Privacy paradox in the mobile environment: The influence of the emotions

Francisco-José Sarabia-Sánchez; Juan-Miguel Aguado; Inmaculada J. Martínez-Martínez

Nota: Este artículo se puede leer en español en:
http://www.elprofesionaldelainformacion.com/contenidos/2019/mar/13_es.pdf

How to cite this article:

Sarabia-Sánchez, Francisco-José; **Aguado, Juan-Miguel**; **Martínez-Martínez, Inmaculada J.** (2019). "Privacy paradox in the mobile environment: The influence of the emotions". *El profesional de la información*, v. 28, n. 2, e280212.

https://doi.org/10.3145/epi.2019.mar.12

Article received on January 1, 2019
Approved on February 18, 2019

Francisco-José Sarabia-Sánchez
https://orcid.org/0000-0002-0370-2839

Universidad Miguel Hernández
Departamento de Estudios Económicos y Financieros
Avda. Universidad, s/n. 03202 Elche (Alicante), Spain
fransarabia@umh.es ✉

Juan-Miguel Aguado
https://orcid.org/0000-0002-8922-3299

Universidad de Murcia
Facultad de Comunicación y Documentación
Campus de Espinardo, s/n. 30100 Murcia, Spain
jmaguado@um.es

Inmaculada J. Martínez-Martínez
https://orcid.org/0000-0003-3807-1325

Universidad de Murcia
Facultad de Comunicación y Documentación
Campus de Espinardo, s/n. 30100 Murcia, Spain
inmartin@um.es

Abstract

The increasing relevance of personal information has sparked a broad debate on privacy issues on the ubiquitous Internet. The so called 'privacy paradox' aims to explain through rational decision-making models the contradictions between stated digital privacy concerns and the actual behaviors in mobile platforms. An analysis of the emotions that arise when users know about unauthorized personal data disclosure is proposed. A survey of smartphone users was conducted shortly after the *Cambridge Analytica* / *Facebook* scandal took place, in order to analyze the nature and intensity of a user's emotions in relation to their knowledge of privacy breaches. The results support the paradox of privacy from an emotional perspective: although the reported emotions are intense, there is no relationship between the management that users make of their privacy settings in social networks and mobile applications and the nature and intensity of the emotions reported.

Keywords

Social networks; Mobile applications; Smartphones; Personal information; Personal data; Data; Privacy; Emotions.

Funding information

The research results presented in this paper are part of the research project *MOB AD: Impact of mobile technologies in strategic and commercial communication* funded by the *Regional Agency for Science and Technology – Seneca Foundation*, *Government of Murcia*, Spain (19451/PI/14).

1. Introduction: mobile environment, ubiquitous social networks, and data economy

The vertiginous development of mobile communications has facilitated the enthronement of personal data as a central economic resource in the current context of the omnipresence of the Internet and digital services (**Gómez-Barroso**; **Feijóo**, 2013; **Aguado**; **Martínez-Martínez**, 2014). Mobile devices have extended into the far reaches of our daily lives and turned even mundane interactions into data points and metadata (**Scoble**; **Israel**, 2014), by facilitating the transfer of everyday social environments to the grid of interactions mediated by technology that constitutes the ubiquitous social networks (**Su**; **Xu**; **Qi**, **2**016).

The current data economy (**West**, 2019) is based on mobile devices, as both a technology of relationship -based on social interactions (**Ling**, 2008)- and a technology of data collection –by the colonization[1] of time and online attention (**Scoble**; **Israel**, 2014)-. The use of mobile applications has led to an increase of the importance of social networks. These, in addition to being affective networks (**Doyle**, 2015), also operate as coding systems for emotional reactions, transforming moods into processable data. In this sense, **Gerlitz** and **Helmond** (2013) contrast the old "economy of *link*" (the advertising value was based on the click) with the current "economy of *like*", where the user's involvement is decisive.

The importance of private information, the omnipresence of social networking platforms (like *Facebook*, *WhatsApp*, and *Instagram*), and the lack of transparency have sparked a multidisciplinary debate on privacy in the context of mobile communications and the ubiquitous internet (**Smith** *et al.*, 2012; **Spiekermann** *et al.*, 2015). This debate is influenced by an increasing awareness of:

- its risks (**Acquisti**; **Brandimarte**; **Loewenstein**, 2015);
- how to protect the data (**Martínez-Martínez**, 2018);
- the implications of giving up data or of informational behavior in the use of mobile services (**Lutz**; **Strathoff**, 2014).

In 2017, the sale of the personal data of more than eighty million users by *Facebook* to *Cambridge Analytica* revived concerns about the risks associated with the dissemination of personal information on mobile social networks. This crisis was one additional step in a series of security failures and compromised practices that did not seem to have much effect on *Facebook*'s usage figures and its applications (**Kanter**, 2018). This shows the validity of the so-called "paradox of privacy" (**Kehr**; **Wentzel**; **Kowatsch**, 2014), which is the contradiction between the concern expressed about online privacy and the actual behavior on mobile platforms.

Investigations into this paradox have focused on rational decision models and the impact of the incentive on the user's calculated decision to transfer personal data (**Kokolakis**, 2017). However, this work proposes an approach that is based on the analysis of the emotions that appear when users become aware of the unauthorized dissemination of their private data. In the following sections, the predominance of rational choice models is observed in the investigations about the association between attitudes and behaviors on digital privacy. Next, the results of a survey about the emotions associated with the mentioned dissemination of personal data are presented and discussed.

2. Paradox of privacy: beyond the cognitive-rational explanation

Since the mid-2000s there has been a proliferation of bibliography about the level of concern of users in relation to the guarantees and consequences of the voluntary transfer of personal data and the incidence of such cession in their informational behavior (**Kokolakis**, 2017). A good portion of this bibliography confirms that, although privacy is a primary concern of users in any activity in an omnipresent Internet, there is no consistent behavior regarding the transfer of data, often occurring in exchange for minimum rewards or simply by saving time or inconveniences (**Kehr**; **Wentzel**; **Kovatsch**, 2014).

This contradiction between the expressed concern and the relative informational behavior is called the "paradox of privacy" (**Acquisti**; **Brandimarte**; **Loewenstein**, 2015). In general, the term refers to the apparent inconsistency between attitudes and behavior on privacy, and may also include the discrepancy between intention and behavior (**Kokolakis**, 2017).

Traditionally, the explanation of the paradox of privacy has been approached from cognitive-rational approaches centered on individual decisions (**Kokolakis**, 2017). There are also proposals that argue that the paradox is caused by the existence of biases in decision making (incomplete information, psychological biases, contextual factors, etc.) that could overcome the presumptions of the cognitive-rational model, although without invalidating it (**Acquisti**; **Brandimarte**; **Lowenstein**, 2015). Other hypotheses such as the preeminence of immediate gratification (**Wang**; **Duon**; **Chen**, 2016), psychological compensation for future rewards, the current effort to provide information (**Krol**, 2016), or the generic recognition of the impossibility of evading the invasion of privacy (**Kokolakis**, 2017) also belong to the set of arguments of the rational approach to the paradox of privacy.

There are studies that question the validity of this paradox, considering the increasing transparency and visibility of the measures for guaranteeing privacy (**Kokolakis**, 2017), or the existence of behaviors to control personal

> "The paradox of privacy is that users value privacy to a high degree, but will give it up in exchange for small rewards"

information outside the privacy dispositions of the system (**Miltgen**; **Peyrat-Guillard**, 2014). Likewise, **Dienlin** and **Trepte** (2015) point out that behaviors are not so paradoxical when analyzed in light of attitude, intention, and concern for privacy. However, both the works that question the paradox and those that support it, are proposed from perspectives based on the principle of rational choice.

> "The debate on privacy is marked by a progressive awareness of its risks, how to protect the data, and the implications of ceding privacy"

This principle and its derived models presuppose that users perform a cost-benefit transaction calculation as a basis to make decisions about the transfer of their personal data (**Acquisti**; **Grossklags**, 2005). This exercise of compensation between risks (costs) and profits (benefits) perceived on the transfer of personal information in the framework of the economy of data is known as the "privacy calculus " or calculated transfer of personal information (**Gómez-Barroso**; **Feijóo**; **Martínez-Martínez**, 2018).

Among the perceived risks are:

- lack of awareness or transparency about the actual uses of the data provided;
- absence of control over personal information once it is transferred.

Inappropriate uses or the transfer of data to unauthorized third parties are significant examples of invasion of privacy (**Min**; **Kim**, 2015). Among the perceived benefits there are a wide range of categories (**Gómez-Barroso**; **Feijóo**; **Martínez-Martínez**, 2018):

- emotional or relational (relevant in the context of social networks and mobile technologies);
- psychological factors (social prestige, novelty);
- factors of functional type, such as the improvement in quality of the service and the saving of time and increased comfort.

Other incentives considered in the bibliography include the monetary reward or the personalization of the service (**Wang**; **Duong**; **Chen**, 2016).

Many researches that apply this cognitive-rational model conclude that incentives, tangible or intangible, modify the decision depending on how much information the user is willing to give (**Gómez-Barroso**; **Feijóo**; **Martínez-Martínez**, 2018). From this rational-transactional perspective, the discrepancy between the concern for privacy and the behavior prone to yield data in exchange for rewards is seen as a paradox. However, several authors point out the need to take into account other factors when assessing the decision about how much and what information they are willing to give. For example, **Kehr**, **Wentzel** and **Kowatsch** (2014) point out that situational factors are decisive when choosing to transfer personal data. **Chen** (2018) points out the importance of social capital as a counterpart to the personal information that is transferred to social networks, and **Li** *et al.* (2017) point out the importance of the emotional component, not only in the favorable territory of mobile social networks such as affective networks (**Doyle**, 2015), but as a factor of complexity when reviewing the paradox of privacy.

In this sense, **Serrano-Puche** (2016) indicates the emergence of studies on an "affective investment" that users make on mobile devices as internet access points, identifying emotional factors in the acceptance and use of data services (**Ovčjak**; **Heričko**; **Polančič**, 2016). Considering these emotional factors may allow a more extensive explanation of the aspects related to the use of mobile services than that offered by strictly cognitive-rational models (**Kehr**; **Wentzel**; **Kowatsch**, 2014; **Lutz**; **Strathoff**, 2014; **Li** *et al.*, 2017).

Several authors have considered emotional factors to explain the paradox of privacy:

- **Hargittai** and **Marwick** (2016) point to apathy as a relevant emotion in the attitudes of young users, especially because, although they understand and care about the risks of giving information on the internet, they feel that they are losing control of their data, which it leads them to accept the situation but blame third parties for the mentioned loss;
- **Lutz** and **Strathoff** (2014) identify trust as an explanatory variable beyond mere cognition: users trust that online companies will use the correct behavior in relation to their personal data;
- some works highlight the difference between primary groups or communities (where the emotional component is essential) and broad or anonymous groups (**Ling**, 2008). This double dimension would explain the duality of a generic caution about privacy in the digital environment and the specific transfer of data in emotionally mediated contexts.

Considering the new context produced as a result of the *Cambridge Analytica* / *Facebook* incident, in this paper we take a look at the perception of the transfer of personal data and the corresponding emotional response of users.

3. Hypothesis

Emotions are mental states of individuals towards concrete stimuli (**Reisenzein**, 2007) that play an important role in the formation of experiences, commitments, and learning. They are composed of a valence (positive or negative emotions), an activation (intensity of emotion, high or low), and a certain level of control (high or low) (**Pekrun**; **Perry**, 2014), with

greater influence than the rational questions in human decisions. Therefore, when users know about the unauthorized dissemination of their personal information in the context of the use of social networks and mobile applications, we believe it is important to recognize which emotions are aroused, with what intensity, and their relationship with privacy decisions.

Individuals respond in significantly different ways to the unauthorized dissemination of their personal data and presumably with different attributed intensities; therefore, we propose:

> H1: The users of social networks and applications have different emotional responses with different intensities when it comes to knowing the possible unauthorized disclosure of their private data.

Participants in social networks seek interpersonal relationships and the use of apps has a functional objective; therefore, it is consistent to assume that users will respond emotionally different to the possible disclosure of their private data. Hence:

> H1a: The emotional response to the unauthorized disclosure of private data in a social network is different from the corresponding one if the disclosure occurs in an app.

For this reason, it is possible to consider that the users show different intensities in their emotional response depending on whether they are using apps or social networks:

> H1b: There are differences in emotional intensities depending on whether the possible unauthorized disclosure of private data comes from an app or a social network.

Since not all emotions express the same level of activation, we understand that individuals who feel emotions of greater activation should report greater emotional intensity than individuals with lower activation emotions:

> H2. There are differences in the intensity attributed by individuals to the different emotions reported when finding out the possible unauthorized disclosure of their private data depending on the level of activation of each emotion.

If emotions have a significant impact on the behavior of individuals, those who show more intense emotions should behave consistently and modify and update their privacy parameters in social networks. However, the paradox of privacy from the perspective of emotional intensity would imply the absence of correspondence between the emotions aroused by the loss of privacy and the behavior of online privacy management. In consequence:

> H3: The modification of the level of privacy in social networks corresponds to a different intensity of the emotional response to the possible unauthorized disclosure of private data.

On the ubiquitous internet, little is known about what motivates users to give personal information beyond their intention to maintain/create interpersonal and leisure relationships (**Krasnova** *et al.*, 2010). The truth is that the chain of incidents of cession of personal data suffered by the users of some networks has caused many to modify their privacy settings. This change must have been more pronounced the smaller the predisposition to yield private information. Nevertheless, **Krasnova** *et al.* (2010) point out that the perception of privacy risks can be mitigated by the perceived control of the level of information that can be disseminated. Therefore, in the absence of information we propose:

> H4: The action of having modified the level of privacy in social networks is independent of the propensity to allow access to personal data in order to use a mobile application.

4. Method

4.1. Participants

The target population is Spaniards between the ages of 18 and 65 who own and use a mobile smartphone, keep data (contacts, photographs, emails, music, etc.) in the cloud, and/or have experience in social networks (*Facebook*, *Instagram*, etc.). The sociodemographic profile of the sample is described in table 1.

Table 1. Sample profile

Sex	Men	200 (50.0%)
	Women	200 (50.0%)
Age	18-25	80 (20.0%)
	26-35	102 (25.5%)
	36-50	118 (29.5%)
	51-65	100 (25.0%)
Educational level	Primary	8 (2.0%)
	Secondary	78 (19.5%)
	Professional education / Technical college	102 (25.5%)
	University	212 (53.0%)

The study is conducted in Spain, a country that leads the ranking of penetration of smartphones by unique users with 88% (*Ditrendia*, 2018). The same proportion of men and women with smartphones has been used, since the significant levels of gender gap accessing this technology are outside the age interval considered. (*INE*, 2018). The age levels were chosen according to generational division type (Generation Z: 18 to 25, Generation Y: 26 to 35, Generation X: 36 to 50, Generation *Boomer*: 54 to 65). As for the studies, there is a greater number of people with higher education (53.0%) since it is the dominant profile of the Internet user via mobile (*AIMC*, 2018).

4.2. Design and procedure

Participants are panelists recruited by the company *Cint*[2] to participate in online research, so the sample (n=400) can be considered non-random, although quotas have been followed by sociodemographic levels. However, we understand that this selection process is close to a random one, as the number of *Cint*'s panelists exceeds 1.2 million in Spain and the participants were contacted randomly. In this case, p=q=50, N>20,000 (infinite), n=400, e=4.85%.

The software used for the questionnaire presented informed consent on the first screen. The appearance of response options was also randomized, thus avoiding the order bias that occurs in static questionnaires. The field work was developed in the last third of June 2018.

> "Social platforms, as well as being affective networks, are coded systems of emotional reactions that transform moods into processable data"

4.3. Instruments

The variables used in this study are:

1) Emotional response to the use of personal data without consent. The bibliography has addressed the emotional response to mobile marketing (**Florido-Benítez**, 2016), advertising (**Pham**; **Wang**, 2017), and smartphone security (**Thorsteinsson**; **Page**, 2014), but we have not found studies on our variable of interest. Derived from the *Cambridge Analytica* / *Facebook* incident, we raise the question:

> "Suppose that it is published in the press that your data (and that of other users) has been used without your consent or knowledge. Check the option that best reflects your feelings if who uses your data is...", differentiating between social networks and applications.

We use the proposed universal emotions from **Ekman** *et al.* (1987) of negative valence –sadness, anger, fear and disappointment- and neutral –surprise-, discarding emotions of joy (we understand that disclosure of private information cannot generate it) and disgust (considering it unrelated to our object of interest). To avoid the bias of extremism we use disappointment as a synonym for anger. As for its activation, we consider anger and disappointment of high intensity, while we recognize sadness and fear of low intensity/activation. The emotions used appear in table 2.

2) Intensity (reported) of the emotional response ('IER_net'; 'IER_apps'). It consists of the declared valuation (because it is a past behavior) on a scale of 10 points (1= little to 10 = much) of the felt emotion. We opted for a mono-item variable, the use of which use is supported by bibliography (**Petrescu**, 2013; **Bergvist**, 2015) and allows a quick, simple and holistic evaluation of a one-dimensional construct. For the answer, a sliding scale was used by means of a mouse.

3) Predisposition to allow applications access to personal data. A list of data types was made, and each user was asked to quantify, on an ordinal scale of four points (1=none, 2=little, 3=quite, and 4=much), the degree of agreement to allow access to personal data in exchange for using an application on the mobile device. The types of data used were those indicated in the first column of table 4.

4) Change of privacy level. The question was: "Have you changed your level of privacy in your social networks in the last year?" with three potential answers: (a) Yes, in all of them; (b) Yes, in some of them; (c) Use the default settings.

5. Results

To check H1 we apply the Kruskal-Wallis H test, because it is the non-parametric version of the variance analysis, since the variables 'IER_net' and 'IER_apps' are ordinal. Table 2 shows the results for both social networks and apps. The differences between the emotional types are important: sadness is hardly mentioned ($n_{social\ networks}$=4; n_{apps}=6), while anger (more cited with $n_{social\ networks}$=171 or 42.75%, n_{apps}=164 or 41.0 %) and disappointment show high intensities. In both cases, the feeling of sadness (of low activation) can be considered marginal, and the reaction of anger is the most frequent and the one with the greatest intensity reported. Among the feelings (except sadness) there are differences in their perceived intensities, so we confirm H1.

To check H1a we built a 5x5 contingency table with the declared emotions for both social networks and apps. We observe that the independence test $\chi 2$=174.36 (df=16, p=0.00, d_{Cohen}=1.76) shows that the users declare significantly different emotions when they refer to an incident in social networks or in apps, thus confirming H1a.

To check H1b (if there are differences in the reported intensities between apps and social networks), we apply the t-test for each emotion, finding that there are no differences in the intensities depending on whether it is on social networks or in apps:

- anger: n=171, t=0.63, df=335.8, p=0.73;
- surprise: n=80, t =0.08, df=157.3, p=0.61;
- fear: n=82, t=0.43, df=161.4, p=0.92;
- disappointment: n=63, t=0.80, df=117.4, p=0.74.

In conclusion, it is not possible to accept H1b.

Table 2. Results of the contrasts for H1

Emotions	For social networks				For apps			
	Me	n	AR	KW-Test	Me	n	AR	KW-Test
Sadness	4.5	4	50.25	Chi-2=89.96 df=4 p=0.00	5.0	6	48.08	Chi-2=60.61 df=4 p=0,00
Anger	9.0	171	245.64		9.0	164	237.06	
Surprise	6.0	80	110.54		7.0	86	138.04	
Fear	8.0	82	184.51		8.0	78	180.31	
Disappointment	9.0	63	222.56		8.5	66	228.76	
Me=Median, AR= Average range, KW-Test= Kruskal-Wallis Test, df= degrees of freedom								

As the intensity of the emotions has been expressed on an ordinal 1-10 scale, to check H2 we applied the Mann-Whitney U test, discarding the feeling of sadness as has n≤6 cases. For most of the cases, regarding the effect sizes –measured by the ratio r=Z/√n (**Lenhard**; **Lenhard**, 2016)- we observe that the different distributions have different median values, except for the emotional binomials anger-disappointment and fear-disappointment. The biggest difference is obtained by the feelings anger-surprise (Z=-8.76, p=0.00, r=0.44). Table 3 presents the numerical findings. We conclude that H2 is confirmed, because emotions with different levels of activation show heterogeneity in their distributions, while the comparison between two active-type feelings yields non-significant results –homogeneity- (Z=-1.42, p=0.16, r=0.07).

Table 3. Results of the contrasts for H2

Emotions	Surprise (Activation: neutral)	Fear (Activation: low)	Disappointment (Activation: high)
Anger (Activation: high)	AR_{anger}= 152,80 $AR_{surprise}$= 68,71 Z=-8,76, p= 0,00 r=0,44***	AR_{anger}= 13,94 AR_{fear}= 100,01 Z= -4,21, p= 0,00 r=0,21**	AR_{anger}= 121,13 $AR_{disappointment}$= 107,63 Z= -1,42, p= 0,16 r=0,07^{ns}
Surprise (Activation: neutral)	--	$AR_{surprise}$= 65,47 AR_{fear}= 97,14 Z= -4,35, p= 0,00 r=0,22**	$AR_{surprise}$= 54,43 $AR_{disappointment}$= 94,31 Z= -5,80, p= 0,00 r=0,29**
Fear (Activation: low)	--	--	AR_{fear}= 66,87 $AR_{disappointment}$= 80,98 Z= -2,05, p= 0,04 r=0,10*
***=High effect, **= Intermediate effect, *=Low effect, ns= not relevant AR=Average Range, Z=Test Z, r=effect size			

To corroborate H3, we applied the Kruskal-Wallis H test considering three possible types of modifications (in all networks, only in some, use the default privacy settings). We find that χ2=4.30, df=2, p=0.12, d_{Cohen}=not significant) so we cannot accept H3 in the sense that different types of levels of modification of privacy levels (which denote different concerns for this) do not show different declared emotional intensities in the case of private data dissemination. This implies that we do not detect a connection between an active behavior on privacy and an intense emotional manifestation of a negative type.

Finally, to test H4, we used the χ2 test, since it is important to check whether the change in privacy levels is independent of the agreement to allow access to private information by mobile applications. Table 4 shows that, except for photographic information (χ2=20.01 p=0.02 d=0.46), the rest of the tests are not significant. Therefore, we confirm the independence except for photographic information, where 62% of users is totally opposed to accessing their albums, screenshots, *WhatsApp* images, and similar.

Table 4. Contrast results for H4

Types of information	n	Test (df=9)
Name and email address	400	χ2=11.59 p=0.23 d=ns
Age, nationality, marital status, and children	397	χ2=16.02 p=0.07 d=ns
Contacts and social networks	395	χ2=10.43 p=0.32 d=ns
Applications used	394	χ2=11.21 p=0.26 d=ns
Searches and purchases made	394	χ2=13.94 p=0.13 d=ns
Advertising checked	394	χ2=13.02 p=0.16 d=ns
Calendar or planner	393	χ2=11.15 p=0.27 d=ns
Location	400	χ2= 8.67 p=0.47 d=ns
Emails and other messages	396	χ2= 8.05 p=0.53 d=ns
Photographs	395	χ2=20.01 p=0.02 d=0.46
Call metadata	395	χ2=10.0 p=0.35 d=ns
Payment methods	394	χ2=14.29 p=0.11 d=ns
Physical activity and health	394	χ2=15.22 p=0.09 d=ns
d= Effect size (d_{Cohen}), ns=not relevant for p≥0.05, df= degrees of freedom.		

6. Debate and conclusions

The paradox of privacy expresses the contradiction in the fact that users value their privacy very much, but at the same time they are willing to give it up in exchange for small rewards. The bibliography has addressed this paradox mainly using cognitive-rational approaches, assuming the user has a logical and consistent behavior with their attitudes and perceptions. But the explanations from the rational behavior approach (incentives to users, context, social capital that they are contributing with, etc.) have not shown a significant advance in understanding why this paradox occurs. Only recently have emotional approaches and variables been included to analyze the transfer of private information by the users themselves in their social networks and in applications. The recent incidents of fraudulent cession of private data (by sale or by access) suffered by *Facebook* users show that users, despite being more concerned about their privacy, are still active in their applications and social networks, and they continue to give away personal information.

> Users, despite being more concerned about their privacy, continue to give away personal information

To address the study of emotions we have raised an incident of unauthorized dissemination of their private data and we have analyzed the resulting reactions, comparing them both with the behavior of change in privacy settings as well as with the propensity to allow access to personal data when using their applications/social networks thorugh the mobile device. The most reported emotion is anger (active feeling) which, along with disappointment (also active emotion), are reported with greater intensity. However, we noticed that for social networks and applications, the emotions reported are of different type, although their reported intensities can be considered similar.

We also found differences in the declared intensity between the emotions of high activation (anger, disappointment), low (fear), and neutral (surprise), but not between the two high activation emotions. Additionally, the higher intensities are also associated with negative emotions of active type (anger and disappointment), while the lower intensities correspond to negative emotions of low activation. This is interesting, because active-type emotions involve changes of mind and behavior, being *a priori* less compatible with attitudes of resignation, conformity, or incongruity. In this sense, the active condition of the emotions reported in relation to a situation of loss of privacy and the intensities associated with these would reinforce the contradictory nature of the privacy paradox.

Users with different levels of privacy do not show differences in the intensity of their declared emotions, in such a way that those who report having changed their privacy in all their social networks show similar emotional intensity than those who use the default settings. Also, the propensity to give up personal data is not related to changes made in privacy settings, except for photographs where, interestingly, users are very reluctant to share (albums, *WhatsApp* images, and screenshots). In conclusion, we detect high anger and disgust at the unauthorized cession of private data but there is no difference in the emotional intensity felt between those who are restrictive with their privacy settings and those who are not. Our results support the paradox of privacy, in the sense that the intense emotional response declared before an incident of unauthorized cession of private data does not correspond to more or less restrictive adjustments of the privacy options. Nor does it correspond to the agreement that social media platforms access personal information in exchange for using applications. There seems to be a certain disconnect –as a basis for the contradiction- between the decisions of informational behavior in relation to the management of privacy and emotions associated with the perception of privacy in social networks and mobile applications.

One possible explanation is that there are previous emotional barriers (isolation, costs of restarting in another network, loss of popularity, need to learn another application, or to be known) that generate 'captive' users of applications and social networks. This captivity is a psychological anchoring that, in line with what **Fox** and **Moreland** (2015) pointed out, can lead users to remain active in social networks due to the social pressure of other members to stay active in them. Therefore, to continue in the social network or to use an application could be more motivated by a psychosocial dependence than by being an autonomous decision, conscious and free for the users.

> Only recently have emotional approaches and variables been considered when analyzing the transfer of private information by the users themselves in social networks and in applications

A second explanation refers to the fact that users can also apply decision processes based on non-linear and non-compensatory criteria. It would be a mistake to consider as banal the gain of a potential incentive (e.g. possibility of contacting friends) against the current transfer of private data, since the emotional burden underlying the incentive may be higher than the intangible cost of transferring private information. Previous research has shown that emotional rewards have a much greater weight than rational rewards, and that different users can follow very different decision rules (**Ovčjak**; **Heričko**; **Polančič**, 2016).

This study is a first approach to the emotional problem, and we believe that future efforts should be made to analyze what emotional aspects are involved (rewards, costs, and effects), as well as the decision rules of the users, in order to

improve the explanation of the paradox of privacy. This paper offers clues about emotional responses, but it has two limitations: having used both basic emotions and declared responses to a hypothetical event. In this sense, it would be interesting to develop studies that situate users in front of a real or simulated incident, so that emotions can be measured without the need to verbalize them (to avoid alexithymia[3] problems) and to know the decision rules involved.

> "Users with different levels of privacy do not show variances in the intensity of their declared emotions"

7. Notes

1. The term "colonization" is used by the cited authors (**Scoble** & **Israel**, 2014) to refer to the growing occupation of daily time and the attention of users for the routines generated through the different services and products of mobile devices (games, social networks, utilities, etc.). The objective of occupying time and attention that was previously devoted to other routines (hence the metaphor 'colonization') is directly related to business models based on capturing, managing and monetizing personal information: the longer and the more often users use certain services, the more and the better personal information they provide.

2. *Cint* is a Swedish company present in more than 80 countries.
https://www.cint.com

For compliance with ethical standards, see
https://www.cint.com/quality-standards

3. Alexithymia is the inability to identify one's emotions.

8. References

Acquisti, Alessandro; **Brandimarte, Laura**; **Loewenstein, George** (2015). "Privacy and human behavior in the age of information". *Science*, v. 347, n. 622, pp. 509-514.
https://doi.org/10.1126/science.aaa1465

Acquisti, Alessandro; **Grossklags, Jens** (2005). "Privacy and rationality in individual decision making". *IEEE security & privacy*, v. 3, n. 1, pp. 26-33.
https://doi.org/10.1109/MSP.2005.22

Aguado, Juan-Miguel; **Martínez, Inmaculada José** (2014). "The relationship is the medium: Understanding media in a mobile age". In: Katz, James. *Living inside mobile social information*. Boston, MA: Boston University Press, pp. 77-108.

AIMC (2018). *20º navegantes en la Red. Encuesta AIMC a usuarios de Internet*. Marzo. *Asociación para la Investigación de Medios de Comunicación*.
http://download.aimc.es/aimc/ARtu5f4e/macro2017/#page=1

Bergkvist, Lars (2015). "Appropriate use of single–item measures is here to stay". *Marketing letters,* v. 26, n. 3, pp. 245-255.
https://doi.org/10.1007/s11002-014-9325-y

Chen, Hsuan-Ting (2018). "Revisiting the privacy paradox on social media with an extended privacy calculus model: The effect of privacy concerns, privacy self-efficacy, and social capital on privacy management". *American behavioral scientist*, v. 62, n. 10, pp. 1392-1412.
https://doi.org/10.1177/0002764218792691

Dienlin, Tobias; **Trepte, Sabine** (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*, v. 45, n. 3, pp. 285-297.
https://doi.org/10.1002/ejsp.2049

Ditrendia (2018). *Informe Ditrendia 2017: Mobile en España y en el mundo*.
https://www.amic.media/media/files/file_352_1289.pdf

Doyle, Kim (2015). "Facebook, Whatsapp and the commodification of affective labour". *Communication, politics & culture*, v. 48, n. 1, pp. 51-65.
https://search.informit.com.au/documentSummary;dn=383824705363393;res=IELHSS

Ekman, Paul; **Friesen, Wallace V.**; **O'Sullivan, Maureen**; **Chan, Anthony**; **Diacoyanni-Tarlatzis, Irene**; **Heider, Karl**; **Krause, Rainer**; **Lecompte, William-Ayhan**; **Pitcairn, Tom**; **Ricci-Bitti, Pio E.**; **Scherer, Klaus**; **Tomita, Masatoshi**; **Tzavaras, Athanase** (1987). "Universals and cultural differences in the judgments of facial expressions of emotion". *Journal of personality and social psychology*, v. 53, n. 4, pp. 712-717.
https://doi.org/10.1037/0022-3514.53.4.712

Florido-Benítez, Lázaro (2016). "The impact of mobile marketing in airports". *Journal of airline and airport management*, v. 6, n. 1, pp. 1-18.
https://doi.org/10.3926/jairm.39

Fox, Jesse; **Moreland, Jennifer J.** (2015). "The dark side of social networking sites: An exploration of the relational and psychological stressors associated with Facebook use and affordances". *Computers in human behavior*, v. 45, n. 168-176.
https://doi.org/10.1016/j.chb.2014.11.083

Gerlitz, Carolin; **Helmond, Anne** (2013). "The like economy: Social buttons and the data-intensive web". *New media & society*, v. 15, n. 8, pp. 1348-1365.
https://doi.org/10.1177/1461444812472322

Gómez-Barroso, José-Luis; **Feijóo, Claudio** (2013). Información personal: la nueva moneda de la economía digital. *El profesional de la información*, v. 22, n. 4, pp. 290-297.
https://doi.org/10.3145/epi.2013.jul.03

Gómez-Barroso, José-Luis; **Feijóo, Claudio**; **Martínez-Martínez, Inmaculada J.** (2018). "Cesión calculada de información personal: factores que influyen en la percepción de beneficio". *El profesional de la información*, v. 27, n. 2, pp. 341-348.
https://doi.org/10.3145/epi.2018.mar.12

Hargittai, Ezster; **Marwick, Alice** (2016). "What can I really do? Explaining the privacy paradox with online apathy". *International journal of communication*, v. 10, n. 21, pp. 3737-3757.
https://doi.org/10.5167/uzh-148157

INE (2018). *Población que usa internet (en los tres últimos meses). Ciencia y tecnología, sociedad de la información (actualizado 13 diciembre 2017)*. *Instituto Nacional de Estadística.* Gobierno de España.
https://bit.ly/1PYwho6

Kanter, Jake (2018) "The backlash that never happened: New data shows people actually increased their Facebook usage after the Cambridge Analytica scandal". *Business insider*, 20 May.
https://www.businessinsider.es/people-increased-facebook-usage-after-cambridge-analytica-scandal-2018-5?r=US&IR=T

Kehr, Flavius; **Wentzel, Daniel**; **Kowatsch, Tobias** (2014). "Privacy paradox revised: Pre-existing attitudes, psychological ownership, and actual disclosure". In: *35th Intl conf on information systems*. Auckland, New Zealand.
https://bit.ly/2R3OdAo

Kokolakis, Spyros (2017). "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon". *Computers & security*, v. 64, pp. 122-134.
https://doi.org/10.1016/j.cose.2015.07.002

Krasnova, Hanna; **Spiekermann, Sarah**; **Koroleva, Ksenia**; **Hildebrand, Thomas** (2010). "Online social networks: Why we disclose". *Journal of information technology*, v. 25, n. 2, pp. 109-125.
https://doi.org/10.1057/jit.2010.6

Krol, Katarzyna K. (2016). *The role of effort in security and privacy behaviours online.* Doctoral dissertation. UCL: University College London.
https://bit.ly/2TibLpn

Lenhard, Wolgang; **Lenhard, Alexandra** (2016). "Calculation of effect sizes". *Psychometrica*.
https://doi.org/10.13140/RG.2.1.3478.4245

Li, Han; **Luo, Xin R.**; **Zhang, Jie**; **Xu, Heng** (2017). "Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors". *Information & management*, v. 54, n. 8, pp. 1012-1022.
https://doi.org/10.1016/j.im.2017.02.005

Ling, Rich (2008). *New tech, new ties*. Cambridge, MA: MIT press. ISBN: 978 0 262515047

Lutz, Christoph; **Strathoff, Pepe** (2014). *Privacy concerns and online behavior – Not so paradoxical after all? Viewing the privacy paradox through different theoretical lenses* (April, 15).
https://doi.org/10.2139/ssrn.2425132

Martínez-Martínez, Dolores-Fuensanta (2018). "Unificación de la protección de datos personales en la Unión Europea: desafíos e implicaciones". *El profesional de la información*, v. 27, n. 1, pp. 185-194.
https://doi.org/10.3145/epi.2018.ene.17

Miltgen, Caroline L.; **Peyrat-Guillard, Dominique** (2014). "Cultural and generational influences on privacy concerns: a qualitative study in seven European countries". *European journal of information systems*, v. 23, n. 2, pp. 103-125.
https://doi.org/10.1057/ejis.2013.17

Min, Jinyoung; **Kim, Byoungsoo** (2015). "How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit and cost". *Journal of the Association for Information Science and Technology*, v. 66, n. 4, pp. 839-857.
https://doi.org/10.1002/asi.23206

Ovčjak, Boris; **Heričko, Marjan**; **Polančič, Gregor** (2016). "How do emotions impact mobile services acceptance? A systematic literature review". *Mobile information systems*. Article ID 825303.
https://doi.org/10.1155/2016/8253036

Pekrun, Reihardt; **Perry, Raimond P.** (2014). "Control-value theory of achievement emotions". In: Pekrun, Reihardt; Linnenbrink-Garcia, Lisa (eds.). *International handbook of emotions in education*, pp. 120-141. London. Routledge. ISBN: 978 0415895026

Petrescu, Maria (2013). "Marketing research using single–item indicators in structural equation models". *Journal of marketing analytics*, v. 1, n. 2, pp. 99-117.
https://doi.org/10.1057/jma.2013.7

Pham, Phuong; **Wang, Jingtao** (2017). "Understanding emotional responses to mobile video advertisements via physiological signal sensing and facial expression analysis". In: *Proceedings of the 22nd Intl conf on intelligent user interfaces*, pp. 67-78. ACM.
http://people.cs.pitt.edu/~jingtaow/research/attentivevideo-iui2017.pdf

Reisenzein, Reiner (2007). "What is a definition of emotion? And are emotions mental-behavioral processes?". *Social science information*, v. 46, n. 3, pp. 424-428.
https://doi.org/10.1177/0539018407046003011O

Scoble, Robert; **Israel, Shel** (2014). *Age of context: Mobile, sensors, data and the future of privacy*. Patrick Brewster Press. ISBN: 978 1 492348436

Serrano-Puche, Javier (2016). "Internet y emociones: Nuevas tendencias en un campo de investigación emergente". *Comunicar*, v. 46, n. 1, pp. 19-26.
https://doi.org/10.3916/C46-2016-02

Smith, Matthew; **Szongott, Christian**; **Henne, Benajmin**; **Von-Voigt, Gabriele** (2012). "Big data privacy issues in public social media". In: *6th IEEE Intl conf* on *digital ecosystems technologies.*
https://doi.org/10.1109/DEST.2012.6227909

Spiekermann, Sarah; **Acquisti, Alessandro**; **Böhme, Rainer**; **Hui, Kai-Lung** (2015). "The challenges of personal data markets and privacy". *Electronic markets*, v. 25, n. 2, pp. 161-167.
https://doi.org/10.1007/s12525-015-0191-0

Su, Zhou; **Xu, Qichao**; **Qi, Qifan** (2016). "Big data in mobile social networks: A QoE-oriented framework". *IEEE network*, v. 30, n. 1, pp. 52-57.
https://doi.org/10.1109/MNET.2016.7389831

Thorsteinsson, Gisli; **Page, Tom** (2014). "User attachment to smartphones and design guidelines". *International journal of mobile learning and organisation*, v. 8, n. 3/4, pp. 201-215.
https://doi.org/10.1504/IJMLO.2014.067020

Wang, Tien; **Duong, Trong-Danh**; **Chen, Charlie C.** (2016). "Intention to disclose personal information via mobile applications: A privacy calculus perspective". *International journal of information management*, v. 36, n. 4, pp. 531-542.
https://doi.org/10.1016/j.ijinfomgt.2016.03.003

West, Sarah-Myers (2019). "Data capitalism: Redefining the logics of surveillance and privacy". *Business & society*, v. 58, n. 1, pp. 20-41.
https://doi.org/10.1177/0007650317718185

Annex. Questions used in the research

Let's assume that your data, and that of others users, has been published in the press, without your consent or knowledge. Check the option that reflects best your feelings if who uses your data is:

	You feel mainly...
A. A social network	☐ Sad ☐ Upset ☐ Surprised ☐ Afraid ☐ Disappointed
B. An application downloaded to the mobile	☐ Sad ☐ Upset ☐ Surprised ☐ Afraid ☐ Disappointed

(After answering each line, a slide bar appears on the screen in order for the respondent to indicate the intensity in which he feels the emotion indicated)

How intense do you feel like that?

Slightly <emot> Very <emot>

Answer for A: variable IER_net

Answer for B: variable IET_apps

C. To what extent do you agree to allow access to the following data in exchange for using an application of your interest on your mobile?

Name and email address
Age, nationality, marital status and children
Contacts and social networks
Applications that you use
Searches and purchases made
Advertising checked
Calendar or planner
Location
Emails and other messages
Photographs
Call metadata
Payment methods
Physical activity and health

1	2	3	4	5	6	7	8	9	10

Response options: 1=none, 2=little, 3=quite and 4=much (without numbers, using radio-buttons).

D. Have you modified the level of privacy in your social networks in the last year?

Yes, in all of them.
Yes, in some of them.
You use the default settings.