2020

Paradoxical Behaviour in Social Media Usage

Ruben Post

Sebstiaan Wiewel

Brian Jansen

Stijn Kaas

PARADOXICAL BEHAVIOUR IN SOCIAL MEDIA USAGE

RUBEN POST[1], SEBSTIAAN WIEWEL[2], BRIAN JANSEN[2] & STIJN KAS[1]

[1] HU University of Applied Sciences Utrecht, Institute for ICT, Utrecht, The Netherlands, e-mail: ruben.post@hu.nl, stijn.kas@hu.nl
[2] Utrecht University, Faculty of Science, Utrecht, The Netherlands, e-mail: s.o.wiewel@students.uu.nl, b.n.janssen@students.uu.nl

Abstract The Privacy Paradox is a recently emerged phenomenon. It looks at a person's intention to disclose information and the actual disclosure of information. In this research, we look at the extent of the relationship between the social media behaviour of a student and their attitude towards privacy. With these results, we can conclude whether they show paradoxical behaviour. These results are derived from a questionnaire among information technology students (n=126) and analyzed to extract the extent of the relationships between certain variables. The data analysis showed significant relationships between several variables, none of which indicated paradoxical behaviour among the population. However, it did give way to various interesting relationships. The results indicate paradoxical behaviour to a certain extent, specifically with regards to social media use self-disclosure and information and privacy concerns and privacy settings. Additionally, the research indicates that the higher the educational background of the participant, the less likely they are to exhibit paradoxical behaviour.

Keywords: online privacy, social media, paradoxical behavior, research paper, Bled eConference.

University of Maribor Press

DOI https://doi.org/10.18690/978-961-286-362-3.27
ISBN 978-961-286-362-3

1 Introduction

In recent years, privacy has become an increasingly influential factor in consumer decision making (Necley, 2017; Lahlou, 2008). Societal behaviour has become aware of the damage privacy-compromising applications, operating systems, and websites can inflict. However, this also introduced paradoxical behaviour. Specifically, society has a tendency towards privacy-compromising actions which results in a dichotomy between privacy attitudes and actual behavior (Acquisti, 2004). This phenomenon has been dubbed "The Privacy Paradox" (Norberg, Horne, & Horne, 2007; Barnes, 2006).

The need for privacy is becoming increasingly prevalent in our daily lives (Finn & Wright, 2016). However, some seem to value it less than others (Kokolakis, 2017; Dienlin & Trepte, 2015). Additionally, the amount of information that is being collected is increasing also (Hargittai & Marwick, 2016). This might indicate paradoxical behaviour. Therefore, the objective of this study is to measure whether students allow for paradoxical behavior showing in their intentions to limit disclosure and the actual personal details they provide on social media. This problem statement leads to the following exploratory research questions:

RQ1: What is the relationship between social media behaviour and the attitude towards privacy?
RQ2: To what extent does social media behavior and the attitude towards privacy vary between educational groups?

To answer these questions, the results of a questionnaire reporting on the individual's social media behavior and attitude towards privacy are analysed. In turn, from a practical perspective, users of social media should be made aware of their potential contradictory behaviour. From a scientific perspective, literature suggests a need for insight and further research into the phenomenon of the privacy paradox (Necley, 2017; Norberg et al., 2007).

The next section discusses the current state of the research field regarding privacy paradoxical behaviour and the relation of educational groups and privacy awareness. After this, the research method, including the explanation and grounding of the measured variables is described. Next, the results of the research are presented and

elaborated through various visualizations. The last section presents the conclusions and discusses the utilized research method and results of the research, followed by possible directions for future research.

2 Background and related work

To answer the research question several subjects are discussed. The current state of these subjects is discussed along with their relationship to this research.

2.1 Online privacy

Society is spending more time online than at any point in history (Huang, 2017; Nie & Erbring, 2002). With over 7.4 billion internet users, most spending more than 10 hours a week online, online privacy has become as important in our daily lives as offline privacy (Huang, 2017; Nie & Erbring, 2002). The definition of privacy is ambiguous and often difficult to conceptualize (Warren & Brandeis, 1890; Martin, 2016). Hence, it is difficult to derive a definition of online privacy. Due to the relative importance of this definition, this research defines a stipulative definition of a constituent of privacy, namely online privacy, for practical purposes. In this research, online privacy is defined as encompassing the handling of data generated by all user-generated online activity.

In recent years, online privacy has been subject to scrutiny by journalists due to increasing awareness and events that reflect badly on the perception of online privacy (Cadwalladr & Graham-Harrison, 2018; Steel & Fowler, 2010). This scrutiny gave way to increased online privacy concern and awareness among internet users (Antón, Earp, & Young, 2010).

2.2 Social media behaviour

Social media is an industry inherently intertwined with online privacy. However, social media has also becomes intertwined in society, with more than 50% of American adults using social media (Perrin, 2015). However, online behaviour indicates a lack of concern for privacy. The results of Perrin (Perrin, 2015) indicate that internet users have become less concerned with how their personally identifiable data is used. Research of Obar and Oeldorf-Hirsch provide context to these results

by indicating that 99% of social media users (which are also part of the internet users population) accept the privacy policy and terms of services without reading them (Obar & Oeldorf-Hirsch, 2018). When social media behaviour is put in the context of the recent scrutiny surrounding online privacy, it indicates a paradoxical trend. This trend has been dubbed "the privacy paradox" (Barnes, 2006; Norberg et al., 2007).

2.3 Privacy paradox

As privacy awareness increases in our society, we are faced with a difficult and ambiguous challenge. With the introduction of social media, privacy got induced in a previously unknown avenue. This new avenue gave way to services without monetary costs associated with them. However, the price is paid in personal data which is (mis)used by the organizations that exploit these social media platforms (Lomborg & Bechmann, 2014).

This introduction gave society access to free services, and the organizations exploiting these services access to data. In turn, society was faced with a question: How far will you go to make use of these free services? This is where the privacy paradox is introduced: a person might say they value privacy while giving away their data to make use of these services (Barnes, 2006; Norberg et al., 2007). For example, a person may have many concerns about companies always knowing where they are based on geographical data, but also frequently upload geographically-tagged social media posts. This is called paradoxical behaviour. This paradoxical behaviour could lead to uninformed consumers and misuse by organizations.

Current research on the privacy paradox indicates that the privacy paradox is not a symptom of youth, but rather concerns people of all ages (Kokolakis, 2017). It should also be noted that this research only regards social media, but the privacy paradox is prevalent in all industries dealing with personal information (Kokolakis, 2017; Schmitz, 2005).

2.4 Educational based privacy awareness

As previously mentioned, the privacy paradox concerns all ages, and therefore all educational groups (Kokolakis, 2017). Different educational groups might have varying attitudes towards privacy or different social media use. For example, these groups might have trouble reading the privacy terms (Hong, Patrick, & Gillis, 2008). Of course, this would be an extreme case. But on a wider scale, groups are affected by their intelligence, as it relates to context awareness and ability to selfregulate, which in turn influences their attitude towards privacy (Baatarjav, Dantu, & Phithakkitnukoon, 2008).

3 Method

The research method is chosen based on the problem statement of this research. Since the problem statement is addressed through hypothesis, a survey is an appropriate research method (Van Dun, Hicks, & Wilderom, 2017).

3.1 Data collection

In order to answer the research questions, a questionnaire is used. The questionnaire can be requested from the authors. The questionnaire offers benefits such as being able to reach a large group of people and offering structured data that can be used in the quantitative analysis. In this questionnaire, participants were asked to rate different statements, which are defined by the variables, on a Likert Scale. For this study a Likert Scale from 1 to 5 was chosen (Joshi, Kale, Chandel, & Pal, 2015; Dawes, 2008). Additionally, with regards to the validity of the questionnaire, by grounding the independent and dependent variables in previous research, the external validity of the questionnaire is increased.

The questionnaire is distributed through web-based sharing. This choice should not affect the results of our research, but given the time span of the research, it was the most feasible solution. The questionnaire was distributed in the network of the researchers, whilst being limited to students of the Utrecht Utrecht and HU University of Applied Sciences Utrecht. The questionnaire was anonymous and no personally identifiable data was included.

3.1.1 Demographics

The participants are gathered using convenience sampling in which the researchers arbitrarily asked information science students from the Utrecht University as well as HU University of Applied Science Utrecht to participate. Hence, the students of these universities formed the sample and unit of analysis and students of Dutch universities our population. As for the sampling method, convenience sampling is a method often used for research that is applicable to a wide population (Etikan, Musa, & Alkassim, 2016). A total of 126 participants of average age 24.5 answered the questionnaire where 65.9% of the respondents are male (*n=83*) and 34.1% female (*n=43*) across four educational groups. Each participant was asked their gender, age, and education level.

3.2 Independent variables

The questionnaire measured four independent variables: social media use, privacy settings, privacy concerns, and self-disclosure of information. These variables are used to describe how much the participant values their privacy and how much privacy they give up to use certain social media features.

Social media use is measured with a scale developed by Leigh Young & Quan-Haase (Young & Quan-Haase, 2013). The first item asked, "How often do you visit social media applications/websites?" the second item asked, "On average, how much time do you spend on social media?" the third item asked, "How many social media friends/followers do you have?" the fourth item asked, "How many of your social media friends/followers do you consider close friends?" and the fifth and final item asked "How often do you post something on social media?". Participants were asked to rate each question in a category on a scale from 1 through 5.

Self-disclosure of information indicates the extent to which the participant agrees with statements related to the disclosure of information on social media and is developed by both Chen (Chen, 2018) and Taddicken (Taddicken, 2014). The first item asked, "I like to share my personal feelings." the second item asked "When I have something to say, I like to share it on social media.", the third item asked "I always find time to keep my profile up-to-date." the fourth item asked "I keep my friends updated about what is going on in my life.", and the fifth and final item asked

"I often geotag my location.". Participants were asked to score the questions from 1 "Not at all" to 5 "Very often".

Privacy setting measures to what extent people withdraw their information (i.e., limiting profile visibility) and set boundaries about with whom they would like to share personal information (i.e., friending) in order to stay private (Chen, 2018). it also measured with a scale developed by Leigh Young & Quan-Haase (Taddicken, 2014). The privacy settings of a participant are described by their profile and information visibility. The first item asked "Who can view your profile?" and "Have you made any changes to your privacy settings since creating your social media account?". Participants were asked to identify who can view their profile (from "Nobody" to "Everybody") and whether they changed their privacy settings (yes/no).

Privacy concern indicates to which extent participants are concerned about the following when using social media and is developed by Chen (Chen, 2018). The first item asked, "The information I submit on social media could be misused." item two asked, "A person can find private information about me on social media." item three asked, "Submitting information on social media, because of what others might do with it." and the fourth and final item asked
"Submitting information on social media, because it could be used in a way I did not foresee.". Participants were asked to score the questions from 1 "not at all concerned" to 5 "very concerned".

The variables **social media use** and **self-disclosure of information** form the facet "Social media behaviour" and privacy settings and privacy concern form the facet "Attitude towards privacy". This is done by averaging the scores of the participant. These facets are used to answer the research questions.

3.3 Independent variables

The dependent variables for this research are the highest level of education of the participants. The participants were asked to identify their highest level of education at the beginning of the questionnaire. As mentioned in the background and related work, the educational background of a responded might have a relation with the attitude towards privacy, which in turn could affect certain relationships between the

independent variables (Baatarjav et al., 2008; Hong et al., 2008; Kokolakis, 2017). The four education groups are high school, Bachelor (WO), Higher Vocational Education (HBO), and Masters (WO).

3.4 Hypotheses

The following hypotheses are stated:

Hypothesis 1: Social media use negatively affect Self-disclosure of information.

This hypothesis supports RQ1 because it a negative relationship would indicate paradoxical behaviour (i.e. the more a person uses social media, the less information they disclose).

Hypothesis 2: Privacy concerns negatively affects privacy settings.

A negative effect on privacy settings means increasing the information withdrawal set by these settings, i.e. having stricter and more privacy secure settings. This hypothesis supports RQ1 because a negative relationship would indicate paradoxical behaviour (e.g. the more privacy concerns a person has, the more information they give away by not adjusting their privacy settings).

Hypothesis 3: Social media behavior significantly affect attitude towards privacy across the full sample.

The first two hypotheses (H1 and H2) are used as a baseline in order to answer H3, which measures the paradoxical behaviour. These variables are used in previous research, which indicated relations between them (Necley, 2017; Barnes, 2006). H3 allows us to answer RQ1.

Hypothesis 4: Social media behavior significantly affects attitude towards privacy differently between the various educational groups.

The educational groups are the dependent variable because previous research indicated a difference in the attitude towards privacy among different educational backgrounds (Necley, 2017; Barnes, 2006). H4 allows us to answer RQ2.

4 Data analysis

After the data collection, the data was anonymously stored and analysed by the researchers using R, Python, and SPSS. The anonymous data can be requested from the researchers, as it cannot be placed in a appendix due to its size.

4.1 Data preparation

All questions in the questionnaire were mandatory, meaning there were no null-values. To be able to analyse the data, the question "Have you made any changes to your privacy settings since creating your social media account?" has been transformed from the scale "Yes/No" to "1 through 5", with yes representing 5 and no representing 1. The internal validity of the questionnaire varied between variables. The social media use sub-scale consisted of three items ($a = .74$), with "How many of your social media friends/followers do you consider close friends?" being dropped, The self-disclosure of information sub-scale consisted of four items ($a = .67$), the privacy setting sub-scale consisted of two items ($a = .64$), and the privacy concern sub-scale consisted of four items ($a = .86$).

4.2 Statistical tests

To answer hypotheses H1, H2, and H3, correlation is an appropriate test because the hypothesis suggest a relationship between variables. H1 looks for a negative relationship between social media use and self-disclosure of information, H2 looks for a negative relationship between privacy concerns and privacy settings, and H3 looks for any effect between social media behaviour and attitude towards privacy.
Social media use and self-disclosure of information are significantly correlated ($r = .41, p \leq .0001$). Therefore, H1 is accepted. Privacy setting and privacy concern are significantly correlated ($r = -0.29, p \leq .001$). Therefore, H2 is accepted. There was a non-significant correlation ($r = -0.02, p = n.s.$) between social media behaviour and attitude towards privacy. Therefore, H3 is not accepted.

H4 was answered using a Multivariate analysis of variance in the form of Pillai's trace because the assumption of homogeneity of variance- covariance is violated in the data. H4 looks for a difference between the effect of social media behaviour and attitude towards privacy between four educational groups. The multivariate result was significant, (Pillai's Trace = .07, F = .22, df = (2), p = .01), indicating a significant difference in social media behavior and attitude towards privacy between High school and Bachelor (WO) graduates. Additionally, the multivariate result was significant, (Pillai's T race = .11, F = 4.25, df = (2), p = .05), indicating a difference in social media behavior and attitude towards privacy between Higher Vocational Education (HBO) and Bachelor (WO) graduates. Lastly, the multivariate result was significant, (Pillai's Trace = .09, F = 2.78, df = (2), p = .01), indicating a difference in social media behavior between Higher Vocational Education (HBO) and Masters (WO) graduates. Based on these tests, H4 is accepted.

5 Results

In sum, the research found two significant relationships. The data analysis accepts both H1 and H2, indicating that the more a person uses social media, the less information they disclose and the more privacy concerns a person has, the more information they give away by not adjusting their privacy settings. These results are especially interesting because by accepting H1 and H2, the research indicates paradoxical behaviour (e.g., the participants say that are worried about the misuse of their data, but do not adjust their privacy settings to reflect this concern). However, by accepting H1, this research does not indicate a significant relation between social media behaviour and attitude towards privacy. Therefore, this research can conclude that the privacy paradoxical behaviour is evident in the sample, but not to the full extent that has been hypothesized. H3 was rejected, indicating that there is no significant correlation between social media behaviour and attitude towards privacy. Additionally, H4 was accepted, indicating that participants with a higher educational background show less paradoxical behaviour with regards to privacy. It should be noted that the nature of the data can only answer the hypotheses. It cannot conclude a causal relationship between the aforementioned variables.

6 Conclusion

During this research, we aimed to find an answer RQ1: **"What is the relationship between social media behaviour and the attitude towards privacy?"** To answer this question, 126 participants filled in a questionnaire. The data these questionnaires provided has been analysed to conclude that there is a non- statistical relationship between social media behaviour and the attitude towards privacy. Additionally, the data was used to answer RQ2: **"To what extent does social media behavior and the attitude towards privacy vary between educational groups?"** The data analysis concluded that the higher a participants educational background, the less likely they were to exhibit paradoxical behaviour.

With regards to previous research, this research confirms the results of both Norberg and Horne (2007) and Young and Quan-Haase (2013) to a certain extent. It confirms the existence of paradoxical behaviour, but does not show a significant relation between the variables measured in the stated previous research (see results of H3). This might be due to the limitation of this research (see section 6), but could have other reasons unknown to the authors.

From a practical perspective, the results of this questionnaire could provide educational material for policymakers regarding privacy and security law. From a scientific perspective, this research adds to the body of knowledge regarding privacy-related behaviour.

7 Limitations and future research

The research has several limitations. First, regarding the sample, all participants are following courses that have information technology as a focal point. This could mean that the students could be biased towards the potential danger of information technology. Even though the internal reliability of the questions was acceptable, generalizing the statistics to the population might not be feasible. However, to conclude the effect this might have had, future research should be done that includes other courses that do not have information technology as a vocal point.

Second, regarding the sample size, the study has a total sample size of 126. This is regarded as a high enough sample to conclude potentially statistical significant relations. However, a higher sample size could show various other significant relations between the variables and educational groups. Specifically, the increasing the sample size per educational group could provide additional insight, as a larger sample size may have indicated additional significant differences.

Furthermore, future research should consider reproducing this research with a different sample and a potentially bigger sample size. Additionally, future research could focus on the effects of privacy paradoxical behaviour among students and whether it opens them up for potential dangers. This could provide useful insight for policymakers and increase the awareness of the importance of online privacy among students as well as all internet users.

References

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. In Proceedings of the 5th acm conference on electronic commerce (p. 21-29). ACM.

Antón, A. I., Earp, J. B., & Young, J. D. (2010). How internet users' privacy concerns have evolved since 2002. IEEE Security & Privacy, 8(1), 21–27.

Baatarjav, E.A., Dantu, R., & Phithakkitnukoon, S. (2008). Privacy management for facebook. In International conference on information systems security (pp. 273–286).

Barnes, S. B. (2006). A privacy paradox: Social networking in the united states. First Monday, 11(9).

Cadwalladr, C., & Graham-Harrison, E. (2018). Revealed: 50 million facebook profiles harvested for cambridge analytica in major data breach. The Guardian, 17, 22.

Chen, H.T. (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, 62(10), 1392-1412.

Dawes, J. (2008). Do data characteristics change according to the number of scale points used? International journal of market research, 50(1), 61-77. Retrieved from http://www.econis.eu/PPNSET?PPN=568721721

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? an in-depth analysis of privacy attitudes and privacy behaviors. European journal of social psychology, 45(3), 285–297.

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. American journal of theoretical and applied statistics, 5(1), 1–4.

Finn, R. L., & Wright, D. (2016). Privacy, data protection and ethics for civil drone practice: A survey of industry, regulators and civil society organisations. Computer Law & Security Review, 32(4), 577–586.

Hargittai, E., & Marwick, A. (2016). "what can i really do?" explaining the privacy paradox with online apathy. International Journal of Communication, 10, 21.

Huang, C. (2017). Time spent on social network sites and psychological well-being: A meta-analysis. Cyberpsychology, Behavior, and Social Networking, 20(6), 346-354.

Hong, Y., Patrick, T. B., & Gillis, R. (2008). Protection of patient's privacy and data security in e-health services. In 2008 international conference on biomedical engineering and informatics (Vol. 1, pp. 643–647).

Joshi, A., Kale, S., Chandel, S., & Pal, D. (2015, Jan 10,). Likert scale: Explored and explained. British Journal of Applied Science & Technology , 7 (4), 396- 403. doi: https://doi.org/10.9734/BJAST/2015/14975

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of cur- rent research on the privacy paradox phenomenon. Computers & security, 64, 122–134.

Lahlou, S. (2008). Identity, social status, privacy and face-keeping in digital society. Social science information, 47(3), 299-330.

Lomborg, S., & Bechmann, A. (2014). Using apis for data collection on social media. The Information Society, 30(4), 256–265.

Martin, K. (2016). Understanding privacy online: Development of a social contract approach to privacy. Journal of Business Ethics, 137(3), 551–569.

Necley, G. (2017). Philosophical views on the value of privacy. In (p. 3-9). Routledge.

Nie, N. H., & Erbring, L. (2002). Internet and society: A preliminary report. 10 IT & society, 1(1), 275–283.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of consumer affairs, 41(1), 100–126.

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

Perrin, A. (2015). Social media usage: 2005-2015. Pew research center, 52–68. Schmitz, A. J. (2005). Untangling the privacy paradox in arbitration. U. Kan.

L. Rev., Steel, E., & Fowler, G. (2010). Facebook in privacy breach. The Wall Street Journal, 18(1)

Taddicken, M. (2014). The 'privacy paradox'in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. Journal of Computer-Mediated Communication, 19(2), 248-273.

Van Dun, D. H., Hicks, J. N., & Wilderom, C. P. (2017). Values and behaviors of effective lean managers: Mixed-methods exploratory research. European management journal, 35(2), 174–186.

Warren, S. D., & Brandeis, L. D. (1890). Right to privacy. Harv. L. Rev., 4, 193.

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on facebook: The internet privacy paradox revisited. Information, Communication & Society, 16(4), 479-500.