FEEL FREE TO USE MY PERSONAL DATA: AN EXPERIMENT ON DISCLOSURE BEHAVIOR WHEN SHOPPING ONLINE

José Luis GÓMEZ-BARROSO

Dpto. Economía Aplicada e Historia Económica

UNED (Universidad Nacional de Educación a Distancia)

Pº Senda del Rey, 11. 28040 Madrid (Spain)

jlgomez@cee.uned.es

FEEL FREE TO USE MY PERSONAL DATA: AN EXPERIMENT ON DISCLOSURE BEHAVIOR WHEN SHOPPING ONLINE

Structured abstract

Purpose: The goal of the article is twofold: to determine the effectiveness of monetary incentives for disclosing personal information, and to confirm the existence of a *bite the bullet* effect whereby people more easily accept providing personal data if they become aware of the requirement when the purchasing decision is almost taken.

Design/methodology/approach: An experiment in which participants made a real purchase on the AliExpress marketplace was carried out. They were asked to login either via the Facebook button or by creating a username and password. A different reimbursement of the price paid for their purchase was offered in each case. This information was presented either at the beginning of the purchasing process or just before completing the purchase order.

Findings: The monetary incentive proved to work well. The *bite the bullet* effect could not be assessed because many participants willingly gave their data to the company even if they had decided not to buy anything.

Social implications: While people continue to publicly declare that they have privacy concerns, their behavior could not be further removed from such concerns.

Practical implications: From a managerial perspective, this is good news. This is a calamity from a policy perspective. More experiments carried out in real settings are needed as a first step for reconsidering public action.

Originality/value: Experiment in a completely real setting, in which participants made a purchase using their own credit card.

Keywords: privacy, personal data, disclosure behavior, experiment, heuristics, e-commerce

1. INTRODUCTION

Understanding how people behave when faced with situations that involve disclosing their personal data has become a topic of utmost importance in our online-mediated societies and economies. Its significance is more than evident if we consider the number of services and applications that have become essential to most people's lives that are currently or potentially subject to personalization. Therefore, it goes without saying that personal information has high economic value. In the retail world, the personal data of existing and potential customers are an

increasingly essential part of day-to-day business practices and, consequently, have become an invaluable asset for any business.

Because online personal information disclosure behavior is context-, culture- and time-dependent, no single theory will be able to explain the vast diversity of situations and behaviors. Moreover, people do not always behave consistently. All this gives rise to the need for experimental research in this area. Yet, however strange it may sound, experiments represent only a minor part of the research efforts addressing online disclosure behavior. On top of that, their applicability is often limited, given that designs are frequently out of touch with what actually happens in the real world.

This work has tried to overcome this problem by carrying out an experiment in a *completely real* setting, in which participants made a purchase using their own credit card on the AliExpress marketplace. First and foremost, the aim of the experiment was to contribute to the field of knowledge, i.e., to experimentally advance the understanding of how people behave when their personal data is requested. More specifically, the objective was twofold: first, to explore whether a monetary incentive, a price discount, affects people's behavior; second, to assess the existence or absence of what we refer to as the *bite the bullet* effect that prevents shoppers from changing their mind about a purchase when conditions are altered, for instance when an unexpected request for personal information is made at a late stage in an online process (of purchase, of downloading a file, of playing a game, etc.). The monetary incentive proved to work well, so well in fact, that the second objective could not be assessed. Nonetheless, the results obtained were equally interesting: people are willing to disclose data in situations where it is not required, or even rational, to do so.

The article is structured as follows. The following section outlines and discusses the use of experiments on personal information disclosure, paying particular attention to those that have dealt with issues similar to the ones focused on by this article: the effectiveness of monetary incentives and context-sensitive heuristics. The third section presents the hypotheses tested by the experiment. The fourth describes the experimental design. Results are shown in the fifth section and discussed in the sixth. The article closes with some concluding remarks and lessons for managers and policy makers.

2. EXPERIMENTS ON PERSONAL INFORMATION DISCLOSURE: MONETARY INCENTIVES AND CONTEXT-SENSITIVE HEURISTICS

Already some way into the 21st century, online personal information disclosure became a distinct field of research, separate from traditional privacy issues (see Gómez-Barroso, 2018a). It is only logical that the interest in the topic has continued to increase: personal data has become a key asset for the development of digital markets, given the ease and speed with which data can now be gathered and used.

The way in which people perceive and manage their privacy today totally contrasts with the situation even just a few years ago. As stated in the introduction, this behavior is not homogeneous, but rather guided by a complex set of factors, different for each individual and with different effects in each situation, and also mediated by heuristics and cognitive biases (see, for instance, Acquisti, Brandimarte and Loewenstein, 2015). This suggests that experimental research is the most appropriate way to draw conclusions. In addition, a second argument plays in favor of the suitability of experiments: what individuals say they would do does not match what they actually do. This "privacy paradox" was already highlighted in pioneering works in this field and has since dominated much of the research agenda (see literature reviews in Kokolakis, 2017 or Barth and de Jong, 2017).

Despite all of the above, most past and present efforts in the field of personal information disclosure continue to attempt to build a single comprehensive model able to explain as many of the motivations and concerns that guide the behavior of people as possible, and are all too often based on questionnaires. In other words, the use of experimental methods in this area is relatively infrequent. When an experimental approach is used, its goal is often to verify or refute the links between concerns, attitudes, behavior, or any of the variables present in the comprehensive models. Gómez-Barroso (2018b) presented a bibliographical review of contributions based on experimental work. The review includes all kinds of experiments as the author reveals that the very concept of experiment is not narrowly defined: "in a significant part of the experiments (...) participants, while immersed in an experimental setting, are finally asked about their feelings or intentions; other works ask individuals to make hypothetical choices". Going through the description of the papers, it can be seen that deception was usually employed and economic incentives were in place in only a few cases, i.e., the number of "economic experiments" is really low.

A subset of the whole corpus of experiments about online disclosure of personal data (either "economic" or not) deals with incentives to disclose. These incentives are either monetary compensation (see below) or a better, more personalized, service (Ward, Bridges and Chitty, 2005; Li and Unger, 2012; Mothersbaugh et al., 2012; Sutanto et al., 2013; Kobsa, Cho,

and Knijnenburg, 2016; Song et al., 2016). Either way, *rational* data holders are expected to make a decision through a "privacy calculus", in which they weigh the benefits and risks associated with how the disclosed data will be used (see, among others, Keith et al., 2013; Wang, Duong and Chen, 2016; Zhu et al., 2017; Gómez-Barroso, Feijóo and Martínez-Martínez, 2018).

Focusing on monetary incentives, their effectiveness is under scrutiny. A number of papers conclude that rewards or monetary incentives are not effective (Andrade, Kaltcheva and Weitz, 2002; Ward, Bridges and Chitty, 2005; Taylor, Davis and Jillapalli, 2009; Lee et al., 2015); moreover, the older and newer of those papers found that monetary rewards actually increase privacy concerns when sensitive information is required. On the contrary, other articles found that offering price discounts, vouchers or sums of money encourage data disclosure (Xie, Teo and Wan, 2006; Hui, Teo and Lee, 2007; Premazzi et al., 2010; Steinfeld, 2015; Feri, Giannetti and Jentzsch, 2016; Babula, Mrzygłód and Poszewiecki, 2017). A third group of papers tried to put a price on particular pieces of personal information; although their conclusions are not so clear-cut, they are cited because people are supposed to reveal that data when offered the amount data is valued at (Huberman, Adar and Fine, 2005; Cvrcek et al., 2006; Carrascal et al., 2011; Acquisti and Grossklags, 2012; Hirschprung et al., 2016).

Virtually all these experiments are conducted in fictitious settings. Often fake websites are built and participants are told that their data, if disclosed, will be given to some unknown company or body. They either employ survey-like methodologies in which participants make hypothetical choices, and/or use deception. Steinfeld (2015) is probably the only paper that can claim to have been performed in a real but very particular setting (the virtual world Second Life).

Strictly speaking, only one paper conducted experiments that try to identify heuristics related to the exact circumstances in which personal data is requested: Acquisti and Grossklags (2012) investigated framing effects replacing a marketer's offer to pay for personal data outright with an offer to discount the price of some product in exchange for the data; they obtained varied results. Taking the "exact circumstances in which personal data is requested" in broader terms, articles analyzing availability effects, in which behavior is influenced by recent information, could also be cited. So far, this is the most studied heuristic; five works fall into this category (Sundar et al., 2013; Baek, 2014, Nofer et al., 2014; Feri, Giannetti and Jentzsch, 2016; Babula, Mrzygłód and Poszewiecki, 2017).

3. HYPOTHESES

Our proposition that the exact juncture at which personal data is requested influences people's response (and consequently disclosure) emerged from anecdotal experience and hearsay (to the best of the authors' knowledge, it has not been formally demonstrated). For instance, it is not the same to ask users to provide their data as a first step in order to give them access to a webpage or media content than to do it later in the process. Indeed, there is a crude, but frequently-used, strategy for gathering data that consists in requiring registration, i.e. personal information, just before allowing users to download a specific (apparently free of charge) content.

In such situations, a manifestation of what can be referred to as the *bite the bullet* effect could influence individual decision making. This effect is a bias towards taking on unexpected costs which would otherwise jeopardize an almost made decision. An inflated charge for credit card use can come as an unpleasant surprise for those buying a plane ticket online but many would go ahead, albeit angrily, with the purchase even if the charge makes the ticket more expensive than the prices found previously on other platforms. A couple may decide to eat dinner really late after being informed, when arriving to the restaurant they had chosen from home, that no table will be available for the next two hours, even though other similar restaurants nearby have tables and that same restaurant offers them a reservation for any of the following days. The *bite the bullet* effect may be caused by a combination of other biases such as: the sunk cost fallacy (time or effort already spent may be high), confirmation bias (disconfirming information tends to be ignored or discounted), endowment effect (giving up an object we feel we own it, before actually having it, is considered a loss), visceral factors (a bit of excitement may sometimes be present), or lock-in effect (to get familiar with another store, procedure or environment entails transaction costs).

Whether such an effect is important when making personal data disclosure decisions – and, consequently, whether personal data collectors take advantage of it– is the second of our research questions. The first is to clarify whether monetary rewards are a useful instrument to gather personal information. As seen in the previous section, there is no straightforward answer to this issue.

To answer these questions, an experiment in which the exact reward for disclosure of personal data is announced either at the beginning or at a late stage of the shopping process was carried out. Our assumption is that initially, when no decision has been taken, the privacy calculus for deciding whether to disclose information or not is made unrestrictedly; however, if the request is made later on, when a determination to buy exists, the *bite the bullet* effect can "ease" the disclosure of data. It is from here that the two research hypotheses arise:

H1: When considering a purchase, monetary incentives in exchange for personal information are not completely effective.

H2: People are prone to disclose personal data –even when not strictly necessary for the transaction data– if it is required late in the shopping experience, just prior to completing the purchase.

4. EXPERIMENTAL DESIGN

When designing the experiment, the first condition was for participants to make a real purchase. Asking them to buy (or not) a specific product as other experiments have done in the past, can lead to results determined by the different utility than participants extract from those products. Moreover, the webpage in which the interaction happens was frequently built for the experiment, which creates an artificial environment. To overcome these problems, participants were given access to a real marketplace. A marketplace encourages transactions (participants can buy whatever they want) and the transactions made are entirely real (money and data go to the company).

Three marketplaces were candidates: Amazon, El Corte Inglés and AliExpress. At the time the experiment was conceived (spring of 2017), Amazon was already too popular and trusted; there was a serious risk that most participants had already given the company their data in previous transactions. El Corte Inglés is the premier Spanish department store; its online business lagged well behind Amazon but it has a solid reputation –most Spaniards trust it and would feel confident when giving their data to it. Therefore AliExpress seemed to be the best option. At that time, it was not as well known as Amazon and, being based in China, it still had to overcome the stereotypes of low-quality and lack of trust regarding data security.

As usually happens with e-commerce stores, AliExpress offers registration either with a username (e-mail address) and password, or by clicking on a social media button. When the experiment was conducted, just three buttons were available in the Spanish version of the AliExpress website: Facebook, VK (Vkontakte) and Google. VK (a Russian social network) was completely unknown to Spanish users and the Google button gave some problems in previous tests. Therefore, Facebook remained as the only (but very adequate for the experiment) option. By registering through a social media button, users give the e-commerce store access to their profile while simultaneously giving information to the social site about their shopping patterns. While people may not be fully aware of the exact dangers this action entails for their privacy, at least they understand what they are doing, as an informal test in the classroom made before the experiment demonstrated (not recorded small-group discussions about privacy

behavior when shopping online –virtually all students where aware of the fact that the online shop could access their profile when clicking on a social media button).

As is also normal, it is not necessary to login to navigate the AliExpress webpage, but you must do so to complete a purchase. However, it was thought that requiring one of the groups to log in from the beginning, before starting the purchasing process, would make it possible to compare behaviors and identify the *bite the bullet* effect. Finally, the reward offered was intended to be as simple as possible: a reimbursement of a percentage of the price, which varied depending on the method used to sign in. This was seen as a neutral and effective approach.

All of these conditions and constraints were used to construct the experiment as follows:

- A first group of participants (control group) was given all the instructions as soon as they were seated in the room. Their task was to make a real purchase on http://es.aliexpress.com. As a first step, they were told to log in either with the Facebook button or with username and laboratory assistants would take note of their choice. In the first case, a reimbursement of 75% of the price was offered with a limit of 15 euros; in the second case, the reimbursement was 50% with a limit of 10 euros. That means that purchases over 20 euros had a cap on the reimbursement offered. Participants were also informed that purchasing was not compulsory, the compensation just for attending was 5 euros. Participants were given 15 minutes to look for a product and 5 more minutes to complete the purchase.
- A second group of participants (treatment group) was only given the first of two sets of instructions when were seated in the room. Their task was again to make a real purchase on http://es.aliexpress.com. They were informed that a reimbursement of 75% of the price was offered with a limit of 15 euros and that further instructions on how to complete the purchase would be given after 15 minutes, the time allowed to select a product. Yet again, participants were informed that purchasing was not compulsory and promised 5 euros simply for attending. When the 15 minutes were up, the second set of instructions informed participants that logging in with the Facebook button was required to obtain the 75% reimbursement; otherwise, they could log in with a username and password and receive a 50% reimbursement (limit 10 euros). An additional five minutes were allowed to complete the order and for laboratory assistants to take note of the log in procedure chosen by each participant.

5. RESULTS

The experiment was conducted at the Lineex laboratory of the Universidad of Valencia (Spain) in December 2017. Two consecutive sessions were carried out with 48 participants each. There were no restrictions to participation, but two conditions were placed on those who wanted to participate: having an active Facebook account, and having a credit card on hand and being prepared to use it to make a real purchase. The demographics are described in Table 1:

Table 1. Demographics (all participants)

	Sex		Age		
	Men	Women	18-24	25-34	>34
Group 1	24	24	37	10	1
Group 2	31	17	37	7	4

Only absolutely necessary data was collected; i.e., whether they logged in or not (and the login option chosen in the former case), and the amount of the purchase. There were some problems with the website, but all were resolved except for one case in which the participant wanted to make a purchase, but the shopping cart did not respond; this participant is considered as a buyer. Table 2 presents the decisions made during the experiment.

Table 2. Results (all participants)

Group 1			Group 2		
	Purchase	No purchase		Purchase	No purchase
Facebook login	33	10	Facebook login	34	12
Username login	1	4	Username login	0	1
			Not logged in	0	1

Average payment was €9.96 for Group 1 and €10.48 for Group 2. Incidentally, the items purchased belonged to the following categories (Group 1+Group 2): Clothing 14+11; Computer and Consumer Electronics 9+8; Cellphones & Accessories 5+2; Home 1+3; Sports and Outdoors 2+1; Leisure 0+1; Other 2+8. This information is taken from the questionnaire that participants completed before leaving the laboratory.

The questionnaire included questions about online activity, online skills, Facebook activity and previous experience with AliExpress. One of the questions asked about previous purchases made on the AliExpress platform. Using this answer, Table 2 is split into Table 3 and Table 4.

Table 3. Results (participants who had previously purchased through AliExpress)

Group 1			Group 2		
	Purchase	No purchase		Purchase	No purchase
Facebook login	22	2	Facebook login	25	6
Username login	1	4	Username login	0	1
			No logged in	0	0

Table 4. Results (participants without previous experience shopping on AliExpress)

Group 1			Group 2		
	Purchase	No purchase		Purchase	No purchase
Facebook login	11	8	Facebook login	9	6
Username login	0	0	Username login	0	0
			Not logged in	0	1

5.1. Group 1 (control group)

To confirm the stated H1 and H2 hypotheses, two results ("sub-hypotheses") were expected to be reached within the control group:

- First (hc1), only a subset of participants were expected to be willing to log in by clicking on the Facebook button: those who were less concerned about privacy, and/or those who were confident that websites process personal information properly, and/or those who valued their data at less than the 5 euros which was the maximum reward (15 and 10 euros were respectively the upper thresholds when logging in using either Facebook or username and password).
- Secondly (hc2), participants who logged in with Facebook were expected to be more active purchasers.

The first assumption was not confirmed. The vast majority, 43 out of 48 participants, logged in with Facebook (see Table 2). The group includes all the participants (19) who had not previously purchased through AliExpress (see Table 4). Using the information collected in the questionnaire, a number of logistic regression analyses were conducted in an effort to find a model that explains the profile of the *Facebook group*. The "main effects" of all the variables and also all the possible interactions of the variables taken in pairs were considered in each attempt. The model whose fit presented better accuracy considering the logarithm of the likelihood and the pseudo-R2 statistic (Nagelkerke R^2=0.937; p=0.004) includes internet

addiction, trust in Facebook's proper handling of data, previous experience with AliExpress, and real knowledge about managing personal data, but none of the variables were significant in the model.

The second sub-hypothesis was fairly well supported: 33 out of 43 *Facebook profile-users* made a purchase, compared to just 1 out of 5 from the username category (see Table 2) (p=0.007 for t-test across averages of the two categories). Nevertheless, it should be pointed out that the percentage of non-purchasers is much higher among participants who had never used the platform before (see Table 3 and Table 4): 8 out of 10 people who did not purchase (i.e., gave access to their Facebook profile without receiving any benefit) had never used the platform.

5.2. Group 2 (treatment group)

As in the case of the control group, two sub-hypotheses were expected to be met:

- First (ht1), participants who were supposed to be willing to log in with the Facebook button have the same profile as in experiment 1, but the group should increase to include those who are reluctant to renounce the purchase they had already decided to make (willing to *bite the bullet*).
- Secondly (ht2), considering that the time to look for products had already run out, logging in should correspond with a firm intention to purchase; i.e., everyone who logged in (either with Facebook or with username/password) should have purchased something, as there is no reason to log in if you have decided not to purchase anything.

With regard to the first point, as expected, almost everyone logged in with Facebook: 46 of 48 participants. Just two people behaved differently: one participant logged in using username and password and another did not log in at all. However, as the number of people from the control group logging in was already so high (hc1 was not supported), there is no room to assess the existence of a *bite the bullet* effect. Therefore, ht1 cannot be supported or rejected.

Very interestingly, ht2 is completely invalidated. In principle, only 34 (login+purchase) + 1 (no login+no purchase) participants acted rationally. Inspecting the results more closely, 4 participants made purchases whose reimbursement was less than 5 euros, i.e., they received the same 5 euros that they would have received for doing nothing (remember that 5 euros is the amount gained just for participating in the experiment); one more participant received 5.11 euros. In conclusion, 30 participants made rational decisions, while 18 did not; of those, 17 participants (35.5%) gave access to their Facebook profile receiving nothing in return; of those,

7 participants had no previous experience with AliExpress, which excludes the option of having given access to their Facebook account in the past (and remembering this fact).

6. DISCUSSION

Online markets move fast. The case of AliExpress is a good example of how just six months can dramatically change market trends and consumer preferences. Though it emerged in the Spanish market earlier, Alibaba did not open an office in Spain until February 2017. There are no official figures, but a consultancy firm (Netrica) reported that AliExpress was rapidly gaining market share after its arrival to the Spanish market.[1] Initially, most users landed in AliExpress via search engines but, little by little, it started to be considered a gateway to online shopping.

This fact had an impact on the outcome of the experiment. When the experiment started to take shape (remember the date: spring of 2017), informal surveys in the classroom confirmed that AliExpress was not well known. When the experiment took place at the end of the year (on top of the time spent in preparing it, some delay was added by a coincidental overdemand of the laboratory facilities), results indicated a relatively well-known company, with many participants having had a previous experience using the platform to purchase goods. The scenario required to assess the *bite the bullet* effect was, therefore, somewhat compromised, as prior knowledge could promote trust, although trust is perfectly compatible with privacy-safe behaviors, such as signing in with username and password. That said, 35 of 96 participants had never purchased through AliExpress, and another 14 had purchased only once, which was an acceptable number to draw conclusions about the *bite the bullet* effect.

Having said this, the results do not reflect the expectations. They show that many participants were happy to click on the Facebook button. Only 7 of 96 participants did not click on it. On many occasions, their behavior was clearly not rational. In the cases in which the behavior can be considered rational, giving access to their Facebook profiles was rewarded with ridiculously low amounts of money, considering the wealth of sensitive and commercially interesting information given to the company.

---

[1] *Amazon vs Aliexpress: la batalla por la corona del ecommerce en España*. https://www.netrica.com/2017/07/13/amazon-aliexpress/

7. CONCLUSIONS: MANAGERIAL AND POLICY IMPLICATIONS

Resignation? (*It doesn't matter what I choose or do, my data is already out there*). Laziness? (*I'm sick of passwords and all that stuff)*. Lack of concern? (*I really don't care about that data mess*). Ignorance? (*In the end, it's just my profile, there's nothing to hide, nothing that can be taken advantage of*).

There is a little bit of everything, but most probably the main ingredient in the cocktail is a lack of concern. Those who are really concerned about privacy overcome barriers (trying) to defend it. The second ingredient is laziness: just one click allows users to skip filling out the same boxes already tediously filled out many times before.

From a managerial perspective, this is good news. Personal information is a key intangible asset for companies and so they employ convoluted strategies for gathering data. It seems, however, that there is no need to put pressure on customers to obtain their data: it is enough not to bother them with too many forms and questions. In this sense, the sign-in button is a great invention, particularly for those companies that have the tools and resources to extract high value from mining social sites. Ultimately, the privacy paradox continues to be a main feature in personal data disclosure behavior. The *The digital society in Spain* report, which is always a valuable national data source, gives some noteworthy figures in its 2018 edition, referring to 2017:[2] 83.7% of the population showed privacy concerns (rated ≥7 on a scale of 1to10), and only 17.3% of respondents declared that they were willing to disclose data in exchange for relevant information, even fewer (12%) when data were exchanged for customized offerings. Moreover, no significant differences by age were reported and those figures had risen from previous years. In conclusion, while people continue to publicly declare that they have privacy concerns, their behavior could not be further removed from such concerns.

This is a calamity from a policy perspective. Regulations are based on the assumption that everyone is concerned with privacy, to a greater or lesser degree depending on the individual, but still a concern for all. It is of course very hard to protect people who do not value being protected, or who at least are not pulling their weight in terms of protecting themselves. Since the privacy paradox seems to be a fact, questionnaires may not be of any help to design policies. Instead, more experiments carried out in real settings are probably needed as a first step for reconsidering public action. This kind of analyses would be the basis for putting in place mindful and geared-to-the-environment policies such as educating the public, thereby departing from strictly legal considerations based on societal perceptions no longer existing. In practical terms, what society as a whole needs is a reflection on how better to reconcile the

[2] https://www.fundaciontelefonica.com/arte_cultura/sociedad-de-la-informacion/sdie-2017/

commodification of personal data with socially positive innovations. For that, imposing yesterday's solutions on tomorrow's problems is of little help.

8. REFERENCES

Acquisti, A., Brandimarte, L. and Loewenstein, G. (2015), "Privacy and human behavior in the age of information", *Science*, Vol. 347 No. 6221, pp. 509-514.

Acquisti, A. and Grossklags, J. (2012), "An online survey experiment on ambiguity and privacy", *Communications & Strategies*, Vol. 88, pp. 19-39.

Andrade, E.B., Kaltcheva, V. and Weitz, B. (2002), "Self-disclosure on the Web: The impact of privacy policy, reward, and company reputation", *Advances in Consumer Research*, Vol. 29 No. 1, pp. 350-353.

Babula, E., Mrzygłód, U. and Poszewiecki, A. (2017), "Consumers' need of privacy protection – Experimental results", *Economics & Sociology*, Vol. 10 No. 2, pp. 74-86.

Baek, Y.M. (2014), "Solving the privacy paradox: A counter-argument experimental approach", *Computers in Human Behavior*, Vol. 38, pp. 33-42.

Barth, S. and 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*, Vol. 34 No. 7, pp. 1038-1058.

Carrascal, J., Riederer, C., Erramilli, V., Cherubini, M. and de Oliveira. R. (2011), "Your browsing behavior for a Big Mac: economics of personal information online", in *Proceedings of the 22nd international conference on World Wide Web*, ACM, New York, pp. 189-200.

Cvrcek, D., Kumpost, M., Matyas, V. and Danezis, G. (2006), "A study on the value of location privacy", in *Proceedings of the Fifth ACM Workshop on Privacy in Electronic Society – WPES '06*,ACM, NewYork, pp. 109-118.

Feri, F., Giannetti, C. and Jentzsch, N. (2016), "Disclosure of personal information under risk of privacy shocks", *Journal of Economic Behavior & Organization*, Vol. 123, pp. 138-148.

Gómez-Barroso, J.L. (2018a), "Uso y valor de la información personal: Un escenario en evolución", *El Profesional de la Información*, Vol. 27 No. 1, pp. 5-18.

Gómez-Barroso, J.L. (2018b), "Experiments on personal information disclosure: past and future avenues", *Telematics and Informatics*, Vol. 35 No. 5, pp. 1473-1490.

Gómez-Barroso, J.L., Feijóo, C. and Martínez-Martínez, I.J. (2018), "Privacy calculus: Factors that influence the perception of benefit", *El Profesional de la Información*, Vol. 27 No. 2, pp. 336-343.

Hirschprung, R., Toch, E., Bolton, F. and Maimon, O. (2016), "A methodology for estimating the value of privacy in information disclosure systems", *Computers in Human Behavior*, Vol. 61, pp. 443-453.

Huberman, B.A., Adar, E. and Fine, L.R. (2005), "Valuating privacy", *IEEE Security & Privacy*, Vol. 3 No. 5, pp. 22-25.

Hui, K.L., Teo, H.H. and Lee, S.Y.T. (2007), "The value of privacy assurance: an exploratory field experiment", *MIS Quarterly*, Vol. 31 No. 1, pp. 19-33.

Keith, M.J., Thompson, S., Hale, J., Lowry, P.B. and Greer, C. (2013), "Information disclosure on mobile devices: re-examining privacy calculus with actual user behavior", *International Journal of Human-Computer Studies*, Vol. 71 No. 12, pp. 1163-1173.

Kobsa, A., Cho, H. and Knijnenburg, B.P. (2016). "The effect of personalization provider characteristics on privacy attitudes and behaviors: An elaboration likelihood model approach". *Journal of the Association for Information Science and Technology*, Vol. 67 No. 11, pp. 2587-2606.

Kokolakis, S. (2017), "Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon", *Computers, & Security*, Vol. 64, pp. 122-134.

Lee, H., Lim, D., Kim, H., Zo, H. and Ciganek, A.P. (2015), "Compensation paradox: the influence of monetary rewards on user behaviour", *Behaviour & Information Technology*, Vol. 34 No. 1, pp. 45-56.

Li, T. and Unger, T. (2012). "Willing to pay for quality personalization? Trade-off between quality and privacy". *European Journal of Information Systems*, Vol. 21 No. 6, pp. 621-642.

Mothersbaugh, D.L., Foxx, W.K., Beatty, S.E. and Wang, S. (2012). "Disclosure antecedents in an online service context: The role of sensitivity of information". *Journal of Service Research*, Vol. 15 No. 1, pp. 76-98.

Nofer, M., Hinz, O., Muntermann, J. and Roßnagel, H. (2014), "The economic impact of privacy violations and security breaches: A laboratory experiment", *Business, & Information Systems Engineering*, Vol. 6 No. 6, pp. 339-348.

Premazzi, K., Castaldo, S., Grosso, M., Raman, P., Brudvig, S. and Hofacker, C.F. (2010), "Customer information sharing with e-vendors: The roles of incentives and trust", *International Journal of Electronic Commerce*, Vol. 14 No. 3, pp. 63-91.

Song, J.H., Kim, H.Y., Kim, S., Lee, S.W. and Lee, J. (2016). "Effects of personalized e-mail messages on privacy risk: Moderating roles of control and intimacy". *Marketing Letters*, Vol. 27 No. 1, pp. 89-101.

Steinfeld, N. (2015), "Trading with privacy: the price of personal information", *Online Information Review*, Vol. 39 No. 7, pp. 923-938.

Sundar, S., Kang, H., Wu, M., Go, E. and Zhang, B. (2013), "Unlocking the privacy paradox: Do cognitive heuristics hold the key? ", in *CHI '13 Extended Abstracts on Human Factors in Computing Systems*, ACM, New York, pp. 811-816.

Sutanto, J., Palme, E., Tan, C. and Phang, C. (2013). "Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users". *MIS Quarterly*, Vol. 37 No. 4, pp. 1141-1164.

Taylor, D.G., Davis, D.F. and Jillapalli, R. (2009), "Privacy concern and online personalization: The moderating effects of information control and compensation", *Electronic Commerce Research*, Vol. 9 No. 3, pp. 203-223.

Wang, T., Duong, T.D. and Chen, C.C. (2016), "Intention to disclose personal information via mobile applications: A privacy calculus perspective", *International Journal of Information Management*, Vol. 36 No. 4, pp. 531-542.

Ward, S., Bridges, K. and Chitty, B. (2005), "Do incentives matter? An examination of on-line privacy concerns and willingness to provide personal and financial information", *Journal of Marketing Communications*, Vol. 11 No. 1, pp. 21-40.

Xie, E., Teo, H. and Wan, W. (2006), "Volunteering personal information on the Internet: Effects of reputation, privacy notices, and rewards on online consumer behaviour", *Marketing Letters*, Vol. 17 No. 1, pp. 61-74.

Zhu, H., Ou, C.X.J., van den Heuvel, W.J.A.M. and Liu, H. (2017), "Privacy calculus and its utility for personalization services in e-commerce: An analysis of consumer decision-making", *Information & Management*, Vol. 54 No. 4, pp. 427-437.