FUNDAÇÃO GETULIO VARGAS
ESCOLA DE ADMINISTRAÇÃO DE EMPRESAS DE SÃO PAULO

VICTOR GUERRA DE OLIVEIRA

PRIVACY FOR SALE:

A STUDY ABOUT USERS TRADING PERSONAL DATA

FOR PERCEIVED BANKING BENEFITS

SÃO PAULO

2019

VICTOR GUERRA DE OLIVEIRA

PRIVACY FOR SALE:

A STUDY ABOUT USERS TRADING PERSONAL DATA

FOR PERCEIVED BANKING BENEFITS

Trabalho Aplicado apresentado à Escola de Administração de Empresas de São Paulo da Fundação Getulio Vargas como requisito para a obtenção do título de Mestre em Gestão para a Competitividade

Campo do Conhecimento: Tecnologia da Informação

Prof. José Luiz Kugler (Orientador)

SÃO PAULO
2019

Oliveira, Victor Guerra de.

Privacy for sale : a study about users trading personal data for perceived banking benefits / Victor Guerra de Oliveira. - 2019.

36f.

Orientador: José Luiz Carlos Kugler.

Dissertação (mestrado profissional MPGC) – Fundação Getulio Vargas, Escola de Administração de Empresas de São Paulo.

1. Proteção de dados. 2. Direito à privacidade. 3. Bancos - Inovações tecnológicas. 4. Experiência do usuário. 5. Tecnologia da informação. I. Kugler, José Luiz Carlos. II. Dissertação (mestrado profissional MPGC) – Escola de Administração de Empresas de São Paulo. III. Fundação Getulio Vargas. IV. Título.

CDU 336.71

Ficha Catalográfica elaborada por: Isabele Oliveira dos Santos Garcia CRB SP-010191/O

Biblioteca Karl A. Boedecker da Fundação Getulio Vargas - SP

VICTOR GUERRA DE OLIVEIRA

PRIVACY FOR SALE:

A STUDY ABOUT USERS TRADING PERSONAL DATA

FOR PERCEIVED BANKING BENEFITS

Trabalho Aplicado apresentado à Escola de Administração de Empresas de São Paulo da Fundação Getulio Vargas como requisito para a obtenção do título de Mestre em Gestão para a Competitividade

Campo do Conhecimento: Tecnologia da Informação

Data da Aprovação:

29 / 05 / 2019

Banca examinadora:

_____

Prof. José Luiz Kugler (Orientador) – FGV-EAESP

_____

Prof. Claudio Luis Carvalho Larieira FGV-EAESP

_____

Prof. Aguinaldo Aragon Fernandes USP

SÃO PAULO
2019

RESUMO

Tecnologias estão disseminadas em todo o mundo, tornando muito mais simples o processo de compartilhar informações e fazendo com que pessoas e empresas possam se conectar umas com as outras. No entanto, o compartilhamento excessivo de dados de privacidade pode resultar em um fenômeno chamado “Paradoxo da Privacidade”. Substancialmente, o Paradoxo de Privacidade indica que as pessoas tendem a compartilhar dados pessoais e de privacidade, mesmo sem ter consciência ou em troca de algum benefício, o que é um ato contraditório para suas próprias crenças.

Destacando a economia atual, o uso de dados, em todos os tipos, molda uma nova maneira de criar produto e serviços. Ao mesmo tempo, as políticas de privacidade e até mesmo os vazamentos de informação estão cada vez mais frequentes nos noticiários, trazendo um senso de risco sobre os dados que estão disponíveis para as empresas e nas redes sociais.

Este estudo é o primeiro a aplicar esse tipo de análise ao cenário bancário, abordando o uso de dados de privacidade pelos bancos e o que poderia ser negociado com o proprietário dos dados para obtê-lo. Destacando o fenômeno do paradoxo da privacidade, o estudo usa estes dados como moeda, abstraído como benefícios bancários ou até mesmo dinheiro através de um estudo quantitativo analisando a relação entre o comportamento de auto revelação, benefícios e as intenções de futuro próximo e distante.

Palavras-chave: Dados de Privacidade; Dados Pessoais; Paradoxo da Privacidade; Bancos; Experiência do Usuário; Inteligência de Dados

ABSTRACT

Technologies are disseminated worldwide making much simpler the process of sharing information and making people and companies connected to each other. However, the oversharing of privacy data could leave to phenomenon called Privacy Paradox. Substantially the Privacy Paradox indicates that people tend to share personal and privacy data even without fully understanding or to have some benefit, which is contradictory act to their own beliefs.

Shedding light on nowadays economy, the use of data, at all kinds, shapes a new way of making products, services and customized solutions. At the same time, privacy policies and breaches are each more often on the news, bringing a sense of risk about the data that is available to companies and on social networks.

This study is first that applies this kind of analysis to the banking scenario, approaching the use of privacy data by the dot.com industry and what could be traded with the data owner in order to have it. Shedding light on the privacy paradox phenomenon, the study uses these data as currency – abstracted as bank benefits or even money – through a quantitative study analyzing the relationship between self-disclosure behavior, benefits, and the intentions of the near and distant future.

Keywords: Privacy Data; Personal Data; Privacy Paradox; Banking; User Experience; Data Business

TABLE OF FIGURES

TABLE OF TABLES

SUMMARY

1. INTRODUCTION

Ubiquitous technologies, such as smartphones and every single app on it, make the most of consumer's data, which keeps the debate of privacy on evidence (Adjerid et al., 2018). Privacy data nowadays is just about becoming a real business to their "first owner". Actually, according to a Symantec (2015) research, at least 30% of respondents willed to trade their e-mail information for chances of winning prizes or even money.

However, lots of surveys results show that the privacy is an important issue for online users worldwide, but most users don't make decisions based on protecting this data (Gerber, Gerber and Volkamer, 2018). This phenomenon is so called "Privacy Paradox", which Acquisti (2005), defined as: when a user has an opinion towards privacy behavior online which results in a dichotomy between privacy attitudes and actual behavior or beliefs.

The dot.com services makes the most of this data to build personalized solutions and almost couldn't exist without it (Berger, 2010) and thinking about banking solutions, goes the same way. According to a Deloitte report (2017) the forecast number of digital users of retail banking services would be about three billion by 2021. Most of them should allow the use of privacy data of their smartphones, smartwatches, tablets, PCs and social medias – even without fully understanding – in exchange of customized products, services and conditions.

Although several researchers have developed studies about the "Privacy Paradox" (Gerber, Gerber and Volkamer, 2018; Obar and Oeldorf-Hirsch, 2018), there are no conclusive works about trading private data in this new banking landscape, since many studies light the behavior itself (Barth and de Jong, 2017; Taddicken, 2014) and many others use examples of e-commerce, or social media to explain this phenomenon (Wang et al., 2015; Hallam and Zanella, 2016; Adjerid et al., 2018).

In order to go further about the decision of trading privacy data, is important to understand about the decision-making process as well, which is the result of several individualities and cannot be considered as totally rational (Nonohay, 2012). Even with the arguments that the decision-making process is not totally rational, there is a theory that simplifies the understanding by bringing to a scenario of this scope, the theory of "Economic Human", where individual decision-makers aim for maximum return (Simon, 1959), bringing at light a possible risk-benefit calculation (Barth and de Jong, 2017).

That way, this paper intends to contribute with a new perspective on a study about users trading privacy data with a bank, which brings the sense of money itself closer to this "negotiation", since some researchers already argued that privacy data is a commodity and can be traded for benefits (Campbell & Carlson, 2002).

2. LITERATURE REVIEW

The literature review was performed in a way that complements the sections of this study. To this end, is going to be show the main points of the works that are considered theoretical references within each theme, and subsequently the use of these for the elaboration of the research model.

2.1. The Privacy Paradox

On the literature review the most accepted explanation about Privacy Paradox is when users have a tendency towards privacy-compromising behavior online which results in a dichotomy between privacy attitudes and actual behavior (Acquisti and Grossklags, 2005).

Information Systems literature review showed that privacy concern makes difference – both encouraging and discouraging – on online activity, as shopping or giving personal information for creating SNS (Social Network Sites) profiles (Culnan and Armstrong, 1999; Malhotra, Kim and Agarwal, 2004).

Although users are aware of the risks of oversharing privacy data, part of them intentionally, or not, make deals with this information, such as giving their e-mail, friends network or location in trade of something or even for the opportunity of using an app or a SNS (Symantec, 2015; Acquisti and Grossklags, 2005; Buck et al., 2014).

Most studies about the Privacy Paradox consists in analysis of behavior itself (Barth and de Jong, 2017) on e-commerce and social networks (Wang et al., 2015; Hallam and Zanella, 2016; Adjerid et al., 2018), both of this majority themes are digital activities supported by devices such as smartphones, tablets and PCs – that leave a lot of digital trace of users. This data can be used in order to make better and customized products, services and solutions for each individual and that's exactly how the dot.com economy survives (Berger, 2010).

An extrapolation of a scenario where each single user does not provide their privacy data could result in a major discouragement of dot.com economy, and there is a risk in this example as a regulation (Min Baek, 2014) – since some countries, as the European ones, could not leave this to a self-regulation with companies and users (Wired, 2018).

Another point of view shows that is not easy to a user agrees or even have understands about privacy policies. However, this statement does not support itself, that's because the issue extends to considerable portion of the interviewed population, including IT professionals who does have knowledge about cookies (a package of navigation data), for example, (Gordon, 2004). It's also interesting to demonstrate that with better and more transparent communications would be possible to help the decision-making by users and tend to solve this negotiation of data (Deuker, 2010), which leads to next theme: decision-making.

2.2. Decision-making based on benefits

The decision-making process is fairly discussed on academic landscape over the past 60 years. However, it can't be considered as a fully rational decision, since the decision-making process is the result of several individualities as mood and any others psychological factors combined to a rational process of identifying problems and aiming solutions (Courtney, 2001; Nonohay, 2012).

However, when the subject is trading privacy data, which can be viewed as a currency for this example, the privacy calculus theory (Dinev and Hart, 2006) makes an important contribution showing that the risk-benefit calculus determines the behavior. Following the interpretation that privacy could be a commodity – which can be exchanged for benefits (Xu, Teo, Tan, & Agarwal, 2009; Papacharissi, 2010) – makes a converging resolution to the theory of "Economic Human", where individual decision-makers aim

for maximum return, provided that having all the knowledge, or this perception, to make the call (Simon, 1959).

Another perspective about the will of sharing their own data on digital platforms, as Facebook, is about the social relations on this environment (Trepte and Reinecke, 2011), which can also be defined as a social reward (Hallam and Zanella, 2016) and could be compared to any other benefit.

2.3. The Theory of Planned Behavior

In this behavior landscape, there is an established theory, the Theory of Planned Behavior (TPB) (Ajzen, 1985, 1991) that can explain behavior itself.

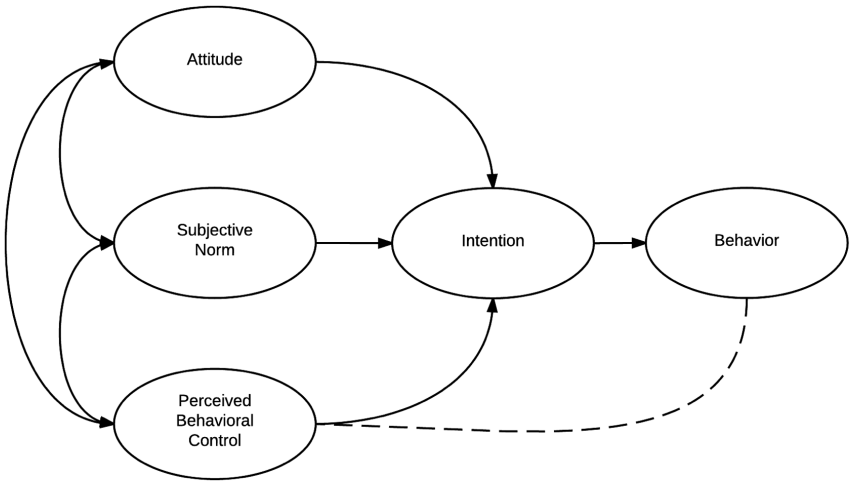

Figure 1 - TPB Concepts (Ajzen, 1985, 1991)

The TPB is broadly used in psychology to explain behaviors over which people have the ability to exert self-control. The theory is composed by 5 components: Attitude, Subjective Norm, Perceived Behavioral Control, Intentio and the Behavior.

Ajzen (1985, 1991) described each one of those components as: Attitude being represented by the act of measuring the results of behavior building; Subjective Norm representing the belief about what other people think about approving or disapproving the behavior; Perceived Behavioral Control refers to the perception of how easy or difficult is performing the behavior itself; Intention is a sign of readiness of an individual to perform

a behavior; Behavior can be defined as the function of compatible intentions and perceptions of behavioral control, producing the behavior.

2.4. The digital banking scenario

Retail banks should invest on customization services and features such as advices for each customer need and in cybersecurity to support the use of data without impairing the user experience (Deloitte, 2017). Besides that, in order to expose the size of this market, the forecast number of digital users of digital banking services, such as smartphone app's, would be about three billion by 2021. (Deloitte, 2017)

Bringing even more light to the subject, Global Fortune 500 companies spend, on average, $34 million a year on mobile application development and about $2 million is invested in mobile security (Intertrust, 2016). Also, security and privacy concern point out to be main decision factor for users to switch banks, showing the importance of this discussion and consequent need of feeling security on mobile banking apps (Huei, Zhang and Chen, 2013; Intertrust, 2016).

Important to mention that exists a co-responsibility of the user and companies in a digital environment, especially when talking about privacy data (Bansal, 2017). However, as already viewed, there are alternatives on user experience process in order to explains better the privacy policies helping the understand and the decision-making process of users who do or do not want to negotiate their own privacy data (Deuker, 2010).

More and more companies realized that data is their most precious asset, and on the banking landscape this is also true, the experience should be unique to each user, attrition needs to be reduced, and customers want to be rewarded (Dash and Das, 2017; Deloitte, 2017).

3. RESEARCH MODEL AND HYPOTHESES

As viewed in the literature review, privacy paradox brings us to a self-disclosure behavior, which is the result of a trade-off privacy itself and benefits. According to Hallam and Zanella (2016), TPB has been successful explaining privacy behaviors.

Based on the TPB literature (Ajzen, 1985, 1991), the research model has the components to analyze behavior itself and it is proposed two intention variables (distant-future and near-future).

This research model is adapted from Hallam and Zanella (2016), that intended to predict a dependable value based on "Privacy Concerns", "Social Rewards", "Near-Future Intentions", "Distant-Future Intention" and the "Self-Disclosure Behavior". However, in order to make a contribution by the lens of a digital bank, inserted in a dot.com economy, the mayor adaptation resides on changing "Social Rewards", to "Rewards" – so it can be considered any kind of reward such as, money or banking benefits, since this study has a focus on the banking industry.

It is expected a negative association between privacy concern (Awareness, Control and Collection) and distant-future intentions, with an increase in privacy concern driving a decrease in distant-future disclosure intentions, just as the work of Hallam and Zanella (2016), which inspired this research and hypothesis, as follows:

H1. Privacy concern is not related to sensitive information self-disclosure behavior.

The original study proposed that "Social Rewards" is positively related to the near-future self-disclosure. So, the new hypothesis brings a concept of any kind of rewards:

H2. Rewards, in general, are positively related to near-future self-disclosure intentions.

As we asked about the near-future, is believed that the distant-future have others lines of reasoning, with more preoccupation about privacy data, and it is expected to be a just the opposite of near-future intentions off conceding your own personal data.

H3. Self-disclosing behavior is not related to distant-future self-disclosure intentions.

H4. Self-disclosing behavior is positively related to near-future self-disclosure intentions.

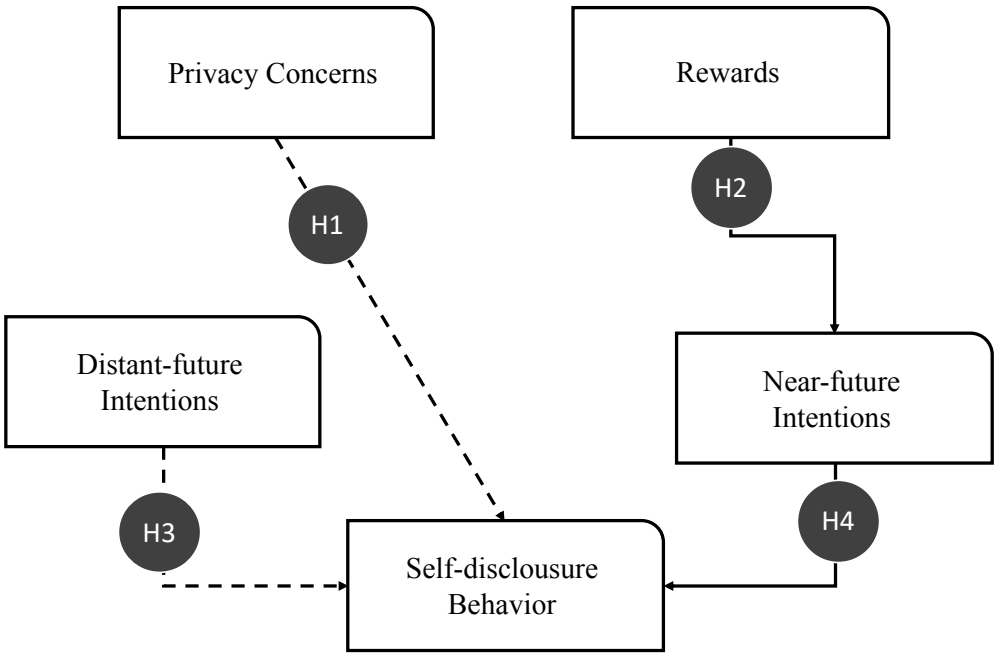

Figure 2 - Research Hypotheses Model (adapted from Hallam and Zanella, 2016)

4. METHODOLOGY

This study uses a survey as the method to collect data; multivariate data analysis was applied to assess the possible relationship among the variables of interest. The survey approach is an important research method, which consists of a standardized approach to collect information on individuals´ behavior and attitudes (Rossi, Wright and Anderson, 2013).

4.1. Participants

The participants were sampled from Pollfish, a survey platform provided by a popular start-up for conducting such pools. Pollfish's survey platform has the capability of achieving almost 200 million smartphone owners, in order to have potential respondents. It is important do notice that prior research has already validated those kinds of platforms – that uses online participant tools, such as Amazon Mechanical Turk (AMT) – as representative as a regular internet sample (Buhrmester et al., 2011).

The quantitative analysis was performed with 386 respondents, achieving a 95% confident level and a margin of error of 5%. The only criteria for selecting participants was being above 18 years old, in order to have respondents with some banking experience or knowledge.

4.2. Instrument

The online survey instrument was based upon a 4-points Likert-type scale. The questions were adapted from the study of Hallam and Zanella (2016). The changes in wording were intended to shed light on the banking perspectives of offering the participants a tangible reward vis a vis the voluntary collection of data, as presented in Appendix A.

4.3. Data

The data obtained is as a CSV file from Survey Monkey. After manipulating this sheet to have declarable collumns and lines for the R scripts it ended with 22 columns and 386 lines, that can be accessed on:

https://drive.google.com/open?id=1_JcT28pNe9toPHU3FOOv8iZ8QU1IMGtE

4.4. Instrument validation

First, we ran an exploratory factor analysis (EFA) for each question of our survey as a variable to understand how much factors did we have. Table 1 reports the clusterization of each variable as a factor itself. Following literature, we only considered factor loadings greater than 0.40 (Hinkin, 1998). One of the "distant-future" variables have been dropped (DF2 - "In the future, I would continue sharing my data like I'm doing now."), since it has a load less than 0.40.

Factor Analysis - Standardized loadings (pattern matrix) based upon correlation matrix

	MR1	MR3	MR5	MR4	MR2
CON1	0.11	**0.60**	0.03	0.07	0.05
CON2	0.00	**0.61**	0.18	0.16	-0.10
CON3	-0.06	**0.64**	-0.07	0.16	0.12
AWA1	-0.06	**0.62**	0.12	-0.02	-0.08
AWA2	0.13	**0.47**	0.07	-0.15	0.30
AWA3	0.11	**0.40**	0.05	-0.25	0.42
COL1	0.05	0.02	**0.56**	0.03	0.08
COL2	-0.03	0.06	**0.67**	0.05	0.03
COL3	0.02	0.02	**0.75**	-0.07	0.03
COL4	0.05	0.14	**0.42**	-0.03	0.26
RE1	**0.59**	-0.06	0.26	-0.02	0.02
RE2	**0.81**	0.12	-0.03	-0.11	-0.12
RE3	**0.49**	0.14	0.07	0.16	0.02
BH1	**0.47**	-0.05	0.00	0.19	0.16
BH2	**0.64**	-0.07	-0.11	0.13	0.23
BH3	**0.66**	-0.11	0.09	0.24	-0.07
NF1	0.39	-0.04	0.16	**0.42**	-0.06
NF2	0.06	0.10	-0.01	**0.87**	0.06
NF3	0.36	0.21	-0.07	**0.40**	-0.10
DF1	0.00	0.04	0.11	0.01	**0.66**
DF2	0.34	0.16	-0.11	0.09	*0.07*
DF3	-0.12	0.00	0.20	0.17	**0.62**

Table 1 – EFA

It is important to notice that differently from Hallam and Zanella (2016) we did have the 5 factors, however during the EFA exercise we were not able to set "The Privacy Concern" as: Awareness, Control and Collection in a clusterization as a single factor. This way the factors are composed as the table below.

MR1:	Rewards + Self Disclosure Behavior
MR2:	Distant-future Intentions
MR3:	Controll + Awareness
MR4:	Near-future Intentions
MR5:	Collection

Table 2 – Factors

5. RESULTS

The research hypotheses were tested using Structural Equation Modeling (SEM). The model was implemented in R and its code is presented in Appendix B. The results are summarized in Table 2, in order to understand the correlation of each factor between them; Figure 2 illustrates the factors and the relationship of the SEM.

Factor correlations

	MR1	MR3	MR5	MR4	MR2
MR1	1.00	*0.22*	0.19	**0.49**	*0.03*
MR3	*0.22*	1.00	**0.38**	*0.19*	**0.36**
MR5	*0.19*	**0.38**	1.00	*0.12*	**0.45**
MR4	**0.49**	*0.19*	*0.12*	1.00	*0.09*
MR2	0.03	**0.36**	**0.45**	*0.09*	1.00

Table 3 - SEM results

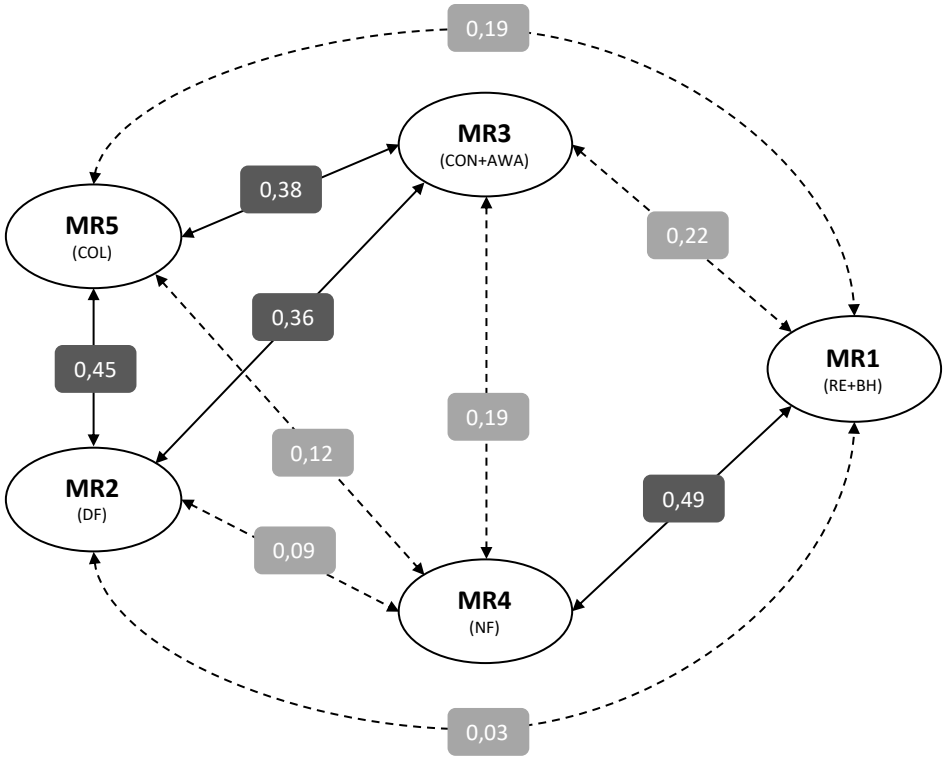

Figure 3 - SEM result

During the EFA exercise we were not able to set "The Privacy Concern" as: Awareness, Control and Collection in a clusterization as a single factor, however, we understood that the banking landscape it is different from other companies, because the

bank already has the privacy data, as cash inflows, name, address, relationship and many other information, therefore, Collection became a single factor itself (MR5).

However, bringing this explanation to the hypothesis analysis turned into no surprise. As expected, both factors – “Collection” (MR5) and “Concern + Awareness” (MR3) – do not have significantly relation to self-disclosure behavior (MR1), supporting H1 – “Privacy concern is not significantly related to sensitive information self-disclosure behavior”.

Another important difference between this study from Hallam and Zanella (2016) is the composition of the factor “Self-disclosure behavior”. Our EFA exercise demonstrated a cluster of this factor added to the rewards variables, therefore, creating the factor “Self-disclosure behavior + Rewards” (MR1), however it was not an issue for the hypothesis validation, since Near-future intentios (MR4) have the greater relation with “Self-disclose behavior + Rewards” (MR1), also supporting H2 – “Rewards, in general, are positively related to near-future self-disclosure”.

Also as expected, the self-disclosure behavior (MR1) has a strongly relation with near-future intentions (MR4) and do not have a significant one with distant-future intentions (MR2), which supports H3 – “Self-disclosing behavior is not significantly related to distant-future self-disclosure intentions” – and H4 – “Self-disclosing behavior is positively related to near-future self-disclosure intentions”.

Hypothesis		Assessment
H1	Privacy concern is not related to sensitive information self-disclosure behavior.	Since "Privacy Concern" is explained as: "Awareness, Control and Collection" we did have to analyze the relation between MR1 with MR3 (Awareness+Control) and MR5 (Collection). MR1 -- MR3 = 0,22 (not significant relation) MR1 -- MR5 = 0,19 (not significant relation)
H2	Rewards, in general, are positively related to near-future self-disclosure intentions.	To understand the relation between Rewards and Near-future self-disclosure intentions we analised MR1 with MR4 (important to notice that MR1 is represented by: Self-disclosure behavior + Rewards) MR1 -- MR4 = 0,49 (significant relation)
H3	Self-disclosing behavior is not related to distant-future self-disclosure intentions.	To understand the relation between Distant-future intentions and Self-disclosure behavior we analised MR1 with MR4. MR1 -- MR2 = 0,03 (not significant relation)
H4	H4. Self-disclosing behavior is positively related to near-future self-disclosure intentions.	Since MR1 was designed during the EFA excercise as "Rewards + Self-disclosure behavior" we already validated this hypothesis on H2. To understand the relation between Self-disclosure behavior and Near-future intentions we analised MR1 with MR4 (important to notice that MR1 is represented by: Self-disclosure behavior + Rewards) MR1 -- MR4 = 0,49 (significant relation)

Table 4 - Hypotheses results

6. DISCUSSION

This present paper sheds light on privacy paradox through a singular landscape. While the work of Hallam and Zanella (2016) is broadly generalizable, our work is the first that applies this kind of analysis to the banking scenario, approaching the use of privacy data by the dot.com industry and what could be traded with the data owner in order to have it. Apropos, we validated our hypothesis and one of the most important result is the relationship about how near-future and distant-future affects the self-disclosure and at what price – as rewards.

It should be pointed out that this work has taken into account different factors in comparison to previous studies (Wang et al., 2015; Hallam and Zanella, 2016; Adjerid et al., 2018). The privacy concern – set as Control, Awareness and Collection – has been changed in this banking landscape, since banks already have participant's information and a lot of privacy data. Thus, a detachment of Collection as a single factor is warranted. It is interesting to note this study showed how important is the factor "Control and Awareness", which is also considered a single factor in this context. Since the participants do not have the same autonomy on Collection they appear to want full control and awareness about their own information.

Moreover, performing this research in a financial industry showed how close is the relation between the customer's information in exchange of some benefit to itself and how the companies should care about privacy concerns since data is valuable.

7. LIMITATIONS AND FUTURE RESEARCH

A usual limitation on behavior research is the self-reporting nature of the survey that indicates a possible social bias (Fisher, 1993). Making the survey anonymous was an attempt to resolve this issue.

There was also an issue with instrument having to drop one of our variables about distant-future as result of the EFA, however, dropping the DF2 variable - "In the future, I would continue sharing my data like I'm doing now." - was not an issue for validation of the distant-future intentions construct.

It was not possible to analyze in a deeper fashion the composition of the sample. Given the approach used by the survey platform – Pollfish – it was impossible to investigate the relationship among the personal characteristics of the respondents; the way the platform was configured allowed the random selection of people above 18 years old and did not take into account specifications about gender, education, income, computer experience and many other characteristics that could be useful.

Notwithstanding, we suggest further research about privacy concerns by adding more characteristics about the participants and applying this same analysis in other user-banking scenarios, bringing a tangible contribution for the banking sector.

8. CONCLUSION

The effort in this work was an attempt to understand the "Privacy Concern", applied to a singular scenario – personal banking – that requires the intense use of consumer data to maximize results and couldn't exist without exploring such data. Thus, this study made possible to understand some of the relationships between the self-disclosure behavior and future intentions (near and distant).

This way it was possible to validate how the privacy paradox can explain banking rewards – or any kind of benefit perceived by potential user – acting on near-future intentions that affects the subsequent behavior, differently from distant-future intentions, which do not directly affect behavior itself.

REFERENCES

Acquisti, A., (2004). Privacy in electronic commerce and the economics of immediate gratification. In: EC ’04 Proceedings of the 5th ACM Conference on Electronic Commerce, USA, 21-29.

Acquisti, A., Grossklags, J., (2005). Privacy and rationality in individual decision making. IEEE Secur. Priv. 3 (1), 26–33.

Adjerid, Idris; Peer, Eyal; and Acquisti, Alessandro. (2018). "Beyond the Privacy Paradox: Objective Versus Relative Risk in Privacy Decision Making". MIS Quarterly, (42: 2) pp.465-488.

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl, & J. Beckmann (Eds.), Action Control: From cognition to behavior (pp. 11e39). Berlin, Heidelberg: Springer (Berlin Heidelberg).

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179e211.

Baek, Y.M., (2014). Solving the privacy paradox: A counter-argument experimental approach. Comput. Hum. Behav. 38, 33–42.

Bansal, G. (2017). – Distinguishing between Privacy and Security Concerns: An Empirical Examination and Scale Validation. – Journal of Computer Information Systems. Vol. 57 Issue 4, p330-343. 14p., 2017.

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. DOI: 10.1016/j.tele.2017.04.013.

Berger, D. D. (2010). Balancing consumer privacy with behavioral targeting. Santa Clara Computer & High Technology Law Journal, 27(3), 3–61.

Buck, C., Horbel, C., Germelmann, C.C., Eymann, T., (2014). The unconscious app consumer: Discovering and comparing the information-seeking patterns among mobile application consumers. In: Twenty Second European Conference on Information Systems, Tel Aviv, Israel, 1–14.

Buhrmester, M., Kwang, T., and Gosling, S. D. 2011. "Amazon's Mechanical Turk: A New Source of Inexpensive, Yet High-Quality, Data?," Perspectives on Psychological Science (6:1), pp.3-5.

Campbell, J. E., & Carlson, M. (2002). Panopticon. com: Online surveillance and the commodification of privacy. Journal of Broadcasting and Electronic Media, 46(4).

Courtney, J. (2001). Decision making and knowledge management in inquiring organizations: toward a new decision-making paradigm for DSS. Decision Support Systems 31, no. 1: 17-38, 2001.

Dash, M., & Das, K. (2017). Customer Attrition Analytics in Banking. International Journal of Business Analytics & Intelligence (IJBAI), 5(2), 7–14.

Deloitte (2017). Digital Banking Benchmark. Deloitte https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/Banking/lu-digital-banking-benchmark.pdf Accessed 07 October 2018.

Deuker, A., 2010. Addressing the privacy paradox by expanded privacy awareness – the example of context-aware services. In: Bezzi, M., Duquenoy, P., Fischer-Hüber, S., Hansen, M., Zhang, G. (Eds.), Privacy and Identity Management for Life. Springer-Verlag, Berlin, Heidelberg, pp. 275–283.

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. European Journal of Social Psychology, 45(3), 285e297.

Dinev, T., Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. Inf. Syst. J. 17 (1), 61–80.

Fisher, R. J. (1993). Social desirability bias and the validity of indirect questioning. Journal of Consumer Research, 303e315.

Gerber, Gerber and Volkamer. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. Computers & Security, Volume 77, August 2018, Pages 226-261.

Gordon, S. (2004). Privacy: A study of attitudes and behaviors in US, UK and EU information security professionals (Symantec White Paper).

Hallam, C.R., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. Computers in Human Behavior, 68, 217-227.

Hinkin, T. R. (1998). A brief tutorial on the development of measures for use in survey questionnaires. Organizational Research Methods, 1(1), 104e121.

Huei, L., Zhang, Y. and Chen, K. (2013) – An Investigation of Features and Security in Mobile Banking Strategy. Journal of International Technology and Information Management - Volume 22., 2013.

MacCallum, R. C., Browne, M. W., & Sugawara, H. M. (1996). Power analysis and determination of sample size for covariance structure modeling. Psychological Methods, 1(2), 130.

Nonohay, R. (2012) – Tomada de decisão e os sistemas cerebrais: primeiros diálogos entre administração, psicologia e neurofisiologia. 149 f. Federal University of Rio Grande do Sul School of Management, 2012.

Obar, J., Oeldorf-Hirsch, A. (2018) – The biggest lit on the Internet: ignoring the privacy policies and terms of service policies of social networking services. Information, Communication & Society, 2018, Pages 1-20.

Papacharissi, Z. (2010). A private sphere: Democracy in a digital age. Polity. PEW. (2014). Public perceptions of privacy and security in the Post-Snowden Era. Pew Research Center.

Rossi, P., Wright, J. and Anderson, A. (2013). Handbook of survey research., Accademic Press.

Symantec (2015). State of privacy report 2015. Symantec. https://www.symantec.com/content/en/us/about/presskits/ b- state- of- privacy-report-2015.pdf Accessed 09 October 2018.

Simon, H. A. (1959). Theories of Decision-Making in Economics and Behavioral Science. American Economic Review, 49, 253-283.

Taddicken, Monika. (2014). The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Differente Forms of Self-Disclosure. Journal of Computer-Mediated Communication, v. 19, n. 2, p. 248-273.

Trepte, S., & Reinecke, L. (2011). The social web as a shelter for privacy and authentic living. In Privacy online (pp. 61e73). Springer.

Wang, N, Zhang B, Liu B, Jin H. (2015). Investigating effects of control and ads awareness on android users' privacy behaviors and perceptions. Proceedings of the seventeenth international conference on human-computer interaction with mobile devices and services, 2015. p. 373-82.

Wired – Europe's new privacy law will change the web, and more., 2018. https://www.wired.com/story/europes-new-privacy-law-will-change-the-web-and-more. Accessed 09 October 2018.

Xu, H., Teo, H.-H., Tan, B.C.Y., Agarwal, R. (2010). The role of push-pull technology in privacy calculus: the case of location-based services. J. Manage. Inf. Syst. 26 (3), 135–173.

APPENDIX A – The Questionnaire

A1.1. Privacy concerns

- Control
  - CON1: Online privacy is really a matter on consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.
  - CON2: Consumer control of personal information lies at the heart of consumer privacy.
  - CON3: Online privacy is invaded when control is lost or unwillingly reduced.
- Awareness
  - AWA1: Companies seeking information online, such as banks, should disclose the way data are collected, processed and used.
  - AWA2: A good consumer online privacy policy should have a clear and reliable disclosure mechanisms for consumers.
  - AWA3: It is very important to me that I am aware and knowledgeable about how my personal information will be used.
- Collection
  - COL1: It usually bothers me when online companies ask me for personal information.
  - COL2: If my bank asks me for personal online information, I would think twice before providing it.
  - COL3: It bothers me to give financial information to so many online companies, such as banks.

- COLL4: I'm concerned that online companies, such as banks, are collecting too much personal information about me.

A1.2. Reward

- RE-1: I disclose personal data online because it fulfills my social needs in some way.
- RE-2: I disclose personal data online because it helps me cultivate good relationships with companies, business partners or even friends.
- RE-3: I disclose personal data online because I derive financial benefits from it.

A1.3. Near-future intentions

- NF-1: If I had today a new wearable device or a new profile on Social Network App, I would openly share my personal data online.
- NF-2: If I had today a new wearable device or a new profile on Social Network App, I would share privacy data in case my bank asked for it in exchange of some benefit, such as a better option of investment, a lower rate on a loan or even a recommendation.
- NF-3: If I had today a new wearable device or a new profile on Social Network App, I would share personal data to obtain a free gift valued at U$50.

A1.4. Distant-future intentions

- DF-1: In the future, I would like to better protect my personal data.
- DF-2: In the future, I would continue sharing my data like I'm doing now. (dropped)
- DF-3: In the future, I intend to be more selective about sharing personal information online.

A1.4. Self-disclosure behavior

- BH-1: I often share personal data such as age, home address and favorite places.

- BH-2: I often share personal data from my smartphone, such as location, photo and contacts.
- BH-3: I often share my financial routine such as purchases, payments and cash inflow.

APPENDIX B – R Scripts

```
### library

library(psych)

library(lavaan)

library(mirt)

library(readxl)

library(semPlot)

### read the db

survey = read_excel("/Users/Shared/Data Privacy Survey.xlsx")

### Exploring

scree(survey)

fa(survey, cor='poly')

fa.parallel(survey, cor='poly')

fa.diagram(fa(survey, cor='poly'), cut=.2)

## factors (EFA)

fa(survey, 4, n.obs=376)

########## result: 5 factors

### SEM

sum(is.na(survey[1:22]))

modelo_ceri <- 'Result =~ CON1 + CON2 + CON3 + AWA1 + AWA2 + AWA3 + COL1

+ COL2 + COL3 + COL4 + RE1 + RE2 + RE3 + NF1 + NF2 + NF3 + DF1 + DF2 + DF3

+ BH1 + BH2 + BH3'

ceri_fit <- lavaan(modelo_ceri,

                   data=survey,

                   auto.var=TRUE,
```

```
auto.fix.first=TRUE,

auto.cov.lv.x=TRUE, estimator = "ML")
```