Privacy Protection on Social Networks: A Scale for Measuring Users' Attitudes in France and the USA

Jean-Éric Pelet[1(✉)] and Basma Taieb[2]

[1] ESCE Paris, Nantes University, Nantes, France
je.pelet@gmail.com
[2] University of Cergy-Pontoise, Cergy, France

Abstract. Registrations on social networks proliferate in the everyday life of users and consumers, and questions remain whether the data they disseminate are kept safe. The protection of online privacy is an increasingly more pressing issue, especially regarding social networks such as Facebook, Twitter, Instagram or LinkedIn, and concerns have arisen among Internet users. Following Churchill's paradigm [1], we have developed a scale to measure privacy-related attitudes (Privacy Policy Concern). In Study 1, 15 interviews were conducted in order to explore attitudes towards privacy policy concerns on social networks and to generate items. In Study 2, a series of confirmatory analyses were conducted using French and American data to validate the scale of concern about the privacy policies of social networks.

Keywords: M-commerce · Website design · Culture · Purchase intention · Revisit intention · Intention to recommend

1 Introduction

Due to its ubiquity and immense reach, the social network Facebook has proven ideal for the online positioning of brands [2]. Even if social networks may enhance our lives in many ways, they also raise new concerns in the context of our "information society", such as the use of data which we, as users, upload or write for sharing purposes. Social networks manage such practices without our knowledge or consent and in an attempt to understand the results which occur from this phenomena, researchers strive to tackle some variables they encompass by working on various topics around them [3]. [4] have worked on 3 scales that enable the development and validation of scales for measuring privacy-related attitudes (Privacy Concern) and behaviors (General Caution and Technical Protection) in the company websites context. [5] have worked on the information disclosure of social network users to show that in social networking contexts, control over personal information is negatively and statistically associated with information disclosure. As demonstrated by [6] several researchers have provided overarching macro models to explain individuals' privacy-related decision making. The most expansive of these macro models is labeled "Antecedents–Privacy Concerns–Outcomes" (APCO), and in order to enhance its contribution and understand even more users' behaviors, [6] propose to consider principles from behavioral economics (such as biases and bounded

Á. Rocha et al. (eds.), *Recent Advances in Information Systems and Technologies*,
Advances in Intelligent Systems and Computing 570, DOI 10.1007/978-3-319-56538-5_77

rationality) and psychology (such as the elaboration likelihood model) that also affect privacy decisions. Top MIS journals such as *MIS Quarterly*, *Information Systems Research*, *European Journal of Information Systems*, *Journal of Strategic Information Systems*, and others have thereby taken to task and published an impressive body of research on privacy (see for references [7–9]).

The collection of personal information has caused serious concerns about the invasion of privacy of individuals [10], to the extent that companies are increasingly committed to the data protection of personal information. The more worried consumers are, the more likely companies will be to adopt data protection and privacy policies. If the expected benefits are below cost, or, more precisely, if the risk of spreading a certain amount of information online is implied, then the consumer perceives a threat to the confidentiality of personal information and will not go through with the purchase. The privacy calculus as explored by some researchers, see for example [11, 12] and defined by [13] as a theory which proposes that an individual's intention to disclose personal information, is based on risk-benefit analysis. According to the privacy calculus theory, individuals compare perceived risks and anticipated benefits. The privacy calculus integers privacy concerns, perceived benefits, and convenience [14]. In this vein, there is a need for constructs that reflect consumers' attitudes towards privacy policy concerns with social networks. The main purpose of this study is to develop and validate a multidimensional scale in order to measure attitude towards the privacy policies of social networks, from a psychological point of view. Among the various routes individuals take in order to make a decision that are the central and the peripheral one, the central one explores rationally formed attitudes and the peripheral route explores external stimuli. *"This is the route of low-effort thinking and heuristic processes when shaping one's behavior"* [3]. On the peripheral route, information processing and decisions are enacted by simple, relatively automatic cognitive heuristics processes that are derived from past experiences and associations. This is what this paper aims at exploring and confirming thanks to the creation of a scale.

Understanding user behavior is vital in order to entice consumers to interact with companies using a company's social networks. Because information processing and decisions are enacted by simple, relatively automatic cognitive heuristics processes that are derived from past experiences and associations [3], we believe that our results show that the proposed scale is a valid and reliable measurement instrument that may serve as a forward step in contributing to current research, the literature and practice. The following section presents a literature review on privacy policy concerns about social networks followed by the exploratory qualitative study and quantitative study. The paper ends with the conclusion, implications, limitations and suggestions for future research.

2 Literature Review on Privacy and Social Networks

The concept of "privacy" is broad, complex, and includes several meanings, to the extent that translating it with the term "confidentiality" or "private life" would be simplistic. Privacy is defined as "the act to ensure that the information is only accessible to those whose access is authorized" by the International Organization for Standardization

(ISO)[1] and the GDPR[2] defines the "privacy by design" as a principle that calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. Respect for privacy is a right covered in Article 9 of the Civil Code. However, this right has been more precisely defined by case law and political doctrine, suggesting the difficulty of establishing a boundary between private life and public life. It is therefore a particular aspect of this definition. [15] showed that the public was more tolerant than professionals, from an ethical point of view, as to certain marketing practices, with the exception of those that can be dangerous, both for the individual and his/her privacy, for example the absence of particular information about a product, which occurs frequently on social networks. As for social networks, we rely on Kaplan and Haenlein's definition [16, p. 61] according to which social networks are considered as "a group of internet-based applications that builds on the ideological and technological foundations of Web 2.0" and which allows for "the creation and exchange of user-generated content."

3 Research Method

Our research method includes both a qualitative and a quantitative study. The main objective of the exploratory phase is to investigate the general impressions of users of social networks, in terms of security of privacy and policy concerns. The aim here is to draw up an inventory of users' feelings about the security of their personal information on the Internet, particularly for those who use social networks both for private and public use. The information gathered during this first phase is then analyzed in order to establish items which will be empirically tested and validated during the quantitative study.

3.1 Study 1: Qualitative Study

Satisfying the criterion of saturation of the data [17], this first exploratory phase, conducted with 15 respondents, revealed a link between the confidence Internet users have in social networks and the behavior they adopt online. We have oriented this first exploratory phase towards a student audience, largely digital and consumers of social networks, in order to facilitate our research. Indeed, 42% of social network users are between the ages of 18 and 34 (US Demographics Study - June 2016). Thus, the sample of the qualitative phase was composed of a student population, of French nationality, aged between 18 and 30 years.

3.2 Results of the Qualitative Study

Each semi-direct interview was recorded before being transcribed and analysed using the common coding system of such an exploratory phase. The first topic - without specific question asked at the beginning to facilitate the answers - addresses the issue of social networking users' attitudes towards this medium. We found that all interviewees

[1] Standard ISO/ IEC 27002:2005.
[2] General Data Protection Regulation: http://www.eugdpr.org/.

claimed not to trust social networks. For example, according to Pauline, *"people can tell so much about other people's lives on Facebook, so that in the end it is more dangerous. Anecdotally, the danger would come from improper use of the social network on the part of users"*. In Coralie's opinion, *"through lack of information and awareness, people can put themselves in dangerous situations."* However, the sub-group of questions about the storage and permeability of access to personal information generated the most varied responses. According to Julie S., *"if we want access to my personal information, we will get there one way or another"*, while - for Jeremy - this was *"not to be public, no need to know."* However, somewhat paradoxically, the respondents did not consider themselves generally worried about the safety of their personal information on social networks. Jeremy told us that *"if I don't put something on Facebook, I cannot really see what I have to fear"*. Interviewees consistently operate a distinction between private social networks, like Facebook, Twitter or Instagram, and professional social networks like LinkedIn and Viadeo. According to Patrick, *"Linkedin and Viadeo are entirely different"*. Indeed, they are more likely to convey a positive image of the user. The personal information shared on professional social networks is thus selected, and, for Laura, *"it is neutral data"*. *"That in itself is not a dangerous thing"*, adds Margot. In addition, using professional social networks as tools to improve the public image of Internet users and to protect their personal information is becoming more and more common. For all respondents, it is up to the user to be careful. Under the personal control of the information published on social networks, participants in the talks highlighted the choice to filter personal information, such as *"institutions attended"*, religious orientation or other categories.

Many denounced a general lack of information about the behavior of global networks and their privacy policies. Specifically, it was found that users consider social networks to be unclear regarding their privacy policies. Julie M. and Agathe think they are *"fuzzy"*, although the consultation of privacy policies and the use of all social networks are accessible to their users. However, among the interviewees, very few said they had actually read the privacy policies of the social networks they use. For many, this is the *"blah",* to borrow the term used by Clara, that nobody is going to read, because of the volume that it represents. It is a *"huge unreadable charter"* according to Patrick, who compares a privacy policy to a contract, which very few people take the time to read, or at least not all the clauses. For Hugo, reading such a privacy policy is *"tedious"* but he concedes and assumes that social networks are very transparent. In fact, we noticed a paradox: users blamed a lack of clarity, but they do not take the time to read the information made available by the social network they use. Agathe would prefer the inclusion of set-up tutorials on the social network: *"At registration, it is much clearer, although they explain that there are parameters to adjust"* which means there is the need to *"teach people to use"*. Patrick provides a more accurate idea of what this user guide could be: *"a presentation similar to a PowerPoint, when registering on the social network. It would be something easy to read, unlike a huge unreadable chart. It should also be a kind of manual for the first steps of the users, on the same model"*. Other interviewees indicated it would increase the awareness of social network users of the privacy policies of these sites and the resulting risks for the security of their personal data. The

feedback at this stage enabled us to prepare eight items for the following confirmatory phase.

3.3 Study 2: Quantitative Research

Survey. The questionnaire firstly posed a series of questions about the use of personal information on social networks. Secondly, the eight items generated from the qualitative research were included and finally evaluated using a 7-point Likert scale for each item (from totally disagree to totally agree) and demographic questions.

Participants. 380 participants from France and 205 participants from the USA were invited to complete the questionnaire online, which asked for both nationality and location to diminish the bias of nationality. This convenience sample included students, employees and retired people who have all already had an exposure to social media. Of the 585 respondents, 38% were men and 62% were women. The high female proportion of participants (62%) reflects the French and US markets share by gender on Facebook [2]. There was a greater representation of people under 34 years old. Participants were informed that all responses they provided would remain confidential and would only be used to develop a measurement of the attitude towards privacy policies of social networks. The personal information provided on social networks varies between France and the USA. For example, almost 36% of French respondents (compared with 77% for Americans) agree to provide their views on gender, while 18% of French respondents are willing to disclose their political views (against 65% of Americans). Descriptive characteristics of the profiles of participants and the use of their personal information on social networks are presented in Appendix 1.

Factorial and Confirmatory Analyses. A series of factorial analyses have been conducted. The values of KMO were greater than the 0.50 required to extract factors from all items. A principal components analysis was performed to extract factors with eigenvalues greater than 1. The item's loading was used to maximize factor purity, identifying items as markers for each factor that had the highest loading in comparison with the other factors. These criteria were adopted and indicated two factors. The proportion of variance explained was almost 70% for Factor 1 and 30% for Factor 2 for France and the USA. Loadings for Factors 1 and 2 are shown in Table 1.

Factor 1 included three items (items 1, 2 and 3) and reflects the social network users' awareness of and concern for privacy policy. This could be labeled "caution with regard to social networks' privacy policies". Factor 2 included five items (items 4, 5, 6, 7 and 8) and reflects the technical aspect of social networks' privacy policies and the need to elaborate tutorials in order to educate users about how to operate them. Factor 2 could be labeled "technical difficulty of use of the privacy policy on social networks".

Following Churchill's paradigm [1], the next step consists in examining the reliability and validity of the scale. The measuring instrument is reliable when the items marked as factors are highly correlated. The validity of the scale checks whether items really measure the construct we suggest. For Factor 1, Cronbach's alpha was .69 and .41 for the USA and France respectively. For Factor 2, alpha was .75 (France) and .81

(USA). The exploratory analysis indicates that for France, Factor 1 is too unreliable. However, after removing some observations, a confirmatory analysis has shown a good internal consistency between items with a Joreskog's Rho score greater than .62 (Table 2).

Table 1. Factor loadings

Items	France		USA	
	KMO = .72		KMO = .72	
	Factor 1 loading	Factor 2 loading	Factor 1 loading	Factor 2 loading
1. I think that social networks are perfectly clear about their privacy policies	.231		.801	
2. I think that social networks' users are sufficiently aware of the privacy policies used by social networks	.116		.798	
3. I've already read the privacy policy of the social network(s) I use	.621		.750	
4. Privacy policies are generally too long		.522		.657
5. Privacy policies are generally difficult to read		.594		.756
6. I would like to know more about the privacy policies used by my social networks		.736		.798
7. I would like social networks to take more measures to make their users aware of their privacy policies		.786		.750
8. I would like some tutorials to be set up in order to inform people about privacy policy when they register on social networks		.717		.808

Table 2. Reliability and validity of the measurement scale of attitude towards the privacy policy of social networks, after removal of observations

	France			USA		
	Cronbach's alpha	Joreskog rho	Rho vc	Cronbach's alpha	Joreskog rho	Rho vc
Factor 1: Caution with regard to social networks' privacy policy	.41	.62	.44	.69	.69	.43
Factor 2: Technical difficulty of social networks' privacy policy	.75	.75	.42	.81	.80	.45

Table 3 shows the comparisons for items of the measurement of attitude towards privacy policy on social networks between men and women. Analysis of variance (ANOVA) was conducted for these gender comparisons. Women indicate more concern for the privacy policy on social networks. In particular, for the items 1, 6 and 7, mean scores were significantly greater for women than men.

Table 3. Attitude towards privacy policy of social networks: comparison between men and women

Items	Men (n = 223) Mean (SD)	Women (n = 350) Mean (SD)	F	P value
1. I think that social networks are perfectly clear about their privacy policies	2.78 (1.61)	3.17 (1.59)	8.11	.005*
2. I think that social networks' users are sufficiently aware of the privacy policies used by social networks	3.02 (1.69)	3.21 (1.63)	1.65	.199
3. I've already read the privacy policy of the social network(s) I use	3.39 (2.04)	3.49 (1.91)	.34	.555
4. Privacy policies are generally too long	5.73 (1.66)	5.89 (1.49)	1.33	.248
5. Privacy policies are generally difficult to read	5.44 (1.59)	5.50 (1.54)	.22	.636
6. I would like to know more about the privacy policies used by my social networks	5.14 (1.74)	5.45 (1.42)	5.43	.020*
7. I would like social networks to take more measures to make their users aware of their privacy policies	5.40 (1.45)	5.73 (1.32)	7.46	.006*
8. I would like some tutorials to be set up in order to inform people about privacy policy when they register on social networks	5.24 (1.63)	5.44 (1.49)	2.21	.137

Table 4 shows the comparisons for items of attitude towards privacy policy on social networks according to age. As with the whole sample, people aged 35 years and older had significantly greater mean scores than younger respondents, indicating more concern and awareness towards their use of social networks' privacy policies, especially, for items 7 and 8.

Table 5 shows the comparisons for items of the measurement instrument between France and the USA. Even if all items are relevant for both countries, however, differences between mean scores were significant ($p < .01$). We consider that the scale is a valid instrument for measuring the attitude towards privacy policy of social networks. Therefore, it could be useful and appropriate for validating the scale in other countries when building up further evidence.

Table 4. Attitude towards privacy policy of social networks: comparison according to age

Items	<25 years (n = 360) Mean (SD)	25 to 34 years (n = 138) Mean (SD)	>35 years (n = 75) Mean (SD)	F	P value
1. I think that social networks are perfectly clear about their privacy policies	3.28 (1.61)	2.60 (1.49)	2.55 (1.57)	13.00	.000*
2. I think that social networks' users are sufficiently aware of the privacy policies used by social networks	3.39 (1.67)	2.80 (1.61)	2.53 (1.46)	12.42	.000*
3. I've already read the privacy policy of the social network(s) I use	3.42 (1.92)	3.43 (2.06)	3.67 (2.00)	.49	.609
4. Privacy policies are generally too long	5.73 (1.60)	5.95 (1.56)	6.05 (1.31)	1.90	.150
5. Privacy policies are generally difficult to read	5.35 (1.58)	5.63 (1.56)	5.81 (1.37)	3.62	.027*
6. I would like to know more about the privacy policies used by my social networks	5.33 (1.49)	5.12 (1.75)	5.73 (1.43)	3.83	.022*
7. I would like social networks to take more measures to make their users aware of their privacy policies	5.61 (1.37)	5.42 (1.47)	5.88 (1.23)	2.72	.066*
8. I would like some tutorials to be set up in order to inform people about privacy policy when they register on social networks	5.36 (1.51)	5.13 (1.76)	5.80 (1.19)	4.57	.011*

Table 5. Attitude towards privacy policy of social networks: comparison between France and the USA

Items	France (n = 368) Mean (SD)	USA (n = 205) Mean (SD)	F	P value
1. I think that social networks are perfectly clear about their privacy policies	2.57 (1.37)	3.83 (1.68)	94.95	.000*
2. I think that social networks' users are sufficiently aware of the privacy policies used by social networks	2.69 (1.53)	3.93 (1.59)	82.80	.000*
3. I've already read the privacy policy of the social network(s) I use	3.23 (2.07)	3.86 (1.69)	13.68	.000*
4. Privacy policies are generally too long	6.26 (1.29)	5.05 (1.69)	90.14	.000*
5. Privacy policies are generally difficult to read	5.72 (1.54)	5.04 (1.50)	25.71	.000*
6. I would like to know more about the privacy policies used by my social networks	5.49 (1.54)	5.05 (1.56)	10.77	.001*
7. I would like social networks to take more measures to make their users aware of their privacy policies	5.82 (1.27)	5.21 (1.47)	26.56	.000*
8. I would like some tutorials to be set up in order to inform people about privacy policy when they register on social networks	5.50 (1.55)	5.12 (1.51)	7.78	.005*

4 Contributions, Limitations and Implications

This study takes place in the context of the growing role of social networks in business strategies. The literature review has shown that Internet users showed some reluctance, even fear, when it came to providing personal information on the Internet. These data are nevertheless essential crops for marketing departments of companies, which then allow them to respond to consumer needs, including the provision of targeted offers, generally appreciated [18]. This is what [19] call the "personalization/privacy" paradox: the need to find solutions.

Our study provides a useful tool for measuring where the fears of social network users lie regarding the security of their data on these platforms - which make up one inexhaustible reservoir - but also the behavior they adopt accordingly. In particular, the scale could discriminate between groups who differ in their level of privacy concerns. However, further evidence of the validity of the scale is required.

It appears to be necessary for users to understand how people protect themselves and want to be protected on social networks in order to reassure users and meet their expectations. The underlying question of data protection is primarily tied up with the effectiveness of companies' digital strategies and how these can be evaluated. This is not

only the animation of communities around brands, but also the maximization of information systems' privacy protection.

Our survey reveals a willingness of Internet users to have more information about the privacy policies of their social networks. To date, this need has been identified by some e-commerce websites, who offer increasing representation of their privacy protection policy, in which they explain in particular their use of cookies, or data navigation. For example, Facebook improved its website, enabling users to be guided in adjusting the privacy settings. This would allow for a better perception of users' feelings when they use social networks, and in turn this would facilitate the study of the impact of this parameter on users' behavior.

Finally, it would be interesting to link content sharing habits and issues with the level of information. In other words, it would be pertinent to know how the level of information accessible to social network users - possibly improved by means of tutorials such as those we propose - impacts on the behavior of these users when they navigate these sites. As a limitation of this study, focusing the exploratory analysis on French students only might be too restrictive.

Appendix 1. Sample of Respondents

Variables		France (n = 368)	USA (n = 205)
Gender	Male	42.10%	33.2%
	Female	57.90%	66.8%
Age	<25 years old	56%	75.1%
	25 to 34 years old	28%	17.1%
	>35 years old	16%	7.8%
What kind of information about yourself do you provide these social networks with?	Gender	Yes (36.4%) No (63.6%)	Yes (77.1%) No (22.9%)
	Relationship status	Yes (81.8%) No (18.2%)	Yes (31.7%) No (68.3%)
	Date of birth	Yes (22.6%) No (77.4%)	Yes (28.3%) No (71.7%)
	City of birth	Yes (15.8%) No (84.2%)	Yes (80.5%) No (19.5%)
	Political views	Yes (18.2%) No (81.8%)	Yes (64.9%) No (35.1%)
	Religious views	Yes (35.6%) No (64.4%)	Yes (15.1%) No (84.9%)
	E-mail	Yes (26.1%) No (73.9%)	Yes (20.5%) No (79.5%)
	Phone number	Yes (78%) No (22%)	Yes (15.8%) No (84.2%)

References

1. Churchill Jr., G.A.: A paradigm for developing better measures of marketing constructs. JMR **16**, 64 (1979)
2. Statista: Age distribution of active social media users worldwide as of 3rd quarter 2014 (2016). https://www.statista.com/statistics/274829/age-distribution-of-active-social-media-users-worldwide-by-platform/. Accessed 22 Nov 2016
3. Dinev, T.: Why would we care about privacy? EJIS **23**(2), 97–102 (2014)
4. Buchanan, T., Paine, C., Joinson, A.N., Reips, U.-.D.: Development of measures of online privacy concern and protection for use on the internet. JASIST **58**(2), 157–165 (2007)
5. Benson, V., Saridakis, G., Tennakoon, H.: Information disclosure of social media users: does control over personal information, user awareness and security notices matter? ITP **28**(3), 426–441 (2015)
6. Dinev, T., McConnell, A.R., Smith, H.J.: Informing Privacy Research through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "Apco" Box, ISR (2016, forthcoming)
7. Bélanger, F., Crossler, R.E.: Privacy in the digital age: a review of information privacy research in information systems. MISQ **35**(4), 1017–1041 (2011)
8. Pavlou, P.A.: State of the information privacy literature: where are we now and where should we go? MISQ **35**(4), 977–988 (2011)
9. Smith, H.J., Dinev, T., Xu, H.: Information privacy research: an interdisciplinary review. MISQ **35**(4), 989–1015 (2011)
10. Lee, D.J., Ahn, J.H.: Managing consumer privacy concerns in personalization: a strategic analysis of privacy protection. MISQ **35**, 423–444 (2011)
11. Dinev, T., Hart, P.: Privacy concerns and levels of information exchange: an empirical investigation of intended e-services use. ESJ **4**(3), 25–61 (2007)
12. Laufer, R.S., Wolfe, M.: Privacy as a concept and a social issue: a multidimensional developmental theory. JSI **33**(3), 22–42 (1977)
13. Serenko, N.: Informational, physical, and psychological privacy as determinants of patient behaviour in health care. In: Handbook of Research on Patient Safety and Quality Care through Health Informatics. IGI Global Publications (2014). doi:10.4018/978-1-4666-4546-2.ch001
14. Dinev, T., Albano, V., Xu, H., D'Atri, A., Hart, P.: Individual's attitudes towards electronic health records – a privacy calculus perspective. AIS (2015, forthcoming)
15. Aggarwal, P., Vaidyanathan, R., Castleberry, S.: Managerial and public attitudes toward ethics in marketing research. JBE **109**, 463–481 (2012)
16. Kaplan, A.M., Haenlein, M.: Users of the world, unite! The challenges and opportunities of social media. BH **53**(1), 59–68 (2010)
17. Ganassali, S.: Faire Parler les Mots: vers un Cadre Méthodologique pour l'Analyse Thématique des Réponses aux Questions Ouvertes. DM **51**, 55–67 (2008)
18. Liu, C., Marchewka, J.T., Lu, J., Yu, C.S.: Beyond concern - a privacy-trust behavioral intention model of electronic commerce. IM **42**, 289–304 (2005)
19. Sutanto, J., Palme, E., Tan, C.H., Phang, C.W.: Addressing the personalization privacy paradox: an empirical assessment from a field experiment on smartphone users. MISQ **37**, 1141–1164 (2013)