and the remaining 34.2% were from smaller cities and rural areas. 39.2% of respondents had university degrees, while others had various types of non-university education backgrounds.

5. Analysis

The scales were assessed using an exploratory factor analysis, subsequent confirmatory factor analysis, and tests of reliability and validity. The exploratory factor analysis (Promax rotation, Maximum Likelihood extraction) was used for the initial assessment of the scales. The KMO was adequate (0.797) and the Bartlett's Test of Sphericity showed approx. Chi-Square of 5727.640, with df = 276, $p < 0.001$. The model had a good fit, Chi-Square = 432.978, df = 147, $p < 0.001$, and extracted six factors that explained 59.93% of variation with cumulative initial Eigenvalues of 69.56%. A subsequent confirmatory factor analysis showed an acceptable fit of the model (CMIN/DF = 1.525; TLI = 0.947; CFI = 0.978; RMSEA = 0.033 (Byrne, 2010). This was achieved by reducing the ISM scale to six items, PAR to three items and WTD to five items. The reliability and validity of the obtained scales was assessed by measuring the composite reliability (above 0.70, Bagozzi & Yi, 2012). As recommended by the Fornell-Larcker criteria (Fornell & Larcker, 1981), all the standardized factor loadings exceeded 0.50; the average variance extracted (AVE) exceeded 0.50; and squared AVE values for each construct were greater than the correlation values of that construct. All these criteria were met (Table 1), which allowed us to perform further analysis.

A common latent bias test was used to compare unconstrained and fully constrained models; the test came back positive (difference in chi-square = 68.1, difference in df = 24, $p < 0.001$). The latent bias corrected model had an appropriate fit: CMIN/DF = 1.525; TLI = 0.947; CFI = 0.978; RMSEA = 0.033.

The structural model (CMIN/DF = 2.006; TLI = 0.958; CFI = 0.986; RMSEA = 0.046; PCLOSE = 0.503) was robust and allowed to proceed with further analysis.

As is typical in explorative models that suggest using a new theoretical approach (SET), attention was paid primarily to the direct relationships between the factors. Therefore, these relationships are predicted in the formulations of the hypotheses. Based on them, the total and indirect (mediated) effects can be measured. These relationships are not hypothesized and serve two other purposes: (a) confirming the appropriateness of modeling on the basis of SET and (b) outlining the

[1] OECD broadband statistics update. Paris, 22 July 2020: https://www.oecd.org/sti/broadband/broadband-statistics-update.htm; Ooma, Best and Worst Countries for Wi-Fi Access: https://www.ooma.com/blog/best-worst-wifi-countries.

Table 1
Validity and Reliability of Constructs.

	Cronbach's Alpha	CR	AVE	PRE	PLC	ISM	WTD	PAR	TR
PRE	0.863	0.865	0.615	**0.784**					
PLC	0.809	0.812	0.590	0.173	**0.768**				
ISM	0.923	0.924	0.802	−0.091	0.145	**0.896**			
WTD	0.872	0.862	0.513	0.056	0.101	0.079	**0.716**		
PAR	0.852	0.835	0.507	0.062	0.139	−0.164	0.256	**0.712**	
TR	0.781	0.779	0.541	−0.304	0.129	0.300	0.277	0.091	**0.735**

Note: PRE – Perceived regulatory effectiveness, PLC – Perceived Lack of Control, ISM – Involvement in Social Media, WTD – Willingness to Disclose Data, PAR – Paranoia TR – Trust, CR – composite reliability, AVE – average variance extracted

directions for future research.

The causal model (Fig. 2) tests the relationships that are predicted in the research model and confirms its structure. First of all, structural equation modeling assumes a correlation between the antecedents. In this model, this relationship confirms the correctness of the modeling assumption that propensity to trust and paranoia represent trust and distrust, since their relation is strongly negative (correlation −0.353; $p < 0.001$).

All predicted direct relationships between variables are significant at the level $p < 0.001$. Additionally, all standardized regression weights are substantial, ranging from 0.19 to 0.39, which means a relatively high explanatory power of each individual direct relationship. However, this also allows for an analysis of all indirect and total effects, which additionally contribute to the understanding of how the willingness to disclose personal data is influenced by the analyzed factors.

As it was modeled, trust and paranoia do not have direct effects on willingness to disclose personal data in e-shopping. The standardized total effect of trust is $\beta = 0.101$; $p < 0.001$; and the standardized total effect of paranoia is $\beta = 0.060$; $p < 0.001$. This confirms that the factor of trust/distrust is important in modeling willingness to disclose personal data on the basis of SET. However, the positive total effect of paranoia is unexpected and largely predetermined by its positive (opposite to what was predicted) influence of paranoia on perceived regulatory effectiveness. This is discussed further in the text.

The influence of perceived regulatory effectiveness on willingness to disclose personal data is twofold: both direct and mediated, which means the presence of partial mediation. The standardized total effect is $\beta = 0.149$; $p < 0.001$; this is generated by the standardized direct effect of $\beta = 0.201$ ($p < 0.001$) and the standardized indirect effect of $\beta =$ -0.052 ($p < 0.001$). The negative indirect effect is predetermined by the strong negative influence of the mediator (perceived lack of control) on the willingness to disclose data ($\beta =$ -0.277 ($p < 0.001$).

An analysis of all direct relationships allows for the hypotheses to be tested (Table 2).

All but one of the hypotheses confirmed the predicted relationships. Hypothesis H9 (paranoia negatively influences the perceived regulatory effectiveness) was rejected, since the relation between the variables was significant, but positive (opposite to what was predicted). All these findings require a more detailed discussion.

6. Discussion, conclusions, and implications

This study's main contribution to the scope of knowledge about the willingness to disclose data online lies in the suggested use of SET as the background for the analysis and findings. The study revealed that reciprocal exchange (involvement in social media) strongly impacts the

Table 2
Tests of Hypotheses (standardized regression weights).

Hypothesized Impacts				Estimate	P	Result
H1	**WTD**	←	**ISM**	0.271	***	Accepted
H2	**WTD**	←	**PRE**	0.166	***	Accepted
H3	**WTD**	←	**PLC**	−0.308	***	Accepted
H4	**PLC**	←	**PRE**	0.187	***	Accepted
H5	**ISM**	←	**TR**	0.204	***	Accepted
H6	**PRE**	←	**TR**	0.264	***	Accepted
H7	**ISM**	←	**PAR**	0.442	***	Accepted
H8	**PLC**	←	**PAR**	0.249	***	Accepted
H9	**PRE**	←	**PAR**	0.231	***	Rejected

Note: PRE – Perceived regulatory effectiveness, PLC – Perceived Lack of Control, ISM – Involvement in Social Media, WTD – Willingness to Disclose Data, PAR – Paranoia TR – Trust, *** significance $p < 0.001$.

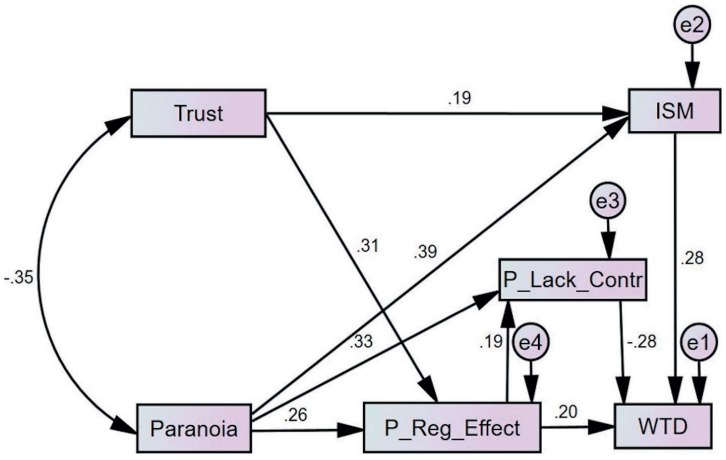

Fig. 2. Causal Model.

willingness to disclose personal data in negotiated exchange settings (buying online). This means that trust-generating reciprocal exchange increases the trust in another type of exchange and increases the willingness to disclose personal data there. Therefore, willingness develops throughout the entire digital ecosystem (Morgan-Thomas et al., 2020), and these findings extend previous knowledge in this area (Yang, 2019). Involvement in social media has no impact on willingness with mediation of the perceived lack of control, which confirms that it influences willingness to disclose personal data only directly.

From the other side, willingness to disclose personal data was positively impacted by perceived regulatory effectiveness, as was expected based on former observations of the importance of legal assurance (Yamagishi & Yamagishi, 1994). Also, as was expected, willingness to disclose personal data was negatively impacted by the perceived lack of control, which represents uncertainties that are present in personal data disclosure situations and supports the earlier observations of Bansal et al. (2016) on the link between uncertainty avoidance and disclosure of personal data.

Both involvement in social media and perceived regulatory effectiveness had a strong impact from trust. This allows to conclude that trust is an important antecedent of willingness to disclose personal data in buying online, but impacts it indirectly via reciprocal interactions in social media and via the perception of the assurance of regulatory systems.

The dispositional antecedent that represents distrust (paranoia) was expected to positively influence involvement in social media and perceived lack of control, but negatively influence perceived regulatory effectiveness. The first two hypotheses have been confirmed, and this corresponds to the findings of earlier studies (Zimaitis et al., 2020a). However, the relationship between paranoia and perceived regulatory effectiveness was significant, but positive. This means that the assumptions used for grounding the hypothesis – paranoid people fail to coordinate their actions with wider groups, ignore rules and regulations (Saalfeld et al., 2018; Imhoff & Lamberty, 2018; Raihani & Bell, 2019) – were not sufficient enough to predict the relationship. At the same time, the relationship between the two factors was significant, which confirms the correctness of the overall modeling, though it seems that this under-researched relationship should be grounded differently.

Paranoia includes not just the aspect of distrust, but also ideas about being harassed, threatened, harmed, persecuted, or mistreated by other people (Colby, 1981). This might mean that a person that exhibits paranoid thinking distrusts other people and looks for support against them in the regulations of legal bodies. Higher levels of paranoia might trigger a higher willingness to perceive that legal regulations might help in safeguarding against the negative intentions of "malevolent others". If this logic is correct, it would justify the positive relationship between paranoia and perceived regulatory effectiveness. However, this requires strong evidence from future studies.

In general, despite the limited earlier evidence of some predicted relationships, the modeling of the considered variables based on SET is relevant and allows managerial insights and outline directions to be developed for further studies.

Having observed a positive impact of perceived regulatory effectiveness on willingness to disclose personal data, the obvious suggestion for businesses would be to unambiguously support the presence of an effective regulatory system (national or international). Regulatory systems have to be reflected in policies of e-stores, and these policies need to be presented to the buyers in a short and clear manner (Meier, et al., 2020). This is an important pre-requisite for the perception about the effectiveness of a regulatory system, which is a critical factor in willingness to disclose personal data.

Another important factor is perception about control over disclosed data. The perception about lack of control is partially offset by the effectiveness of legal regulations. However, it signals that businesses should use all available means to inform buyers about how they could control disclosed information, and in this way reduce the perception of lack of control. Providing clear information regarding personal data handling and inviting users to make decisions about how their information should be used would strongly increase overall willingness to share personal data.

Also, it seems that communication on social media is very suitable in terms of developing trust. Intensive use of social networks strongly increases willingness to disclose personal data outside of the networking context. Therefore, the suggestion for business is to integrate marketing activities with social media and invite users to connect to e-stores using social media accounts as often as possible.

This needs to be summarized with an implication addressed toward policy-makers. Since a buyer's willingness to disclose their personal data is subject to their perceptions about regulation effectiveness and control, the population needs to be made aware to the highest possible level about their rights regarding privacy, as well as the mechanisms that regulate and control the use and sanction the misuse of personal data. Public policy should be strongly oriented toward educating consumers about regulatory systems.

7. Limitations and future research

The current study has several limitations; some of which indicate opportunities for future research.

One of the limitations is the gender imbalance in the sample. Though the comparison of means of all measured variables demonstrated no differences among male and female groups of respondents, the disproportion of this type needs to be avoided in similar studies.

The study was carried out in a country characterized by a high level of Wi-Fi accessibility and a well-developed internet infrastructure. It largely represents the broad context of the EU, where GDPR is followed. However, it would be valuable to replicate the study in different (less strict) regulatory environments that may predetermine different levels of consumer trust and the perception of the effectiveness of regulatory systems. Therefore, a comparison of the effects in various regulatory environments presents a promising research direction.

This study concentrates on dispositional factors, while data disclosure might also be impacted by situational factors (Sharma & Crossler, 2014; Masur, 2019). This opens a broad range of opportunities to elaborate on the suggested model while considering purchase importance, urgency, perceptions regarding the specific online store, and many more. It seems that a research direction that considers situational factors would be really broad and include wide range of opportunities.

Additionally, since the SET framework includes the aspect of power relations of exchange participants, the inequality of power among them may be included to explain why exchange participants declare limited willingness to disclose data but are highly involved in social media, where date disclosure is routine. The use of SET also allows the perception of benefits that are obtained for data disclosure to be considered. Therefore, one more broad direction for future research includes elaborating on opportunities when using SET in studies on data disclosure.

And finally, the presence of a positive relationship between paranoia and perceived regulatory effectiveness needs further elaboration. Due to a rather limited number of studies on paranoia in non-clinical contexts, the interpretations of these findings need to be supported by additional evidence, which represents another specific research direction.

Funding

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

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix 1

Scales and Their Sources

Variable and Scale Items	Source
Trust (TR) – Propensity to Trust scale:	Frazier et al. (2013)
I usually trust people until they give me a reason not to trust them	
Trusting another person is not difficult for me	
My typical approach is to trust new acquaintances until they prove I should not trust them	
My tendency to trust others is high	
Paranoia (PAR) – shortened version of Paranoia Trait scale	Fenigstein & Vanable (1992)
Someone has it in for me	
I sometimes feel as if I'm being followed	
I often wonder what hidden reason another person may have for doing something nice for you	
It is safer to trust no one	
I have often felt that strangers were looking at me critically	
I tend to be on my guard to people who are somewhat more friendly than expected	
Involvement in social media (ISM) – Social Media Use Integration (SMUIS)	Jenkins-Guarnieri et al. (2013)
I feel disconnected from friends when I have not logged into social networkI would like it if everyone used social networks to communicateI would be disappointed if I could not use social networks at allI get upset when I can't log on to social networkI prefer to communicate with others mainly through social networksSocial networks play an important role in my social relationshipsI enjoy checking my social network accountI don't like to use social networksUsing social networks is part of my everyday routineI respond to content that others share using social networks	
Willingness to disclose personal data (WTD) – short version of the scale:	Gupta et al. (2010) and Heirman et al. (2013)
While purchasing goods or services in online, you are often asked to provide to them your personal data. Please, specify, how much are you willing to provide personal data of each type:	
Home address	
Mobile phone number	
Email address	
Date of birth	
Marital status	
Name	
Last name	
Gender	
Perceived regulatory effectiveness (PRE):	Lwin et al. (2007)
The existing laws in my country and internationally, (such as General Data Protection Regulation, GDPR)* are sufficient to protect consumers' online privacy	
There are stringent international laws to protect personal information of individuals on the Internet	
The government is doing enough to ensure that consumers are protected against online privacy violations	
Perceived lack of control (PLC) – Perceived Control scale:	Wang et al. (2016)
I am usually bothered when I do not have control over personal information that I provide to online stores*	
I am usually bothered when I do not have control over personal information or autonomy over decisions about how my personal information is collected, used and shared by online stores*	
I am concerned when personal information control is lost or unwillingly reduced as a result of a marketing transaction with online stores*	

*Modifications of the original statements

References

Appel, G., Grewal, L., Hadi, R., & Stephen, A. T. (2020). The future of social media in marketing. *Journal of the Academy of Marketing Science, 48*(1), 79–95. https://doi.org/10.1007/s11747-019-00695-1.

Bagozzi, R. P. (1975). Social Exchange in Marketing. *Journal of the Academy of Marketing Science, 3*(2), 314–327. https://doi.org/10.1177/009207037500300222.

Bagozzi, R. P., & Yi, Y. (2012). Specification, evaluation, and interpretation of structural equation models. *Journal of the Academy of Marketing Science, 40*(1), 8–34. https://doi.org/10.1007/s11747-011-0278-x.

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management, 53*(1), 1–21. https://doi.org/10.1016/j.im.2015.08.001.

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics, 34*(7), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013.

Berry, N., Emsley, R., Lobban, F., & Bucci, S. (2018). Social media and its relationship with mood, self-esteem and paranoia in psychosis. *Acta Psychiatrica Scandinavica, 138*(6), 558–570. https://doi.org/10.1111/acps.12953.

Bird, J. C., Evans, R., Waite, F., Loe, B. S., & Freeman, D. (2019). Adolescent paranoia: Prevalence, structure, and causal mechanisms. *Schizophrenia bulletin, 45*(5), 1134–1142. https://doi.org/10.1093/2Fschbul/2Fsby180.

Bird, J. C., Waite, F., Rowsell, E., Fergusson, E. C., & Freeman, D. (2017). Cognitive, affective, and social factors maintaining paranoia in adolescents with mental health problems: A longitudinal study. *Psychiatry research, 257*, 34–39. https://doi.org/10.1016/j.psychres.2017.07.023.

Blau, P. (1964). *Exchange and Power in Social Life*. New York: Wiley.

Byrne, B. M. (2010). *Structural equation modeling with AMOS: Basic concepts, applications, and programming* (2nd Ed.). Routledge Taylor & Francis Group.

Castelo-Branco, I., Cruz-Jesus, F., & Oliveira, T. (2019). Assessing Industry 4.0 readiness in manufacturing: Evidence for the European Union. *Computers in Industry, 107*, 22–32. https://doi.org/10.1016/j.compind.2019.01.007.

Chang, Y. S., & Fang, S. R. (2013). Antecedents and distinctions between online trust and distrust: Predicting high-and low-risk internet behaviors. *Journal of Electronic Commerce Research, 14*(2), 149.

Cheshire, C. (2007). Selective incentives and generalized information exchange. *Social Psychology Quarterly, 70*(1), 82–100. https://doi.org/10.1177/019027250707000109.

Colby, K. M. (1981). Modeling a paranoid mind. *Behavioral and Brain Sciences, 4*(4), 515–560. https://doi.org/10.1017/S0140525X00000030.

Coleman, J. S. (1990). *Foundations of Social Theory*. Harvard University Press.

Davidovic, D., & Harring, N. (2020). Exploring the cross-national variation in public support for climate policies in Europe: The role of quality of government and trust. *Energy Research & Social Science, 70*, Article 101785. https://doi.org/10.1016/j.erss.2020.101785.

Degutis, M., Urbonavičius, S., Zimaitis, I., Skare, V., & Laurutytė, D. (2020). Willingness to disclose personal information: How to measure it? *Engineering Economics, 31*(4), 487–494. https://doi.org/10.5755/j01.ee.31.4.25168.

Della Libera, C., Larøi, F., Raffard, S., Quertemont, E., & Laloyaux, J. (2020). Exploration of the paranoia hierarchy in the general population: Evidence of an age effect

mediated by maladaptive emotion regulation strategies. *Cognitive Neuropsychiatry, 25*(5), 387–403. https://doi.org/10.1080/13546805.2020.1824868.
Dinev, T., & Hart, P. J. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080.
Ellett, L., Lopes, B., & Chadwick, P. (2003). Paranoia in a nonclinical population of college students. *Journal of Nervous and Mental Disease, 191*(7), 425–430. https://doi.org/10.1097/01.NMD.0000081646.33030.EF.
Emerson, R. M. (1981). Social Exchange Theory. In M. Rosenberg, & R. H. Turner (Eds.), *Social Psychology: Sociological Perspectives* (pp. 30–65). Basic Books.
Emerson, R. M. (1976). Social exchange theory. *Annual Review of Sociology, 2*, 335–362. https://doi.org/10.1146/annurev.so.02.080176.002003.
Fenigstein, A., & Vanable, P. A. (1992). Paranoia and self-consciousness. *Journal of Personality and Social Psychology, 62*(1), 129–138. https://doi.org/10.1037/0022-3514.62.1.129.
Fenster, M. (2008). *Conspiracy Theories: Secrecy and Power in American Culture*. University of Minnesota Press.
Foa, U. G., & Foa, E. B. (1974). *Societal Structures of the Mind*. Charles Thomas.
Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50. https://doi.org/10.2307/3151312.
Frazier, M. L., Johnson, P. D., & Fainshmidt, S. (2013). Development and validation of a propensity to trust scale. *Journal of Trust Research, 3*(2), 76–97. https://doi.org/10.1080/21515581.2013.820026.
Fuster, H., Chamarro, A., & Oberst, U. (2017). Fear of missing out, online social networking and mobile phone addiction: A latent profile approach. *Aloma, 35*(1), 23–31.
Gefen, D., & Pavlou, P. (2006). An inverted-U theory of trust: The moderating role of perceived regulatory effectiveness of online marketplaces. *Information Systems Research, article in advance*, 1–20.
Gromann, P. M., Heslenfeld, D. J., Fett, A.-K., Joyce, D. W., Shergill, S. S., & Krabbendam, L. (2013). Trust versus paranoia: Abnormal response to social reward in psychotic illness. *Brain, 136*(6), 1968–1975. https://doi.org/10.1093/brain/awt076.
Gupta, B., Iyer, L. S., & Weisskirch, R. S. (2010). Facilitating global e-commerce: A comparison of consumers' willingness to disclose personal information online in the US and India. *Journal of Electronic Commerce Research, 11*(1), 41–52.
Heckathorn, D. D. (1985). Power and trust in social exchange. In E. J. Lawler (Ed.), *Advances in Group Processes, 2* (pp. 143–167). JAI Press.
Heirman, W., Walrave, M., Ponnet, K., & van Gool, E. (2013). Predicting adolescents' willingness to disclose personal information to a commercial website: Testing the applicability of a trust-based model. Article 3 *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 7*(3). https://doi.org/10.5817/CP2013-3-3.
Homans, G. C. (1961). *Social Behaviour: Its Elementary Forms*. Taylor & Francis.
Hong, W., & Thong, J. Y. L. (2013). Internet privacy concerns: An integrated conceptualization and Four Empirical Studies. *MIS Quarterly, 37*(1), 275–298. https://doi.org/10.25300/MISQ/2013/37.1.12.
Hong, W., Chan, F. K. Y., & Thong, J. Y. L. (2019). Drivers and inhibitors of internet privacy concern: A multidimensional development theory perspective. *Journal of Business Ethics, 168*, 539–564. https://doi.org/10.1007/s10551-019-04237-1.
Imhoff, R., & Lamberty, P. (2018). How paranoid are conspiracy believers? Toward a more fine-grained understanding of the connect and disconnect between paranoia and belief in conspiracy theories. *European Journal of Social Psychology, 48*(7), 909–926. https://doi.org/10.1002/ejsp.2494.
Jack, A. H., & Egan, V. (2018). Childhood bullying, paranoid thinking and the misappraisal of social threat: Trouble at school. *School Mental Health: A Multidisciplinary Research and Practice Journal, 10*(1), 26–34. https://doi.org/10.1007/s12310-017-9238-z.
Jenkins-Guarnieri, M. A., Wright, S. L., & Johnson, B. (2013). Development and validation of a social media use integration scale. *Psychology of Popular Media Culture, 2*(1), 38–50. https://doi.org/10.1037/a0030277.
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. https://doi.org/10.1111/isj.12062.
Kim, J., Lee, C., & Elias, T. (2015). Factors affecting information sharing in social networking sites amongst university students: Application of the knowledge-sharing model to social networking sites. *Online Information Review, 39*(3), 290–309. https://doi.org/10.1108/OIR-01-2015-0022.
King, J. (2018). *Privacy, Disclosure, and Social Exchange Theory* [Doctoral Dissertation, UC Berkeley]. *UC Berkeley Electronic Theses and Dissertations.* https://escholarship.org/uc/item/5hw5w5c1.
Kollock, P. (1994). The emergence of exchange structures: An experimental study of uncertainty, commitment, and trust. *American Journal of Sociology, 100*(2), 313–345. https://doi.org/10.1086/230539.
Kramer, R. M. (2008). Organizational paranoia: Origins and dysfunctional consequences of exaggerated distrust and suspicion in the workplace. 21st Century Handbook of Organizations: A Reference Handbook; Sage Publications: Los Angeles, GA, USA, 231-238. http://doi.org/10.4135/9781412954006.n73.
Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology, 25*(2), 109–125. https://doi.org/10.1057/jit.2010.6.
Lambe, C. J., Wittmann, C. M., & Spekman, R. E. (2001). Social exchange theory and research on business-to-business relational exchange. *Journal of Business-to-Business Marketing, 8*(3), 1–36. https://doi.org/10.1300/J033v08n03_01.
Lee, Y-H., & Yuan, C. W. (2020). The privacy calculus of "friending" across multiple social media platforms. Social Media + Society, 6(2), 479-500. https://doi.org/10.1177/2056305120928478.
Lévi-Strauss, C. (1969). The Elementary Structures of Kinship (rev. ed.). Beacon.
Lwin, M., 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. https://doi.org/10.1007/s11747-006-0003-3.
Malgieri, G., & Custers, B. (2018). Pricing privacy – The right to know the value of your personal data. *Computer Law & Security Review, 34*(2), 289–303. https://doi.org/10.1016/j.clsr.2017.08.006.
Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 311–416. https://doi.org/10.1287/isre.1040.0032.
Martin, K. (2018). The penalty for privacy violations: How privacy violations impact trust online. *Journal of Business Research, 82*, 103–116. https://doi.org/10.1016/j.jbusres.2017.08.034.
Mason, O. J., Stevenson, C., & Freedman, F. (2014). Ever-present threats from information technology: The cyber-paranoia and fear scale. Article 1298 *Frontiers in Psychology, 5*. https://doi.org/10.3389/fpsyg.2014.01298.
Masur, P. K. (2019). *The theory of situational privacy and self-disclosure. In Situational Privacy and Self-Disclosure*, 10.1007/978-3-319-78884-5 (pp. 131–182). Cham: Springer.
Meier, Y., Schäwel, J., & Krämer, N. C. (2020). The shorter the better? Effects of privacy policy length on online privacy decision-making. *Media and Communication, 8*(2), 291–301. https://doi.org/10.17645/mac.v8i2.2846.
Meisel, S. F., Garety, P. A., Stahl, D., & Valmaggia, L. R. (2018). Interpersonal processes in paranoia: A systematic review. *Psychological Medicine, 48*(14), 2299–2312. https://doi.org/10.1017/s0033291718000491.
Metzger, M. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication, 9*(4). https://doi.org/10.1111/j.1083-6101.2004.tb00292.x.
Miltgen, C. L., & Smith, H. J. (2015). Exploring information privacy regulation, risks, trust, and behavior. *Information & Management, 52*(6), 741–759. https://doi.org/10.1016/j.im.2015.06.006.
Molm, L., Takahashi, N., & Peterson, G. (2000). Risk and trust in social exchange: An experimental test of a classical proposition. *American Journal of Sociology, 105*(5), 1396–1427. https://doi.org/10.1086/210434.
Morgan-Thomas, A., Dessart, L., & Veloutsou, C. (2020). Digital ecosystem and consumer engagement: A socio-technical perspective. *Journal of Business Research, 121*, 713–723. https://doi.org/10.1016/j.jbusres.2020.03.042.
Morimoto, M. (2020). Privacy concerns about personalized advertising across multiple social media platforms in Japan: The relationship with information control and persuasion knowledge. *International Journal of Advertising, 1–21*. https://doi.org/10.1080/02650487.2020.1796322.
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. https://doi.org/10.1177/1094670511424924.
Naslund, J. A., Bondre, A., Torous, J., & Aschbrenner, K. A. (2020). Social media and mental health: Benefits, risks, and opportunities for research and practice. *Journal of technology in behavioral science, 5*(3), 245–257. https://doi.org/10.1007/s41347-020-00134-x.
Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x.
Omrani, N., & Soulié, N. (2018). Individual, contextual and macro antecedents of online privacy concern: The case of data collection in Europe. SSRN Electronic Journal. Advance online publication. https://doi.org/10.2139/ssrn.3168714.
Parish, J., & Parker, M. (2001). The age of anxiety: Conspiracy theory and the human science [Monograph]. *The Sociological Review Monograph Series, 48*(S2), 1–210.
Raihani, N. J., & Bell, V. (2019). An evolutionary perspective on paranoia. *Nature human behaviour, 3*(2), 114–121. https://doi.org/10.1038/2Fs41562-018-0495-0.
Robinson, 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. https://doi.org/10.1016/j.tele.2016.09.006.
Saalfeld, V., Ramadan, Z., Bell, V., & Raihani, N. J. (2018). Experimentally induced social threat increases paranoid thinking. *Royal Society Open Science, 5*(8), 1–12. https://doi.org/10.1098/rsos.180569.
Sharma, S., & Crossler, R. E. (2014). Disclosing too much? Situational factors affecting information disclosure in social commerce environment. *Electronic Commerce Research and Applications, 13*(5), 305–319. https://doi.org/10.1016/j.elerap.2014.06.007.
Sherchan, W., Nepal, S., & Paris, C. (2013). A survey of trust in social networks. *ACM Computing Surveys, 45*(4), 47. https://doi.org/10.1145/2501654.2501661.
Sierra, J. J., & McQuitty, S. (2005). Service providers and customers: Social exchange theory and service loyalty. *Journal of Services Marketing, 19*(6), 392–400. https://doi.org/10.1108/08876040510620166.
Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly, 35*(4), 989–1015. https://doi.org/10.2307/41409970.
Szymczak, H., Kücükbalaban, P., Lemanski, S., Knuth, D., & Schmidt, S. (2016). Trusting Facebook in crisis situations: The role of general use and general trust toward Facebook. *Cyberpsychology, Behavior, and Social Networking, 19*(1), 23–27. https://doi.org/10.1089/cyber.2015.0450.
Urbonavičius, S. (2020). Willingness to disclose personal data online: not just a situational issue. Proceedings of AIRSI 2020 Conference, Zaragoza University, 66-90.

Urbonavičius, S., & Zimaitis, I. (2018). The mediating role of paranoia on online consumer behaviour. Proceedings of the 9th EMAC Regional Conference, Prague, Czech Republic, 12–14 September 2018.
Varey, R.J. (2015). Social Exchange (Theory). In Wiley Encyclopedia of Management (eds C.L. Cooper, N. Lee and A.M. Farrell). https://doi.org/10.1002/9781118785317.weom090245.
Wakefield, R. (2013). The influence of user affect in online information disclosure. *The Journal of Strategic Information Systems, 22*(2), 157–174. https://doi.org/10.1016/j.jsis.2013.01.003.
Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management, 36*(4), 531–542. https://doi.org/10.1016/j.ijinfomgt.2016.03.003.
Weil, D., Fung, A., Graham, M., & Fagotto, E. (2005). The effectiveness of regulatory disclosure policies. *Journal of Policy Analysis and Management, 25*(1), 155–181. https://doi.org/10.1002/pam.20160.
Wieringa, J., Kannan, P. K., Ma, X., Reutterer, T., Risselada, H., & Skiera, B. (2019). Data analytics in a privacy-concerned world. *Journal of Business Research, 122*, 915–925. https://doi.org/10.1016/j.jbusres.2019.05.005.
Yamagishi, T., & Yamagishi, M. (1994). Trust and commitment in the United States and Japan. *Motivation and Emotion, 18*, 129–166. https://doi.org/10.1007/BF02249397.
Yang, X. (2019). How perceived social distance and trust influence reciprocity expectations and eWOM sharing intention in social commerce. *Industrial Management & Data Systems, 119*(4), 867–880. https://doi.org/10.1108/IMDS-04-2018-0139.
Zeng, F., Ye, Q., Li, J., & Yang, Z. (2020). Does self-disclosure matter? A dynamic two-stage perspective for the personalization-privacy paradox. *Journal of Business Research, 124*, 67–675. https://doi.org/10.1016/j.jbusres.2020.02.006.
Zhang, X. P., Cai, Y. L., & Zhao, L. (2019). Analysis implications of general trust model on consumer's trust in CBEC sellers. Proceedings of the 2nd International Workshop on Advances in Social Sciences (IWASS 2019).
Zhao, J., Zhu, C., Peng, Z., Xu, X., & Liu, Y. (2018). User willingness toward knowledge sharing in social networks. *Sustainability, 10*(12), 4680. https://doi.org/10.3390/su10124680.
Zhang, R., & Fu, J. S. (2020). Privacy management and self-disclosure on social network sites: The moderating effects of stress and gender. *Journal of Computer-Mediated Communication, 25*(3), 236–251. https://doi.org/10.1093/jcmc/zmaa004.
Zimaitis, I. Urbonavicius, S, Degutis, M., Kaduskeviciute, V. (2020a) Impact of age on the willingness to disclose personal data in e-shopping. Proceedings of EMAC 11th Regional Conference, Zagreb.
Zimaitis, I., Degutis, M., & Urbonavičius, S. (2020). Social media use and paranoia: Factors that matter in online shopping. *Sustainability, 12*(3), 904. https://doi.org/10.3390/su12030904.

Dr. Sigitas Urbonavicius is a Professor at Vilnius University, Department of Marketing. Having his educational background from the universities in the US and Lithuania, he developed his experience working on research/teaching/consulting projects in more than 20 countries. He serves as an Editor-in chief for the journal *Organizations and Markets in Emerging Economies* and is a member of editorial boards for several other journals. His research interests include numerous aspects of consumer behavior, especially concentrating on the privacy issues online. The newest projects he leads are concentrated on the impacts of factors that range from trust to exaggerated distrust and their impacts on the online behavior. He has published in Journal of Consumer Behavior, Journal of Marketing Education, International Journal of Market Research, EuroMed Journal of Business, International Journal of Culture, Tourism and Hospitality Research and others.

Dr. Mindaugas Degutis is an Associated Professor at Vilnius University, Department of Marketing since 2010. He has previously worked in the Institute of Political Science and International Relations at the University of Vilnius. He has graduated top of his class during both undergraduate and graduate studies at the Department of Sociology, Vilnius university and later completed his PhD on electoral behavior in Lithuania at Institute of Political Science and International Relations at the University of Vilnius in 2002. His research interests are in areas of consumer behavior, subjective well-being, electoral studies, political marketing. He has published in Sustainability, Journal of Marketing Education, Baltic Journal of Management, Engineering Economics and other journals.

Ignas Zimaitis is a PhD candidate in Marketing at the Faculty of Economics and Business Administration in Vilnius University and the assistant editor at the journal *Organizations and Markets in Emerging Economies*. He teaches Fundamentals of Marketing, E-marketing, International E-marketing and E-commerce courses at the Faculty of Economics and Business Administration in Vilnius University and Digital Marketing, and Digital Marketing Tools courses in Vilnius University Business School. His research interests include online consumer behavior, paranoid consumer behavior, controversial advertising, and the implications of gamification in online learning. He has publications in Journal of Marketing Education, Engineering Economics and Sustainability. His conference papers were presented at EMAC regional and AMS conferences.

Vaida Kaduškevičiūtė is a PhD candidate at Vilnius University Faculty of Economics and Business Administration (Lithuania). Her main research field is exploring showrooming and webrooming phenomenon in multichannel purchasing environment. Secondary field of expertise is usage of personal data for marketing purposes and consumer willingness to disclose their information. Research findings were already published in international journal Market-Tržište, additionally presented in EMAC Regional conference 2018 and 2019. In 2020 author won the best full-article award at the conference AIRSI2020.

Vatroslav Skare, PhD, is an Associate Professor at the Marketing Department of the Faculty of Economics & Business, University of Zagreb, Croatia. He received his Masters degree and PhD in marketing from University of Zagreb, Croatia. His research interests include digital marketing, product and brand management and country image. He has published contributions to books and articles in national and international journals (e.g. Journal of Business Research). His academic activities also include active participation in academic and professional organizations and teaching at executive education programs by using business simulations. As a consultant, he has been involved in numerous marketing projects in different industries, including Tourism, Retail, Publishing & Media, ICT, and Real Estate.

VILNIUS TECH
Vilnius Gediminas Technical University

Journal of Business Economics and Management
ISSN 1611-1699 / eISSN 2029-4433
2022 Volume 23 Issue 3: 551–568
https://doi.org/10.3846/jbem.2022.16119

INFLUENCE OF TRUST AND CONSPIRACY BELIEFS ON THE DISCLOSURE OF PERSONAL DATA ONLINE

Ignas ZIMAITIS, Sigitas URBONAVIČIUS*, Mindaugas DEGUTIS, Vaida KADUŠKEVIČIŪTĖ

Faculty of Economics and Business Administration, Vilnius University, Vilnius, Lithuania

Received 15 February 2021; accepted 13 September 2021; first published online 28 February 2022

Abstract. The issue of trust-based personal data disclosure online remains of high importance both in social networking and online purchasing. Additionally, social networking is linked with a controversial factor of conspiracy beliefs that recently received attention because of Covid-19 pandemic. Conspiracy beliefs trigger activities online, but generate hesitations in regards to rational ideas, requests and procedures. Therefore, it is unclear how they impact rational requests of data disclosure in online shopping. The paper analyses how trust and conspiracy beliefs impact willingness to disclose personal data in social networking and in online shopping. The modelling based on the social exchange theory conceptualizes these two online activities as reciprocal and negotiated types of exchange. The findings based on structural equation modelling show some similarities between the impacts of trust and conspiracy believes in case of social networking, but disclose their radical differences in regards to willingness to disclose personal data in online purchasing.

Keywords: trust, conspiracy beliefs, social networking, self-disclosure, willingness to disclose personal data, social exchange theory.

JEL Classification: M31.

Introduction

One of the major trends in modern business is digitalisation of almost all its functions (Koe & Sakir, 2020; Shpak et al., 2020). This is especially noticeable in digital marketing, personalized advertising and online selling that experience a substantial growth in almost all countries of the world (Morimoto, 2021; Vadana et al., 2019; Wirtz et al., 2017). However, the success of digital marketing and e-commerce is highly dependent on the extensive use of customer personal data (Bleier et al., 2020). In order to develop personalized offers and be efficient in online sales, businesses largely employ user-generated data that helps reaching their marketing objectives (Strycharz et al., 2019). Though technical means of data collection are rapidly developing, the collection of personal data is not easy because consumers tend

*Corresponding author. E-mail: *sigitas.urbonavicius@evaf.vu.lt*

to be worried about the issues of personal data disclosure and the loss of privacy (Grosso & Castaldo, 2014; Cheng & Wang, 2018). This makes their willingness to disclose personal data rather low, often limited to the types and amount of data that is absolutely required to make a transaction or to reach another online objective (Bansal et al., 2016).

The willingness to disclose personal data online includes a number of rather complex considerations and has several meanings (Degutis et al., 2020). There are very strong arguments to state that willingness to provide personal data is a situational (contextual) factor that depends on where, when, for what purpose the data is being disclosed (Bansal et al., 2016; Masur, 2019; Padyab et al., 2019). The amount and types of data disclosed also depend on a situation. In rather basic cases of online shopping, it is required to provide just a minimal information (like name, address, e-mail address); in more complex ones it is required to disclose more extensive set of personal information, often amended with the permission to track online activities or geographical location (Joinson & Paine, 2007; Wang et al., 2016; Martin & Palmatier, 2020). Quite often some part of the personal information is "a must", since otherwise the objective (online transaction or a digital service) cannot be provided (Zimmer et al., 2010; Prince, 2018). In many other cases, the requests for information/permissions are more flexible, and providing of the personal data largely depends on the willingness of a person to provide it (Mosteller & Poddar, 2017). In this case, the dispositional type of the willingness to provide data starts to be increasingly important. It means that some people are more pre-disposed to disclose personal facts than others and that some other dispositional or attitudinal factors also impact the willingness to disclose data (Urbonavičius, 2020). Among such, the factors of trust-distrust nature play the most important roles (Chang & Fang, 2013; Bansal et al., 2016; Kim et al., 2019).

General trust is a trait that positively impacts numerous human interactions, including activities online that require disclosure of personal data. However, trust is differently linked with willingness to disclose personal data in social networking and in online shopping. People are rather easily disclosing details of their private lives in social networking, but are rather restrictive to do it in registering for online shopping reasons (Barth & de Jong, 2017). These two data disclosure situations have been quite extensively analysed separately, but their linkage in terms of the willingness to disclose personal data has been observed rather recently (Zimaitis et al., 2020a, 2020b). The supportive climate and continuous interactions with peers develop trust and encourage further interactions, thus developing extensive data disclosure in social networking (Lin et al., 2020). Data disclosure in online buying is much more formalized and regulated, and the mechanisms of the disclosure are rather different (Robinson, 2018; Degutis et al., 2020). These differences have been integrated into a model that was grounded on the Social Exchange Theory (SET) by classifying data disclosure in social media as reciprocal social exchange and data disclosure in online shopping as negotiated social exchange, justifying the interaction between them (Zimaitis et al., 2020b; Urbonavicius et al., 2021). Trust played an important predictive role in regards to both instances.

On the other hand, the online activities are impacted by variables that reflect the uncertainty and are linked with not necessarily relevant perceptions of risks, distrust or false beliefs (Ahmad & Sun, 2018). One of controversial factors that represents distrust in commonly known facts is beliefs in conspiracies (van Prooijen & de Vries, 2016). The issue of

conspiracy beliefs recently received a new wave of attention from researchers because of Covid-19 (Georgiou et al., 2020; Pellegrini et al., 2021). It has been observed that conspiracy beliefs are linked with social networking (Goreis & Kothgassner, 2020). However, the impact of conspiracy beliefs on data disclosure in social media and – even more – in online purchasing presents a noticeable research gap that is addressed in this study. This attempt is based on the use of SET as the theoretical grounding that helps to consider trust and conspiracy beliefs as two key antecedents of the data disclosure in social media and of the willingness to disclose personal data in online shopping. More concretely, the study is aiming to answer these research questions: "How the impact of trust and conspiracy beliefs on self-disclosure in social networking and on willingness to disclose personal data in online purchasing can be modelled with the help of SET?" "What are the total effects of trust on self-disclosure in social networking and on willingness to disclose personal data in purchasing online?" "What are the total effects of conspiracy beliefs on self-disclosure in social networking and on willingness to disclose personal data in online purchasing?" The modelling of interactions is based on earlier studies that employed social exchange theory in marketing-related studies (Mosteller & Poddar, 2017; King, 2018; Zimaitis et al., 2020b). The model that is developed in the current study reflects a case of personal data disclosure and thus presents a novelty aspect among the applications of SET. Analysis of empirical data allows to test the predicted relationships and to draw conclusions.

The paper consists of five main parts: literature review, methodology (research model, measures and data), analysis (testing of hypotheses), discussion and conclusions together with limitations and directions for future research.

1. Literature review

Theoretical backgrounds. The research interest in issues of privacy and personal data disclosure perhaps starts from the concept of privacy paradox – the observation of the declared privacy concerns and limited willingness to disclose personal data, followed with rather relaxed behaviours in data disclosure (Norberg et al., 2007; Weinberger et al., 2017a, 2017b). In order to explain the paradox and other privacy and data disclosure issues, a number of theoretical backgrounds and models have been employed. The privacy-related issues have been analysed on the basis of the theory of planned behaviour, technology acceptance model and principal-agent theory (Kim & Kim, 2014; Zhao et al., 2018; Parker & Flowerday, 2021). The attempts of a deeper analysis were made from the commodity view of privacy and from the aspect of psychological ownership over personal information (Xu et al., 2011; Kehr et al., 2015). This allowed to analyse ownership-risk interaction on the basis of prospect theory. Such an interpretation evolved into the concept of privacy calculus that emphasizes the rational behaviour of consumers. It is assumed that they evaluate the trade-off between the value they obtain from the data disclosure and the potential negative consequences of the loss of control over the disclosed data (Kehr et al., 2015). Though privacy calculus is criticized for the putting to high emphasis on argument of rationality (Kehr et al., 2015; Wakefield, 2013), this approach is accepted by many researchers who agree that consumers tend to disclose facts about themselves in exchange for the foreseen benefits (Barth & Jong, 2017; Robinson, 2017).

Social exchange theory. The above-mentioned theoretical approaches help to analyse privacy issue and personal data disclosure to a large extent, but they do not specifically address the two typical online behaviours: social networking and online purchasing, where the approaches in regards to the personal data disclosure are different. This requires to look for a different theoretical background that would allow the two types and link them with the relevant antecedents. The suitable solution for this is the use of Social Exchange Theory. This theory has been developed by George C. Homans (1961) and Phillip Blau (1964), followed by Richard Emerson (1976). Though the theory uses the principles of rationality in human behaviour, it considers the difference of its manifestation in negotiated and reciprocal exchange (Levi-Strauss, 1969; Emerson, 1981). An exchange of the negotiated type occurs when the terms of an exchange are discussed by the participating parties in advance, therefore at the moment of the exchange they are agreed on and formalized. The basis for the negotiation is benefits and costs of the exchange, though there might be additional aspects of the exchange (such as timing, etc.) included as well. These conditions are present in many exchanges that include economic aspect, and they are typically classified as negotiated exchanges (Molm et al., 2000). Reciprocal exchange is based on mutual interactions of an exchange participants that are performed in response of the earlier behaviour of an exchange partner. This is based on the expectation that a partner will reciprocate in a similar manner. The terms of the exchange are not agreed upon in advance, which means that this type of an exchange is largely based on the mutual and gradually developed trust (Molm et al., 2000). This type of exchange of occurs in networking and friendships (Olk & Gibbons, 2010).

Disclose of personal data online. Very early in its development, the SET started to consider information as a resource that could be used in exchanges (Foa & Foa, 1974). This interpretation of information as an important type of resources continues to be used in modern contexts (Cheshire, 2007). SET helped to analyse privacy related behaviours or attitudes (Metzger, 2004; King, 2018) and rather recently SET was specifically used in studies on willingness to disclose personal data in online purchasing (Zimaitis et al., 2020b). Though this research stream is not yet widely developed, it seems to be very promising, because it is able to reflects and integrate data disclosure in social networking and in online shopping.

In case when the SET is employed, social networking and disclosure information on social networks is considered as reciprocal, while purchasing online and willingness to disclose personal information there – as negotiated exchange.

People are using social media in order to interact with others, to socialize. The typical interaction means providing information about themselves, their experiences, feelings or emotions to others with expectation that the other side will respond similarly, which perfectly represents a reciprocal exchange situation (Cheng et al., 2011). Other aspects of reciprocal exchange are also present in social networking: there is no formalised obligation to reciprocate, exchange relations develop gradually, on the basis of mutual trust. In terms of regulations, social networks apply just very general rules/terms to be followed, no strict assurance structures are present, the shortest forms of informing about them are the most preferred (van der Schyff et al., 2020; Meier et al., 2020). Important outcome of the participation in social networking is self-disclosure to others, as the result of mutual trust that develops in the process of reciprocal interactions (Lee & Choi, 2017). Social media allows rather easy

disclosure of personal information to other persons, and many people are doing this rather willingly (Schlosser, 2020; Varnali & Toker, 2015; Zhang & Fu, 2020). The information is revealed with high levels of openness and spontaneity as an outcome of general trust that is further developed in reciprocal social networking (Koohikamali et al., 2017).

The disclosure of personal information in the case of online purchasing is different. The process typically is formalized by terms of an agreement that includes aspects about how the provided personal data can be used. The other side grants its handling in accordance to the certain procedures that often are predetermined or assured by wider legal regulations (Goddard, 2017). Perceptions about the effectiveness of assurance are among the important factors in this type of social exchange (Hong et al., 2021). In online purchasing one side of interaction typically is an online store that requires to provide certain amount of information to enable a transaction. Additional amounts of personal information can be provided in exchange for other benefits – easier access, convenience in future transactions, monetary compensation, etc. (Malgiery & Custers, 2018). All this perfectly describes the information disclosure situation that SET categorizes as a negotiated social exchange. However, the negotiated exchanges between individuals and online stores are not necessarily continuous: a buyer may disclose personal data as it is required for a single-time transaction, and limit it to the scope of mandatory information that is absolutely necessary for the one specific transaction (Urbonavičius, 2020). Broader disclosure of personal data is required for registration to online stores, since it includes both the mandatory and additional items of personal information.

It is important that some empirical evidence confirms the interaction between social networking/personal data disclosure in social networks and willingness to disclose personal data in online shopping. Though not yet abundant, it allows to predict impact of reciprocal exchange on negotiated exchange (Zimaitis et al., 2020b; Degutis et al., 2020).

Trust. Trust is an antecedent of various behavioural intentions, and it is especially salient in social exchange relationships (Bernerth & Walker, 2009). Trust is also an essential factor for modelling numerous internet-based activities, including online transactions (Zhang et al., 2020). It is observed that online trust highly depends on past experiences with online activities (Chen et al., 2015; Dinev et al., 2006; Murphy, 2003) and develops over repeated interactions (Alarcon et al., 2018). In the disclosure of personal data as a social exchange, trust plays the role that is of the special importance, since it both creates and is created by the reciprocity of social exchange (Molm et al., 2000). When it regards transactions that require information, trust also is one of the major factors that encourage individuals to disclose information about themselves (Koohikamali et al., 2017). However, trust influences the willingness to disclose information in online purchasing (that is a form of negotiated exchange) not just directly. Since trust develops in the process of reciprocal social exchanges, that are present in social networking, the growing involvement in social media increases the level of personal disclosure in social networking. Additionally, self-disclosure is a result of trust-based perceptions about the safety of self-disclosure, which means that perceptions about the effectiveness of regulations mediate the impact of trust on self-disclosure. Thus, the total effects of trust on self-disclosure include its direct and all indirect impacts:

H1: Total effect of trust on self-disclosure in social networking is positive.

On the other hand, SET suggests that online selling also includes elements of reciprocity (Swoboda & Winters, 2021). Therefore, the above-mentioned effects of trust are also present in the process of data disclosure in online shopping. This is supported by the conceptual statement of SET developers that trust is important in both types of social exchange (Emerson, 1981). Again, this is applicable to the exchange of information: it is found that dispositional trust is one of the main predictors of the willingness to disclose personal data in online purchasing (Meinert et al., 2006; Chen et al., 2015; Keith et al., 2015; Zimaitis et al., 2020b). This is not limited to just the direct impact of trust on the willingness to exchange data. The impact of trust often is mediated by additional factors, two of them being extremely important.

First, having limited relative power against an online store, an individual tends to rely on additional assurance of third parties. Most typically, the role of a third party is played by legal systems, procedures and institutions that look after the privacy issues in online activities (Zimaitis et al., 2020b). Positive perception on effectiveness of regulations increases the relative power of individuals in their social exchange with online stores, and contribute to willingness to disclose personal data online. For instance, introduction of GDPR in 2018 increased buyers' sense of perceived security, third-party assurance and perceived openness (Zhang et al., 2020). Therefore, the impact of trust on willingness to disclose personal data online is mediated by perceived regulatory effectiveness.

Second, recent findings show that willingness to disclose personal data in online purchasing is also positively impacted by other online activity: social networking (Zimaitis et al., 2020b). Social networking or the overall involvement in social media might seem not closely linked with activities in online shopping; however, SET helps to explain this relationship. There is an evidence (Zimaitis et al., 2020b) that involvement in social media (reciprocal exchange) impacts the willingness to disclose data in online shopping (negotiated exchange). This even stronger justifies both direct and indirect impact of trust on willingness to disclose personal data in online shopping. Specifically, it means that the impact of trust on willingness to disclose personal data in online purchasing is mediated by factors that represent activities in social networking and are reciprocal by their nature.

Therefore, trust is expected to exert both direct and indirect positive impact on willingness to disclose personal data in online purchasing:

H2: Total effect of trust on willingness to disclose personal data in online purchasing is positive.

Conspiracy beliefs. Conspiracy beliefs refer to personal allegations that powerful groups or authorities are implementing misdemeanours or other unethical behaviours towards society and represents a form of distrust (van Prooijen & de Vries, 2016). Beliefs in conspiracies has been attracting attention of researchers already for some time; however, worldwide pandemic generated additional growth of interest for this phenomenon (Georgiou et al., 2020; Pellegrini et al., 2021). The nature of this factor suggests that people with higher level of conspiracy beliefs should be cautious about disclosing their personal information. At the same time, people, who believe in conspiracy theories, tend to be involved into social networking in order to find support and confirmation for their beliefs (Allington et al., 2021; Goreis &

Kothgassner, 2020). It is relevant to expect that conspiracy beliefs play more and more important role in social networking and positively impact involvement in social media that is influenced by numerous factors of both dispositional and situational nature (Chung et al., 2019). This is additionally justified by fact that some reasons for the involvement in social media might be triggered by rather unexpected personal characteristics (such as paranoia, as disclosed by Urbonavičius & Zimaitis, 2018; Zimaitis et al., 2020a) or by the search for information on rather controversial ideas, including conspiracy theories (Allington et al., 2021). Additionally, involvement in social networks offer opportunities to interact with others sharing similar ideas regarding conspiracies (Allington et al., 2021). Therefore, conspiracy beliefs are expected to have direct positive impact on involvement in social media. One of the reasons of involvement in social media includes the desire to preserve social image and enhance it in the eyes of significant others (Douglas et al., 2019). Being noticed and "visible" seems to be even more important to people who tend to represent original ideas, life-styles and beliefs (Bazarova & Choi, 2014). Therefore, conspiracy beliefs not just motivate to be active in social networking, but also stimulate conspiracy believers to self-disclose themselves to similar others in a more exaggerated way then typically. This justifies the proposition that conspiracy beliefs impact self-disclosure in social networking both directly and via mediation of the involvement in social networking. We predict that the total effect of conspiracy beliefs on self-disclosure in social networking is positive:

H3: Total effect of conspiracy beliefs on self-disclosure in social networking is positive.

The link between conspiracy beliefs and willingness to disclose personal data in online purchasing is still largely unknown and represents a research gap. However, individuals with conspiracy beliefs typically are cynical about the majority of regulations and express rather negative attitudes towards all kinds of authorities in general (Goreis & Voracek, 2019). Therefore, any regulated activity or request should be perceived by them negatively, and conspiracy beliefs should reduce the willingness to disclose personal data in all of them. Since the interaction between an individual and an online store is largely regulated, conspiracy beliefs should impact the willingness to disclose personal data in online purchasing negatively.

The direct negative impact of conspiracy beliefs on the willingness to disclose personal data in purchasing lacks empirical evidence, but is somehow predictable on the basis of the indirect considerations and logical arguments. However, the question how conspiracy beliefs influence the willingness to disclose data in online purchasing is complicated by the fact that the willingness is also impacted by the effects of social networking. Since it is predictable that conspiracy beliefs impact activities in social networking positively, these may exert further positive indirect effect of conspiracy beliefs towards the willingness to disclose data in online purchasing. This positive indirect effect would conflict with negative direct influence of conspiracy beliefs, and the direction of total effect on the willingness to disclose data in online shopping appears unknown. The lack of empirical evidence does not allow to know whether the direct negative or indirect positive effect is be stronger. We propose that the total effect of conspiracy beliefs will be negative, despite the existing indirect positive effects:

H4: Total effect of conspiracy beliefs on willingness to disclose personal data in online purchasing is negative.

Mediators. As discussed above, trust and conspiracy beliefs impact the dependent variables both directly and indirectly. The two considered mediators include involvement in social networking and the factor of perceived regulatory effectiveness.

Involvement in social networking. Networking with the help of social media is a part of daily lives of population (Appel et al., 2020). People are involved in social media in various ways and at different levels, but in all instances they share own information in exchange to information shared by their peers. From the perspective of social exchange theory, involvement in social networking is a form of mutual trust-based reciprocal exchange (Yang, 2019; Zimaitis et al., 2020b). This is even stronger supported by the fact that the use of social media platforms involves interactions between users with rather limited or non-existent formal regulations of the information exchange (King, 2018).

Perceived regulatory effectiveness. The concept of perceived regulatory effectiveness is associated with consumer attitudes regarding to capability of the legal regulations to provide protection for internet users in terms of the online privacy (Urbonavičius, 2020; Moyaery & Urbonavičius, 2021). This perception largely depends on a personal trait of trust (measured as general trust, dispositional trust, propensity to trust) (Sun et al., 2018). Perceived regulatory effectiveness has been found to be positively related with perceived privacy control (Xu et al., 2011) and perception of security (Balapour et al., 2020), but negatively linked to perceived privacy risks (Xu et al., 2011) and perceived privacy concerns (Skrinjaric et al., 2019). Most importantly, the perceived regulatory effectiveness has been found to be related to willingness to disclose personal data, as the negotiated type of social exchange (Skare et al., 2020; Urbonavičius, 2020; Zimaitis et al., 2020a).

2. Research model, measures and data

The study aims to assess total effects of trust and conspiracy beliefs on self-disclosure in social media and on willingness to disclose personal data in online purchasing. The modelling is based on social exchange theory and includes two mediators: involvement in social media and perceived regulatory effectiveness (Figure 1).

The key interest of this study is concentrated on the total effects of the two antecedents: trust and conspiracy beliefs on the two dependent variables: self-disclosure in social media and willingness to disclose personal data in online shopping. The set of total effects includes direct effects together with indirect effects that are mediated by involvement in social media

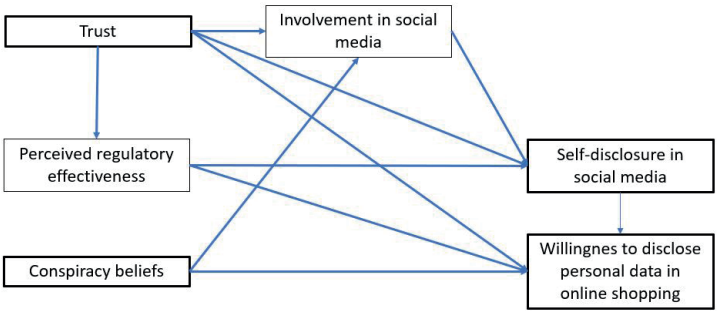

Figure 1. Research model

and perceived regulatory effectiveness. The importance of the two mediators and the presence of directs effects are justified by the earlier findings that help developing the research model (Zimaitis et al., 2020b).

The survey is based on the questionnaire, which included scales that has been successfully used in former studies. All items were measured on a 1–7 Likert scale. More specifically, the perceived regulatory effectiveness scale (3 items, $\alpha = 0.83$) was adapted from Lwin et al. (2007); a minor amendment was made to include GDPR in one of the statements; the scale with this adaptation has been successfully used by Zimaitis et al. (2020a) and Urbonavicius et al. (2021). Trust was measured on a 4-item scale (Frazier et al., 2013). The involvement in social media was assessed with 10-items SMUIS scale, developed by Jenkins-Guarnieri et al. (2013). Self-disclosure was measured with 6-items scale, recently used by Jacobson et al. (2020). Willingness to disclose personal data (WTD) was measured by using the scale that was initiated by Gupta et al. (2010) and later used by Heirman et al. (2013). Conspiracy beliefs were assessed using the Brotherton et al. (2013) generic conspiracist beliefs scale. The scale was reduced to 7 items; two items were modified in order to include the two most recent conspiracy beliefs (vaccinations and 5G issues).

The data was collected in Lithuania with the use of a representative online survey; the sample included 1000 respondents. After visual inspection 15 unengaged respondents were removed, therefore the analysis was based on 985 responses. The sample included respondents from 15 to 60 years old; 29% were in the age group of 15–29; 32% the represented the group of 30–44; remaining 39% were 45–60 years old. By gender, 49% were males and 51% females. 53% of the respondents had university education.

Exploratory factor analysis (maximum likelihood; Promax rotation with Kaiser normalization) showed good sampling adequacy (KMO = 0.897), Bartlett's test of sphericity was significant (0.000), approx. Chi-square 1555.330, df = 345. The extracted factors explained 61.804 of the total variance (cumulative Eigenvalues 68.527). There were only 23 (4.0%) non-redundant residuals, which confirmed the adequacy. All loadings were above 0.5 (validity), at least 0.2 difference of variables in factors, and no more than 0.7 correlation between factors (the largest was 0.521), which refers to acceptable discriminant validity.

Confirmatory factor analysis showed a good model fit: CMIN/DF = 2.992; TLI rho2 = 0.948; CFI = 954; RMSEA = 0.045 (Byrne, 2010). Further validity check showed that in all instances average variance extracted (AVE) >0.5, composite reliability (CR) >0.7, root of AVE greater than correlations (Table 1).

Table 1. Validity checks

	CR	AVE	Conspir	SelfDiscl	RegEffect	SocMediaInt	Trust	WTD
Conspiracy	0.900	0.566	0.752					
Self-Disclosure	0.899	0.598	0.228	0.773				
Regulation Effectiveness	0.819	0.601	0.067	0.159	0.775			
Social Media	0.909	0.559	0.103	0.547	0.211	0.748		
Trust	0.914	0.726	0.039	0.176	0.272	0.233	0.852	
WTD	0.873	0.580	–0.041	0.020	0.298	0.185	0.270	0.762

The result of common latent bias test was positive (difference in chi-square = 518.8, difference in df = 32, p = 0.000), therefore the data imputation was performed with consideration of the common latent factor.

3. Testing of hypotheses

The fit of the structural model (CMIN/DF = 2.593; TLI = 0.982; CFI = 0.998; RMSEA = 0.040) allowed testing the hypotheses (Figure 2).

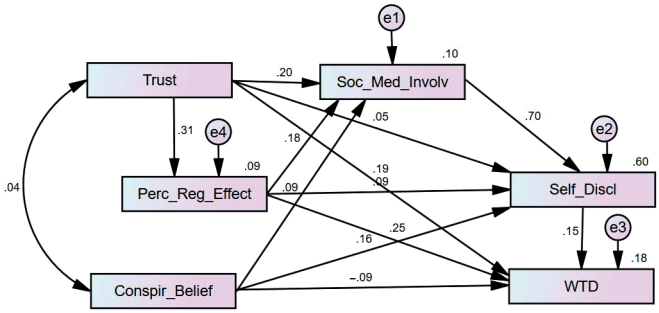

Figure 2. Structural model

All individual relationships in the model appeared significant.

Direct effects. All direct effects among the variables appeared significant. This means that every indirect effect, as well as all total effects are also significant, which allows to test hypotheses about total effects. The level of significance of direct effects was $p < 0.001$ in all cases, except three instances: Conspiracy beliefs on social media involvement ($p = 0.003$), trust on self-disclosure ($p = 0.030$) and conspiracy beliefs on WTD ($p = 0.003$).

Mediation. Involvement in social media mediated the relationships from trust to self-disclosure, from perceived regulatory effectiveness to self-disclosure and from conspiracy beliefs to self-disclosure. Its direct effect on self-disclosure was very strong ($\beta = 0.703$, $p < 0.001$). Perceived regulatory effectiveness was an important mediator of trust in regards to both dependent variables; its direct effect on self-disclosure in social networks was $\beta = 0.088$; on willingness to disclose personal data in purchasing $\beta = 0.246$ ($p < 0.001$ in both instances).

The hypotheses were concentrating on the total effects of trust and conspiracy beliefs on self-disclosure in social networks and on willingness to disclose personal data in e-purchasing. For this, the standardized total effects have been assessed (Table 2).

Table 2. Standardized Total Effects

	Conspiracy beliefs	Trust
Self-disclosure	0.242	0.246
Willingness to disclose data in online purchasing	–0.062	0.304

Total effects of trust on self-disclosure in social media was strong and positive, thus H1 was confirmed. Trust influenced self-disclosure in three different ways: directly, via media-

tion of involvement in social media and via mediation of perceived regulatory effectiveness. Direct and indirect effects were positive and significant; however, the direct effect was weaker than indirect (β = 0.047 and β = 0.204, respectively).

Total effect of trust on willingness to disclose data in online shopping was strong β = 0.304; the hypothesis H2 was confirmed. This influence was composed from the direct effect β = 0.191 and indirect effect of β = 0.113 that is a sum of effects in four paths (see the structural model in Figure 2).

Hypothesis H3 predicted positive total effect of conspiracy beliefs on self-disclosure in social networking. It was confirmed, the total effect is β = 0.242. It is made up from the direct effect of β = 0.160 and indirect effect with mediation of involvement in social media (β = 0.062).

The most contradictory was H4, since it included aggregation of the direct negative and indirect positive effects of conspiracy beliefs on willingness to disclose data in online shopping. The analysis showed that the direct effect was negative β = –0.088 and relatively stronger than indirect positive effect (β = 0.034), which resulted in to negative total effect of β = –0.054). Therefore, H4 was confirmed.

4. Discussion

A causal model outlined two alternative ways how the analysed antecedents may impact willingness to disclose personal data in shopping online: in both cases the total effect is combined of direct and indirect (mediated) effects. The positive direct effect of trust is in compatibility with social exchange theory statements about the importance of negotiation type of exchange and trust in social interactions (Molm et al., 2000). Negative direct effect of conspiracy beliefs was rather under-researched and not empirically assessed, therefore the findings of the current study present a new evidence on the issue. The finding stays in accordance with the conceptualization of the construct as the one that is linked to the extreme distrust.

The second way how the analysed factors impact WTD is through social media involvement and via the self-disclosure in social networks. Both trust and conspiracy beliefs have positive relations with social media involvement, which positively and very strongly impacts self-disclosure and willingness to disclose personal data. These findings are in accordance with findings of earlier studies (e.g. Kim & Park, 2013; Chen et al., 2015; Koohikamali et al., 2017) that reported relation between trust and social media/self-disclosure. However, this study further elaborates on not much researched (only addressed by Urbonavicius et al., 2021) relation between reciprocal exchange (represented by disclosure of information in social media) and negotiated exchange (represented by disclosure of personal data in online shopping) and once again confirms suitability of social exchange theory for research on the topic of personal data disclosure.

Overall, the study demonstrates that conspiracy beliefs is an important factor for social networking and self-disclosure in social media (as predicted by Douglas et al., 2019; Goreis & Kothgassner, 2020). More specifically, the impact of conspiracy beliefs on self-disclosure in social networks is stronger than on general involvement in social media (β = 0.160 and 0.076, respectively). This is a very novel observation that signals that conspiracy beliefs are stronger

linked with demonstration of the self to others than being involved in other networking activities. It also contributes to the understanding of the issue by showing that conspiracy beliefs have an ambiguous impact on willingness to disclose personal data in online shopping: the direct negative effect is largely compensated by the positive indirect effect.

Conclusions

Conclusions and managerial implications. The study allows to make several conclusions and managerial implications. First, the study confirms that influence of trust factors on willingness to disclose personal data online can be successfully grounded on SET. This adds to the theoretical knowledge about SET applications in marketing research. Second, the results suggest conclusion that trust is a very important factor in the SET-based model that positively influences both the data disclosure in social networking and the willingness to disclose personal data online. This is supported by other studies and is in-line with the conceptual framework of SET. Third, the study allows to conclude that conspiracy beliefs encourage involvement in social media and, consequently, the self-disclosure in social networking. However, in case of the willingness to disclose personal data in online shopping, the positive effect that is mediated by self-disclosure in social networking is weaker than negative direct effect of conspiracy beliefs. Therefore, the final conclusion is that conspiracy beliefs influence the willingness to disclose personal data in online shopping negatively.

The main managerial implication is based on the observation that negative effects of conspiracy beliefs on willingness to disclose personal data in online shopping could be at least partially neutralized through social networking that represents a two-way communication and stands for reciprocal social exchange. This suggests that businesses may consider a closer integration between the sites of social networking and online shopping, since the trust in social networking positively impacts the data disclosure in shopping.

Additionally, active support to regulatory systems as well as active promotion of social networking that prompts self-disclosure of consumers should be an aim of organizations that want to encourage disclosure of consumer data.

Limitations and further research. The main limitation of the current study is related to the scale that was used to measure conspiracy beliefs. The concept of conspiracy beliefs is rapidly evolving, and the tested beliefs have to be adequately included into studies. Though there is no evidence of any imperfections of the measurement in this study, the assessment of conspiracy beliefs remains to be limited to the specific time period and to the cultural context where the research has been performed.

The current study demonstrates importance of trust and conspiracy beliefs in regards of data disclosure and suggests ideas for future research. The findings suggest that further studies may consider to include factors of previous personal experience with personal data breaches, benefits of data disclosure, and power relations in exchange, which also are important aspects of SET. Additionally, future research can focus on how conspiracy believes impact institutional and interpersonal trust as the necessary elements of social exchanges.

Funding

This project by the Research Council of Lithuania (LMTLT) under Agreement No S-MIP-19-19.

Disclosure statement

Authors declare that they have no competing financial, professional, or personal interests from other parties.

References

Ahmad, W., & Sun, J. (2018). Modeling consumer distrust of online hotel reviews. *International Journal of Hospitality Management*, *71*, 77–90. https://doi.org/10.1016/j.ijhm.2017.12.005

Alarcon, G. M., Lyons, J. B., Christensen, J. C., Bowers, M. A., Klosterman, S. L., & Capiola, A. (2018). The role of propensity to trust and the five factor model across the trust process. *Journal of Research in Personality*, *75,* 69–82. https://doi.org/10.1016/j.jrp.2018.05.006

Allington, D., Duffy, B., Wessely, S., Dhavan, N., & Rubin, J. (2021). Health-protective behaviour, social media usage and conspiracy belief during the COVID-19 public health emergency. *Psychological Medicine, 51*(10), 1763–1769. https://doi.org/10.1017/S003329172000224X

Appel, G., Grewal, L., Hadi, R., & Stephen, A. T. (2020). The future of social media in marketing. *Journal of the Academy of Marketing Science*, *48*(1), 79–95. https://doi.org/10.1007/s11747-019-00695-1

Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management*, *52*, 1–13. https://doi.org/10.1016/j.ijinfomgt.2019.102063

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management*, *53*(1), 1–21. https://doi.org/10.1016/j.im.2015.08.001

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, *34*(7), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Bazarova, N. N., & Choi, Y. H. (2014). Self-disclosure in social media: Extending the functional approach to disclosure motivations and characteristics on social network sites. *Journal of Communication*, *64*(4), 635–657. https://doi.org/10.1111/jcom.12106

Bernerth, J., & Walker, H. J. (2009). Propensity to trust and the impact on social exchange. An empirical investigation. *Journal of Leadership & Organizational Studies*, *15*(3), 217–226. https://doi.org/10.1177/1548051808326594

Blau, P. (1964). *Exchange and power in social life.* Wiley.

Bleier, A., Goldfarb, A., & Tuckerc, C. (2020). Consumer privacy and the future of data-based innovation and marketing. *International Journal of Research in Marketing*, *37*(3), 466–480. https://doi.org/10.1016/j.ijresmar.2020.03.006

Brotherton, R., French, C. C., & Pickering, A. D. (2013). Measuring belief in conspiracy theories: The generic conspiracist beliefs scale. *Frontiers in Psychology*, *4*, 1–15. https://doi.org/10.3389/fpsyg.2013.00279

Byrne, B. M. (2010). *Structural equation modeling with AMOS: Basic concepts, applications, and programming* (2nd ed.). Routledge Taylor & Francis Group.

Chang, Y. S., & Fang, S. R. (2013). Antecedents and distinctions between online trust and distrust: Predicting high-and low-risk internet behaviors. *Journal of Electronic Commerce Research*, *14*(2), 149.

Chen, Y., Yan, X., Fan, W., & Gordon, M. (2015). The joint moderating role of trust propensity and gender on consumer's online shopping behaviour. *Computers in Human Behavior*, *43*, 272–283. https://doi.org/10.1016/j.chb.2014.10.020

Cheng, F. C., & Wang, Y. S. (2018). The do not track mechanism for digital footprint privacy protection in marketing applications. *Journal of Business Economics and Management*, *19*(2), 253–267. https://doi.org/10.3846/jbem.2018.5200

Cheng, J., Romero, D. M., Meeder, B., & Kleinberg, J. (2011). Predicting reciprocity in social networks. In *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing* (pp. 49–56). IEEE. https://doi.org/10.1109/PASSAT/SocialCom.2011.110

Cheshire, C. (2007). Selective incentives and generalized information exchange. *Social Psychology Quarterly*, *70*(1), 82–100. https://doi.org/10.1177/019027250707000109

Chung, K. L., Morshidi, I., Yoong, L. C., & Thian, K. N. (2019). The role of the dark tetrad and impulsivity in social media addiction: Findings from Malaysia. *Personality and Individual Differences*, *143*, 62–67. https://doi.org/10.1016/j.paid.2019.02.016

Degutis, M., Urbonavičius, S., Zimaitis, I., Skare, V., & Laurutytė, D. (2020). Willingness to disclose personal information: How to measure it? *Engineering Economics*, *31*(4), 487–494. https://doi.org/10.5755/j01.ee.31.4.25168

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce – A study of Italy and the United States. *European Journal of Information Systems*, *15*, 389–402. https://doi.org/10.1057/palgrave.ejis.3000590

Douglas, K. M., Uscinski, J. E., Sutton, R. M., Cichocka, A., Nefes, T., Ang, C. S., & Deravi, F. (2019). Understanding conspiracy theories. *Political Psychology*, *40*(S1), 3–35. https://doi.org/10.1111/pops.12568

Emerson, R. M. (1976). Social exchange theory. *Annual Review of Sociology*, *2*, 335–362. https://doi.org/10.1146/annurev.so.02.080176.002003

Emerson, R. M. (1981). Social exchange theory. In M. Rosenberg & R. H. Turner (Eds.), *Social psychology: Sociological perspectives* (pp. 30–65). Basic Books.

Foa, U. G., & Foa, E. B. (1974). *Societal structures of the mind*. Charles Thomas.

Frazier, M. L., Johnson, P. D., & Fainshmidt, S. (2013). Development and validation of a propensity to trust scale. *Journal of Trust Research*, *3*(2), 76–97. https://doi.org/10.1080/21515581.2013.820026

Georgiou, N., Delfabbro, P., & Balzan, R. (2020). COVID-19-related conspiracy beliefs and their relationship with perceived stress and pre-existing conspiracy beliefs. *Personality and Individual Differences*, *166*, 110201. https://doi.org/10.1016/j.paid.2020.110201

Goddard, M. (2017). The EU general data protection regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, *59*(6), 703–705. https://doi.org/10.2501/IJMR-2017-050

Goreis, A., & Kothgassner, O. D. (2020). Social media as vehicle for conspiracy beliefs on COVID-19. *Digital Psychology*, *1*(2), 36–39. https://doi.org/10.24989/dp.v1i2.1866

Goreis, A., & Voracek, M. (2019). A systematic review and meta-analysis of psychological research on conspiracy beliefs: Field characteristics, measurement instruments, and associations with personality traits. *Frontiers in Psychology*, *10*, 1–13. https://doi.org/10.3389/fpsyg.2019.00205

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). IGI Global. https://doi.org/10.4018/978-1-4666-6074-8.ch022

Gupta, B., Iyer, L. S., & Weisskirch, R. S. (2010). Facilitating global e-commerce: A comparison of consumers' willingness to disclose personal information online in the US and India. *Journal of Electronic Commerce Research*, *11*(1), 41–52.

Heirman, W., Walrave, M., Ponnet, K., & van Gool, E. (2013). Predicting adolescents' willingness to disclose personal information to a commercial website: Testing the applicability of a trust-based model. Cyberpsychology: *Journal of Psychosocial Research on Cyberspace*, *7*(3), 3. https://doi.org/10.5817/CP2013-3-3

Homans, G. C. (1961). *Social behaviour: Its elementary forms*. Taylor & Francis.

Hong, W., Chan, F. K. Y., & Thong, J. Y. L. (2021). Drivers and inhibitors of internet privacy concern: A multidimensional development theory perspective. *Journal of Business Ethics*, *168*, 539–564. https://doi.org/10.1007/s10551-019-04237-1

Jacobson, J., Gruzd, A., & Hernández-García, Á. (2020). Social media marketing: Who is watching the watchers? *Journal of Retailing and Consumer Services*, *53*, 1–12. https://doi.org/10.1016/j.jretconser.2019.03.001

Jenkins-Guarnieri, M. A., Wright, S. L., & Johnson, B. (2013). Development and validation of a social media use integration scale. *Psychology of Popular Media Culture*, *2*(1), 38–50. https://doi.org/10.1037/a0030277

Joinson, A. N., & Paine, C. B. (2007). Self-disclosure, privacy and the internet. In *Oxford handbook of Internet psychology* (pp. 237–252). Oxford University Press.

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. https://doi.org/10.1111/isj.12062

Keith, M. J., Babb, J. S., Lowry, P. B., Furner, C. P., & Abdullat, A. (2015). The role of mobile-computing self-efficacy in consumer information disclosure. *Information Systems Journal*, *25*(6), 637–667. https://doi.org/10.1111/isj.12082

Kim, D., Park, K., Park, Y., & Ahn, J. H. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior*, *92*, 273–281. https://doi.org/10.1016/j.chb.2018.11.022

Kim, J., & Kim, J. (2014). A study on the causes of information privacy concerns and protective responses in e-commerce: Focusing on the principal-agent theory. *The Journal of Information Systems*, *23*(4), 119–145. https://doi.org/10.5859/KAIS.2014.23.4.119

Kim, S., & Park, H. (2013). Effects of various characteristics of social commerce (s-commerce) on consumers' trust and trust performance. *International Journal of Information Management*, *33*(2), 318–332. https://doi.org/10.1016/j.ijinfomgt.2012.11.006

King, J. (2018). *Privacy, disclosure, and social exchange theory* [Dissertation]. University of California, Berkeley.

Koe, W. L., & Sakir, N. A. (2020). The motivation to adopt e-commerce among Malaysian entrepreneurs. *Organizations and Markets in Emerging Economies*, *11*(1), 189–202. https://doi.org/10.15388/omee.2020.11.30

Koohikamali, M., Peak, D. A., & Prybutok, V. (2017). Beyond self-disclosure: disclosure of information about others in social network sites. *Computers in Human Behaviour*, *69*, 29–42. https://doi.org/10.1016/j.chb.2016.12.012

Lee, S., & Choi, J. (2017). Enhancing user experience with conversational agent for movie recommendation: Effects of self-disclosure and reciprocity. *International Journal of Human-Computer Studies*, *103*, 95–105. https://doi.org/10.1016/j.ijhcs.2017.02.005

Lévi-Strauss, C. (1969). *The elementary structures of kinship* (Revised ed.). Beacon.

Lin, C. Y., Chou, E. Y., & Huang, H. C. (2020). They support, so we talk: The effects of other users on self-disclosure on social networking sites. *Information Technology & People*, *34*(3), 1039–064. https://doi.org/10.1108/ITP-10-2018-0463

Lwin, M., 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. https://doi.org/10.1007/s11747-006-0003-3

Malgieri, G., & Custers, B. (2018). Pricing privacy – the right to know the value of your personal data. *Computer Law & Security Review*, *34*(2), 289–303. https://doi.org/10.1016/j.clsr.2017.08.006

Martin, K. D., & Palmatier, R. W. (2020). Data privacy in retail: Navigating tensions and directing future research. *Journal of Retailing*, *94*(4), 449–457. https://doi.org/10.1016/j.jretai.2020.10.002

Masur, P. K. (2019). The theory of situational privacy and self-disclosure. In *Situational privacy and self-disclosure* (pp. 131–182). Springer, Cham. https://doi.org/10.1007/978-3-319-78884-5_7

Meier, Y., Schäwel, J., & Krämer, N. C. (2020). The shorter the better? Effects of privacy policy length on online privacy decision-making. *Media and Communication*, *8*(2), 291–301. https://doi.org/10.17645/mac.v8i2.2846

Meinert, D. B., Peterson, D. K., Criswell, J. R., & Crossland, M. D. (2006). Privacy policy statements and consumer willingness to provide personal information. *Journal of Electronic Commerce in Organizations*, *4*(1), 1–17. https://doi.org/10.4018/jeco.2006010101

Metzger, M. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication*, *9*(4). https://doi.org/10.1111/j.1083-6101.2004.tb00292.x

Molm, L., Takahashi, N., & Peterson, G. (2000). Risk and trust in social exchange: An experimental test of a classical proposition. *American Journal of Sociology*, *105*(5), 1396–1427. https://doi.org/10.1086/210434

Morimoto, M. (2021). Privacy concerns about personalized advertising across multiple social media platforms in Japan: The relationship with information control and persuasion knowledge. *International Journal of Advertising*, *40*(3), 431–451. https://doi.org/10.1080/02650487.2020.1796322

Mosteller, J., & Poddar, A. (2017). To share and protect: Using regulatory focus theory to examine the privacy paradox of consumers' social media engagement and online privacy protection behaviors. *Journal of Interactive Marketing*, *39*, 27–38. https://doi.org/10.1016/j.intmar.2017.02.003

Moyaery, M., & Urbonavičius, S. (2021). Importance of privacy regulatory environments on willingness to disclose personal data in e-stores. In *Proceedings of AIRSI 2021 Conference* (pp. 41–44). Zaragoza University, Spain.

Murphy, G. B. (2003). Propensity to trust, purchase experience, and trusting beliefs of unfamiliar e-commerce ventures. *New England Journal of Entrepreneurship*, *6*(2), 53–64. https://doi.org/10.1108/NEJE-06-02-2003-B008

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Olk, P. M., & Gibbons, D. E. (2010). Dynamics of friendship reciprocity among professional adults. *Journal of Applied Social Psychology*, *40*(5), 1146–1171. https://doi.org/10.1111/j.1559-1816.2010.00614.x

Padyab, A., Päivärinta, T., Ståhlbröst, A., & Bergvall-Kåreborn, B. (2019). Awareness of indirect information disclosure on social network sites. *Social Media+ Society*, *5*(2), 2056305118824199. https://doi.org/10.1177/2056305118824199

Parker, H. J., & Flowerday, S. (2021). Understanding the disclosure of personal data online. *Information & Computer Security*, *29*(3), 413–434. https://doi.org/10.1108/ICS-10-2020-0168

Pellegrini, V., Giacomantonio, M., De Cristofaro, V., Salvati, M., Brasini, M., Carlo, E., Mancini, F., & Leone, L. (2021). Is Covid-19 a natural event? Covid-19 pandemic and conspiracy beliefs. *Personality and Individual Differences*, *188*, 111011. https://doi.org/10.1016/j.paid.2021.111011

Prince, C. (2018). Do consumers want to control their personal data? Empirical evidence. *International Journal of Human-Computer Studies*, *110*, 21–32. https://doi.org/10.1016/j.ijhcs.2017.10.003

Robinson, 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. https://doi.org/10.1016/j.tele.2016.09.006

Robinson, S. C. (2018). Factors predicting attitude toward disclosing personal data online. *Journal of Organizational Computing and Electronic Commerce*, *28*(3), 214–233. https://doi.org/10.1080/10919392.2018.1482601

Schlosser, A. E. (2020). Self-disclosure versus self-presentation on Social media. *Current Opinion in Psychology*, *31*, 1–6. https://doi.org/10.1016/j.copsyc.2019.06.025

Shpak, N., Kuzmin, O., Dvulit, Z., Onysenko, T., & Sroka, W. (2020). Digitalization of the marketing activities of enterprises: Case study. *Information*, *11*(2), 109. https://doi.org/10.3390/info11020109

Skare, V., Urbonavicius, S., Laurutyte, D., & Zimaitis, I. (2020). Dispositional willingness to provide personal data online: Antecedents and the mechanism. In *Proceedings of the European Marketing Academy 49th Conference.*

Skrinjaric, B., Budak, J., & Rajh, E. (2019). Perceived quality of privacy protection regulations and online privacy concern. *Economic Research-Ekonomska Istraživanja*, *32*(1), 982–1000. https://doi.org/10.1080/1331677X.2019.1585272

Strycharz, J., van Noort, G., Helberger, N., & Smit, E. (2019). Contrasting perspectives-practitioner's viewpoint on personalised marketing communication. *European Journal of Marketing*, *53*(4), 635–660. https://doi.org/10.1108/EJM-11-2017-0896

Sun, Y., Zhang, Y., Shen, X. L., Wang, N., Zhang, X., & Wu, Y. (2018). Understanding the trust building mechanisms in social media: Regulatory effectiveness, trust transfer, and gender difference. *Aslib Journal of Information Management*, *70*(5), 498–517. https://doi.org/10.1108/AJIM-03-2018-0072

Swoboda, B., & Winters, A. (2021). Reciprocity within major retail purchase channels and their effects on overall, offline and online loyalty. *Journal of Business Research*, *125*, 279–294. https://doi.org/10.1016/j.jbusres.2020.12.024

Urbonavičius, S. (2020). Willingness to disclose personal data online: Not just a situational issue. In *Proceedings of AIRSI 2020 Conference* (pp. 66–90). Zaragoza University, Spain.

Urbonavičius, S., & Zimaitis, I. (2018). The mediating role of paranoia on online consumer behaviour. In *Proceedings of the 9th EMAC Regional Conference.* Prague, Czech Republic.

Urbonavicius, S., Degutis, M., Zimaitis, I., Kaduskeviciute, V., & Skare, V. (2021). From social networking to willingness to disclose personal data when shopping online: Modelling in the context of social exchange theory. *Journal of Business Research*, *136*, 76–85. https://doi.org/10.1016/j.jbusres.2021.07.031

Vadana, I. I., Torkkeli, L., Kuivalainen, O., & Saarenketo, S. (2019). Digitalization of companies in international entrepreneurship and marketing. *International Marketing Review*, *37*(3), 471–492. https://doi.org/10.1108/IMR-04-2018-0129

van der Schyff, K., Flowerday, S., & Furnell, S. (2020). Duplicitous social media and data surveillance: An evaluation of privacy risk. *Computers & Security*, *94*, 101822. https://doi.org/10.1016/j.cose.2020.101822

van Prooijen, J.-W., & de Vries, R. E. (2016). Organizational conspiracy beliefs: Implications for leadership styles and employee outcomes. *Journal of Business Psychology*, *31*, 479–491. https://doi.org/10.1007/s10869-015-9428-3

Varnali, K., & Toker, A. (2015). Self-disclosure on social networking sites. *Social Behavior and Personality*, *43*(1), 1–14. https://doi.org/10.2224/sbp.2015.43.1.1

Wakefield, R. (2013). The influence of user affect in online information disclosure. *The Journal of Strategic Information Systems*, *22*(2), 157–174. https://doi.org/10.1016/j.jsis.2013.01.003

Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management*, *36*(4), 531–542. https://doi.org/10.1016/j.ijinfomgt.2016.03.003

Weinberger, M., Bouhnik, D., & Zhitomirsky-Geffet, M. (2017a). Factors affecting students' privacy paradox and privacy protection behavior. *Open Information Science*, *1*(1), 3–20. https://doi.org/10.1515/opis-2017-0002

Weinberger, M., Zhitomirsky-Geffet, M., & Bouhnik, D. (2017b). Factors affecting users' online privacy literacy among students in Israel. *Online Information Review*, *41*(5), 655–671. https://doi.org/10.1108/OIR-05-2016-0127

Wirtz, B. W., Göttel, V., & Daiser, P. (2017). Social networks: Usage intensity and effects on personalized advertising. *Journal of Electronic Commerce Research*, *18*(2), 103–123.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, *12*(12), 798–824. https://doi.org/10.17705/1jais.00281

Yang, X. (2019). How perceived social distance and trust influence reciprocity expectations and eWOM sharing intention in social commerce. *Industrial Management & Data Systems*, *119*(4), 867–880. https://doi.org/10.1108/IMDS-04-2018-0139

Zhang, J., Hassandoust, F., & Williams, J. E. (2020). Online customer trust in the context of the general data protection regulation (GDPR). *Pacific Asia Journal of the Association for Information Systems*, *12*(1), 86–122. https://doi.org/10.17705/1pais.12104

Zhang, R., & Fu, J. S. (2020). Privacy management and self-disclosure on social network sites: The moderating effects of stress and gender. *Journal of Computer-Mediated Communication*, *25*(3), 236–251. https://doi.org/10.1093/jcmc/zmaa004

Zhao, J., Zhu, C., Peng, Z., Xu, X., & Liu, Y. (2018). User willingness toward knowledge sharing in social networks. *Sustainability*, *10*(12), 4680. https://doi.org/10.3390/su10124680

Zimaitis, I., Degutis, M., & Urbonavicius, S. (2020a). Social media use and paranoia: Factors that matter in online shopping. *Sustainability*, *12*(3), 904. https://doi.org/10.3390/su12030904

Zimaitis, I., Urbonavicius, S., Degutis, M., & Kaduskeviciute, V. (2020b). Impact of age on the willingness to disclose personal data in e-shopping. In *Proceedings of EMAC 11th Regional Conference*. Zagreb. http://proceedings.emac-online.org/pdfs/R2020-84569.pdf

Zimmer, J. C., Arsal, R. E., Al-Marzouq, M., & Grover, V. (2010). Investigating online information disclosure: Effects of information relevance, trust and risk. *Information & Management*, *47*(2), 115–123. https://doi.org/10.1016/j.im.2009.12.003

NOTES

NOTES

Vilniaus universiteto leidykla
Saulėtekio al. 9, III rūmai, LT-10222 Vilnius
El. p. info@leidykla.vu.lt, www.leidykla.vu.lt
bookshop.vu.lt, journals.vu.lt
Tiražas 15 egz.