# A Discrepancy between Objective and Perceived Privacy Risks? Understanding Messaging Service's Discontinuance Usage

Verena Kessler Verzar
*University of Augsburg*, verena.kesslerverzar@uni-a.de

Adeline Frenzel-Piasentin
*University of Augsburg*, adeline.frenzel@uni-a.de

Daniel Veit
*University of Augsburg*, daniel.veit@uni-a.de

# A Discrepancy between Objective and Perceived Privacy Risks? Understanding Messaging Service's Discontinuance Usage

Verena Kessler Verzar[1], Adeline Frenzel-Piasentin[1], and Daniel J. Veit[1]

[1] University of Augsburg, Augsburg, Germany
{verena.kesslerverzar,adeline.frenzel,daniel.veit}@uni-a.de

**Abstract.** The number of users discontinuing messaging services due to perceived privacy risks has grown rapidly in recent months. Still, research on privacy risks in this context has not received much attention. We aim to examine the impact of objective and perceived privacy risks on discontinuance usage. To determine the level of objective privacy risks, we analyze the privacy policy of the messaging service WhatsApp. So far, we identify aggregation, secondary use, identification, and increased accessibility to be the most prevalent objective risks. We propose a longitudinal design to capture individuals' perceived privacy risks and test the influence of both risk dimensions on the discontinued use of messaging services. We contribute to literature by disentangling the interplay of objective and perceived privacy risks on discontinuance.

**Keywords:** Privacy risks, perceived risks, objective risks, discontinuance usage

## 1 Introduction

Privacy as a human right receives increasing attention due to fast technological developments [1]. The opportunity to collect an immense amount of data about every individual using digital technologies gives rise to customers being more aware of potential privacy risks [2], [3]. Such perceived privacy risks include the usage of social networking sites (SNS) and messaging services (MS), e.g., WhatsApp, Telegram, or Signal [4]. Recently, the update of WhatsApp's privacy policy and terms of use led to critics, and to tens of millions of users switching to other MS [5], [6]. However, in many cases the discontinuance has been sparked by an increase in perceived privacy risks whereas the actual objective privacy risks of using WhatsApp remain about the same [7].

In information systems (IS) research, these two dimensions of privacy risks, namely perceived and objective, have been investigated in the past. Various studies on perceived privacy risks captured people's individual conception of risk [8]–[10]. Objective privacy risk in contrast is based on verifiable facts, for example a company's data practices or browser privacy settings [11]. Extant literature also acknowledges the fact that objective and perceived levels of privacy risks may significantly differ from

17th International Conference on Wirtschaftsinformatik,
February 2022, Nürnberg, Germany

each other [12]. The relationship between individuals' privacy risk perceptions and perceived benefits, the so-called *privacy calculus* [13], and its influence on usage behavior has been studied in privacy literature [9], [14], [15]. These studies exhibit mixed findings leading to further research focusing on the *privacy paradox*: the deviation of privacy attitudes and actual behavior [16]. However, most studies only focus on perceived privacy risks but fail to investigate the impact of the discrepancy between objective and perceived privacy risks on the discontinuance usage. The aim of this study is thus to identify the levels of objective and perceived privacy risk and to assess the impact of both risk dimensions on users' actual discontinuance usage. Hence, we pose the following research questions:

*(1) How do objective and perceived privacy risks of MS interact and (2) how do objective and perceived privacy risks influence users' discontinuance usage?*

Exploring this question is critical for several reasons. First, although objective as well as perceived privacy risks have been studied separately, the interaction of these two risk dimensions remains unknown. Second, it is unclear how the interplay of objective and perceived privacy risks impacts the discontinuance usage of individuals. To respond to our research question, we conduct a longitudinal field survey. We expect to extend the understanding of privacy risks as drivers of discontinuance usage. Practitioners will know how objective and perceived privacy risks interact, differ, or correspond, and how they can improve transparency of privacy policies.

## 2 Theoretical Foundation

### Privacy Risks

Objective privacy risks are generally verifiable, as they are based on facts that can be found in the real world. Unlike perceived risks, objective privacy risks are not influenced by individual judgement [14]. Internet browser settings, privacy regulations and a company's data practices may be potential sources of objective privacy risks [11]. Prior research has shown that individuals react to differences in objective privacy risks, e.g., in the form of different privacy settings [11], [13]. Perceived risks on the other hand can be described as an individual's perception of the unpredictable outcome of participating in an activity. In a digital environment it can be understood as the degree to which a person thinks the usage of an IS is insecure and may lead to undesired consequences [17], [18]. While an individual's risk perception can be evaluated based on scales [19], other approaches are needed to be able to judge the objective dimension of risk.

In order to assess the level of objective privacy risks in this study, we adapt an existing taxonomy with potential categories of risk. We use the taxonomy of privacy by Solove [20] as foundation as it provides a comprehensive understanding of privacy and clearly defines distinct categories and subcategories of potential privacy risks. Moreover, Solove's taxonomy have served as a fundament to understand the concept of privacy

and its dimensions in previous IS literature [1], [12], [21]. We extend this fundamental taxonomy by technical aspects [22]. Solove's taxonomy consists of three main categories that represent actions with potential privacy risks, namely *information collection*, *information processing* and *information dissemination* [20]. Each of these categories consists of multiple subcategories which will be used to assess the objective privacy risks. Detailed definitions can be found in Solove and Kanwal [20], [22].

**Research Model**

We develop a research model to provide a better understanding of the relationship between privacy risks and discontinuance usage (see Figure 1). A large stream of literature focuses on IS usage and continuance behaviors [23]. In accordance with the privacy calculus, weighing the costs of IS usage with expected benefits, privacy risks negatively impact continuous behavioral aspects [24]–[26]. For a long time, low levels of continuance behaviors were assumed to be congruent with high levels of discontinuance and vice versa [26]. However, more recently research views discontinuous usage as an independent construct. Still, it is likely, but not necessary that continuance and discontinuance use share the same predictors [27]–[29]. To this point, we focus our study on the relationship between privacy risks and discontinued usage (and regard perceived benefits as control variable); thus, we hypothesize:

*Hypothesis 1. Privacy risks positively influence user's discontinuance usage.*

We aim to investigate the relationship between privacy risks and discontinuance use in more detail by taking the interplay of objective and perceived privacy risk into account. Both dimensions have been studied separately in the past [11], [30], but literature has shown that the objective and perceived level of risk may be significantly disparate [12]. Hence, the difference between these two dimensions may play a role when evaluating the impact of privacy risk on discontinuance usage. This view is grounded in behavioral perspectives of the privacy paradox according to which users deviate from normative privacy-calculus based accounts due to limitations such as knowledge deficiency or cognitive biases [11]. Therefore, only if an individual's risk perceptions are higher than the objective risks (e.g., due to incomplete information), this individual will discontinue IS usage. Hence, the hypothesis of privacy risks positively influencing discontinuance usage is not generalizable. Based on this, we conclude our remaining hypotheses as follows:

*Hypothesis 2a. If a user's perceived privacy risks are higher than the objective risks, privacy risks positively influence user's discontinuance usage.*

*Hypothesis 2b. If a user's perceived privacy risks correspond to the objective risks, privacy risks negatively influence user's discontinuance usage.*

*Hypothesis 2c. If a user's perceived privacy risks are lower than the objective risks, privacy risks negatively influence user's discontinuance usage.*

As a first step, we determine objective privacy risks. Our methodology will be outlined in the following.

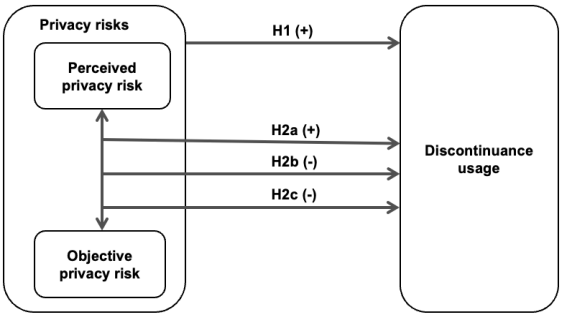


**Figure 1.** Research model

## 3 Methodology

In order to test our hypotheses and answer our research question we first need to assess the level of objective risks of MS. We choose a particular MS, namely WhatsApp, to identify objective risks. The most important source for our study is WhatsApp's privacy policy which outlines the company's data collection, processing, and usage practices. Additionally, the privacy policy describes WhatsApp's privacy preserving measures and is thus a solid basis for our analysis. In this study, we refer to the privacy policy which was last amended on January 4th, 2021 and applies to the European area [31]. As additional sources for our objective privacy risk analysis, we use two help center entries from WhatsApp's website [32], [33], because they are necessary to understand the content of the privacy policy in order to be able to judge the level of objective privacy risk.

For our objective risk analysis, we apply the Q-sort method as it is a common approach for the systematic study of individual viewpoints with the goal of achieving a generalizable understanding [34], [35]. So far, we conducted one round of sorting with a total of 13 judges (4 researchers, 8 students, and 1 practitioner). For this, we divided the privacy policy into three equally long sections, that were sorted by three different judges each. The fourth group of three judges analyzed the included help center articles. The first author was additionally part of all four sorting groups, so that every section of the privacy policy and help center entry was sorted by four judges in total. When we assigned the judges to their respective groups, we ensured the broadest possible distribution of gender and educational background.

To perform the sorting, each judge was provided with the privacy policy section or help center entries that were to be sorted. In addition, the judges received a set of standard instructions along with the definitions of each individual subcategory of the privacy taxonomy. The judges were instructed to familiarize themselves with these definitions

and match them with the text passages where they find evidence for the corresponding privacy risk.

## 4 First Results and Outlook

To identify the most relevant categories of objective risk of WhatsApp, we determine how often each subcategory of risk was placed by our judges in relation to the maximum possible number of placements per dimension. The average relative placement over all subcategories was at 18.11%. Based on this, the most prevalent risk subcategories are *aggregation* at 35.13% relative placement, *secondary use* scoring 30.06% and *identification* as well as *increased accessibility* both at 29.11%. These are the risks our judges found the most evidence for in WhatsApp's privacy policy and help center entries. Moreover, *surveillance* and *exclusion* are above average relative placement, at 26.27% and 24.05% respectively. Below the average relative placement were hence appropriation at 13.92%, disclosure scoring 11.08%, breach of confidentiality at 10.44%, insecurity with 8.86% relative placement, other privacy techniques at 6.65% and interrogation as well as cryptographic techniques both scoring 5.38%. These subcategories are thus less relevant regarding objective risk.

In our first round of sorting, we reach an average inter-judge raw agreement of 82.14%. Consequently, our results exhibit decent validity. To further increase the reliability, we will perform a second round of sorting. For this, we will ask the same judges to participate, but they will each be provided a different section of the privacy policy or help center articles than in the first round. In addition, we will exclude some risk subcategories that exhibited a low average relative placement score.

In order to assess our two hypotheses and the level of perceived privacy risk, we will conduct a longitudinal online field survey among MS users with four collection points (t0, t1, t2, t3), the initial start as well as surveys after 3, 6 and 12 months. Thereby, we will not only include WhatsApp but consider the usage of other MS as well as SNS and potentially assess their objective risks, too. To measure individuals' privacy risk perceptions, we will use a 9-point Likert scale based on Xu et al. [19] and Malhotra et al. [30]. We will adopt additional measurement items [25], [29] to capture users' discontinuance usage of MS. Furthermore, we will collect other variables relevant to the privacy context, such as perceived benefits [10], intention to discontinuance [29], herding [36], and perceived usefulness [28]. After assessing their perceptions of risk, we will compare participants' answers with our objective risk assessment resulting from Q-sort. Finally, we will collect control variables such user's disposition to value privacy [37].

We expect to contribute to privacy literature by disentangling the interplay of objective and perceived privacy risks on discontinuance in order to explain why users deviate from normative accounts of privacy-related behavior. From a practical perspective, we expect to provide an understanding of the discrepancy between objective and perceived privacy risks.

## References


1. Bélanger, F., Crossler R.E.: Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. MIS Quarterly 35, 1017–1041 (2011)
2. McKinsey & Comapany, https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative (Accessed: 31.08.2021)
3. Forbes, https://www.forbes.com/sites/forbestechcouncil/2020/12/14/the-rising-concern-around-consumer-data-and-privacy/?sh=70391675487e (Accessed: 31.08.2021)
4. Userlike, https://www.userlike.com/en/blog/messaging-data-privacy-survey (Accessed: 31.08.2021)
5. Business Insider, https://www.businessinsider.com/whatsapp-privacy-policy-delay-three-months-2021-1 (Accessed: 31.08.2021)
6. Forbes, https://www.forbes.com/sites/zakdoffman/2021/01/19/if-you-quit-whatsapp-for-imessage-signal-or-telegram-beware-this-dangerous-mistake/?sh=5a0377322cd9 (Accessed: 31.08.2021)
7. Tech Advisor, https://www.techadvisor.com/news/social-networks/whatsapp-facebook-data-sharing-3800374/ (Accessed: 31.08.2021)
8. Buckman, J.R.,Bockstedt, J.C.,Hashim, M.J.: Relative Privacy Valuations Under Varying Disclosure Characteristics. Information Systems Research 30, 375–388 (2019)
9. Dinev, T., Hart, P.: An Extended Privacy Calculus Model for E-Commerce Transactions. Information Systems Research 17, 61–80 (2006)
10. Xu, H., Teo, H.-H., B, Tan, B., Agarwal, R.: The Role of Push–Pull Technology in Privacy Calculus: The Case of Location-Based Services. Journal of Management Information Systems 26, 135–173 (2009)
11. Adjerid, I.,Peer, E.,Acquisti, A.: Beyond the Privacy Paradox: Objective Versus Relative Risk in Privacy Decision Making. MIS Quarterly 42, 465–488 (2018)
12. Brandimarte, L., Acquisti, A., Loewenstein, G.: Misplaced Confidences: Privacy and the Control Paradox. Social Psychological and Personality Science 4, 340–347 (2013)
13. Culnan, M.J., Armstrong, P. K.: Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. Organization Science 10, 104–115 (1999)
14. Ernst, C.-P.H.: Risk Hurts Fun: The Influence of Perceived Privacy Risk on Social Network Site Usage. In: Ernst, C.-P. H.: Factors Driving Social Network Site Usage. pp. 45–56. Springer Fachmedien, Wiesbaden (2014)
15. Wagner, A., Olt, C., Abramova, O.: Calculating Versus Herding In Adoption And Continuance Use Of A Privacy-Invasive Information System: The Case Of COVID-19 Tracing Apps. Proceedings of the 29th European Conference on Information Systems (ECIS), Marrakesh, Morocco, 1-16 (2021)
16. Barth, S., de Jong, M.: The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. Telematics and Informatics 34, 1038–1058 (2017).

17. Glover, S., Benbasat, I.: A Comprehensive Model of Perceived Risk of E-Commerce Transactions. International Journal of Electronic Commerce 15, 47–78 (2010)
18. Karwatzki, S., Trenz, M., Veit, D.: Yes Firms Have My Data but What Does It Matter - Measuring Privacy Risks. Proceedings of the 26th European Conference on Information Systems (ECIS) Portsmouth, UK, 1-15 (2018)
19. Xu, H., Dinev, T., Smith, J., Hart, P.: Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. Journal of the Association for Information Systems 12, 798–824 (2011)
20. Solove, D.J.: A Taxonomy of Privacy. University of Pennsylvania Law Review 154, 477-560 (2006)
21. Acquisti, A., Brandimarte, L., Loewenstein, G.: Privacy and human behavior in the age of information. Science 347, 509–514 (2015)
22. Kanwal, T., Anjum, A., Khan, A.: Privacy preservation in e-health cloud: taxonomy, privacy requirements, feasibility analysis, and opportunities. Cluster Computing 24, 293–317 (2021)
23. Burton-Jones, A., Stein, M.-K., Mishra, A.: IS Use. MIS Quarterly Research Curations, (2017)
24. Turel O., Zhang, Y.: Should I e-collaborate with this group? A multilevel model of usage intentions. Information & Management 48, 62–68 (2011)
25. Nicolaou, A.I., McKnight, D.H.: Perceived Information Quality in Data Exchanges: Effects on Risk, Trust, and Intention to Use. Information Systems Research 17, 332–351 (2006)
26. Bhattacherjee, A.: Understanding Information Systems Continuance: An Expectation-Cornfirmation Model. MIS Quarterly 25, 351–370 (2001)
27. Turel, O.: Quitting the use of a habituated hedonic information system: a theoretical model and empirical examination of Facebook users. European Journal of Information Systems 24, 431–446, (2015)
28. Parthasarathy, M., Bhattacherjee, A.: Understanding Post-Adoption Behavior in the Context of Online Services. Information Systems Research 9, 362–379 (1998)
29. Maier, C., Laumer, S., Weinert, C., Weitzel, T.: The effects of technostress and switching stress on discontinued use of social networking services: a study of Facebook use. Information Systems Journal 25, 275-308 (2015)
30. Malhotra, N. K., Kim, S. S., Agarwal, J.: Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. Information Systems Research 15, 336–355 (2004)
31. WhatsApp Privacy Policy, https://www.whatsapp.com/legal/updates/privacy-policy-eea?lang=en (Accessed: 09.08.2021)
32. WhatsApp Help Center: How we work with the Facebook Companies, https://faq.whatsapp.com/general/security-and-privacy/how-we-work-with-the-facebook- companies (Accessed: 11.08.2021)
33. WhatsApp Help Center: Objecting to the processing of your personal data, https://faq.whatsapp.com/general/security-and-privacy/objecting-to-the-processing-of-your-personal-data (Accessed: 11.08.2021)

34. Moore, G. C., Benbasat, I.: Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation. Information Systems Research 2, 192–222 (1991)
35. Liang, H., Xue, Y., Pinsonneault, A., Wu, Y.: What Users Do Besides Problem-Focused Coping When Facing IT Security Threats: An Emotion-Focused Coping Perspective. MIS Quarterly 43, 373–394 (2019)
36. Zhao, X., Tian, J., Xue, L.: Herding and Software Adoption: A Re-Examination Based on Post-Adoption Software Discontinuance. Journal of Management Information Systems 37, 484–508 (2020)
37. Karwatzki, S., Dytynko, O., Trenz, M., Veit, D.: Beyond the Personalization–Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization. Journal of Management Information Systems 34, 369-400 (2017)