Who Needs Privacy? Exploring the relation between personality and need for privacy

Tobias Dienlin[1] & Miriam Metzger[2]

[1] University of Vienna

[2] University of California Santa Barbara

Author Note

Tobias Dienlin, Department of Communication, University of Vienna, Germany; Miriam Metzger, Department of Communication, University of California, Santa Barbara, United States of America.

Correspondence concerning this article should be addressed to Tobias Dienlin, University of Vienna, Department of Communication, 1090 Vienna, Austria. E-mail: tobias.dienlin@univie.ac.at

Abstract

Privacy is an important societal topic. Living in an information age, people constantly have to decide what information to share, which service to use, or when to communicate. All these decisions are reflective of and determined by the users' need for privacy. It is relevant to understand who needs more and who needs less privacy, because desiring privacy often requires justification. For example, well-known statements such as 'who has nothing to hide has nothing to fear' imply that people who desire privacy are suspicious. Although such suspicions might be justified in some cases, it could also be that people desiring more privacy are just more introverted, anxious, creative, or prudent. In this study we, hence, plan to explore the relation between personality and the need for privacy. Personality factors and facets will be operationalized using the HEXACO personality inventory. Need for privacy will be captured with a multidimensional approach, including informational and social privacy, need for privacy from government agencies, or need fro privacy from companies. Adopting an exploratory analytical framework, we will collect a sample of more than 800 respondents representative of the US in terms of age, gender, and ethnicity. The relations between personality and privacy will be explored using structural equation modeling. Potential implications will be discussed.

Keywords: Privacy, need for privacy, personality, HEXACO, structural equation modeling

Who Needs Privacy? Exploring the relation between personality and need for privacy

In light of the increasing digitization of everyday life, which has led to several sweeping societal changes such as the commodification and monetization of personal information (Sevignani, 2016), privacy has become a major topic of public and academic interest. Despite the topic's importance, to date we still know surprisingly little about the relation between privacy and personality (Masur, 2018, p. 155). Why do some people feel they need or desire more privacy than others do, and how do these people differ from one another?

We believe it is relevant to understand better this research questions, because people who desire privacy are often confronted to justify their need for privacy. For example, well-known statements such as 'who has nothing to hide has nothing to fear' imply that people who desire privacy are suspicious. Indeed, it is only logical that people who commit crimes and who are insincere in fact benefit from more privacy. However, it could also be that people desiring more privacy are just more introverted, anxious, creative, or prudent. We therefore believe that a better understanding of the relation between personality and privacy is relevant. Also from an academic perspective, several theories argue that personality determines privacy behaviors (Masur, 2018, p. 155) However, to date there is almost no empirical research that can be used to deduce well-informed hypotheses. As a result, the main question of this paper is: What are personality factors and facets that best explain peoples' felt need for privacy?

The Need for Privacy

The theoretical concept of privacy is complicated and contested (Nissenbaum, 2010, p. 71). Thus, we first outline our own understanding of privacy. First and foremost, privacy captures a *withdrawal* from others or from society in general, which (b) happens *voluntarily* and with *control* (Westin, 1967). Several models suggest that privacy is multi-dimensional. For example, in a theory-driven treatise Burgoon (1982) argued that

privacy has four dimensions: informational, social, psychological, and physical privacy. Pedersen (1979), by contrast, conducted an empirical factor analysis of overall 94 items and found six dimensions of privacy: reserve, isolation, solitude, intimacy with friends, intimacy with family, and anonymity. Next, Schwartz (1968) or Masur, Teutsch, and Dienlin (2018) differentiated between horizontal and vertical privacy; whereas horizontal privacy captures withdrawal from peers, vertical privacy addresses withdrawal from superiors or institutions (e.g., government agencies or business companies).

For the purpose of this study, we will hence employ a multifaceted model of need for privacy. We fill focus on (a) vertical privacy with regard to people's felt need for withdrawal from government surveillance and private companies, (b) horizontal privacy in terms of the perceived need for withdrawal from other people, psychological and physical privacy, and (c) both horizontal and vertical privacy as captured by people's felt need for informational privacy, anonymity, and privacy in general.

According to Trepte and Masur (2017), the need for privacy is a secondary need—it is not an end in itself, but rather a way to satisfy other more fundamental needs such as safety, sexuality, recovery, or contemplation. Specifically, Westin (1967) defined four ultimate purposes of privacy: (1) self-development (i.e., the integration of experiences into meaningful patterns), (2) autonomy (i.e., the desire to avoid being manipulated and dominated), (3) emotional release (i.e., the release of tension from social role demands), and (4) protected communication (i.e., the ability to foster intimate relationships). Not least, privacy facilitates self-disclosure (Dienlin, 2014), which is necessary for attaining social support, initiating relationships, and getting close to other people (Omarzu, 2000).

On the other hand, however, privacy can also have negative aspects. For example, it is possible to have too much privacy. Human beings are inherently social, and being overly cut-off from others can diminish flourishing, nurture deviant behavior, or introduce power asymmetries (Altman, 1975). The fact that privacy fosters self-disclosure presents also a potential risk, because others might disagree, disapprove, or misuse the information in

other contexts (Petronio, 2010). Privacy can also help conceal power-asymmetries, wrongdoing, or crimes such as violence or theft. The dialectical tension between the positive and negative aspects of privacy likely causes variability across individuals in their need for privacy. In this study we now ask, what role does personality play in determining individual-level variations in need for privacy?

Predicting the Need for Privacy

So far, not a lot of studies have explicitly analyzed the relation between personality and need for privacy. We are aware of only two studies that conducted an empirical analysis Hosman (1991). And as there is no established theory connecting privacy and personality, it is difficult to formulate precise and well-informed hypotheses. As a result, in this study we adopt an exploratory perspective. We will adopt a large-scale perspective on personality, in order not to miss potentially relevant personality factors and facets.

To this end, we build on the HEXACO inventory of personality (Lee & Ashton, 2018). The HEXACO model stands in the tradition of Big Five approach (John & Srivastava, 1999), and it represents a broad understanding of personality. It measures overall six factors (see below), which have four specific facets each. We build not only on general factors but also specific facets, because we do not expect that the also very specific need for privacy will relate closely to the overarching factors. (For example, consider that privacy concerns, a variable conceptually close to need for privacy, shows only small relations to the Big Five factors (Bansal, Zahedi, & Gefen, 2010; Junglas, Johnson, & Spitzmüller, 2008).) Another reason for choosing the HEXACO model was that in addition to the Big Five factors the HEXACO model includes a sixth one labeled Honesty Humility, plus another facet labeled Altruism, which together seem promising to investigate the nothing to hide argument. In what follows, we briefly present all factors and provide some tentative thoughts on how they and selected facets might relate to privacy.

Honesty-Humility. Honesty-Humility consists of the facets "sincerity," "fairness," "greed avoidance," and "modesty." We could imagine that honesty-humility relates to need for privacy for several reasons. First, it has often been argued that people need privacy because they have something to hide (are hence less honest, sincere, or fair). The so-called *nothing-to-hide argument* states that "If you have nothing to hide, you have nothing to fear." For example, the nothing-to-hide argument implies that data mining and surveillance by government entities "is not likely to be threatening to the privacy of law-abiding citizens. Only those who are engaged in illegal activities have a reason to hide this information" (Solove, 2007, p. 753).

Logically, people who actually commit crimes may face even greater risk from self-disclosure compared to others, because government agencies and people would surely disapprove of their activities (Petronio, 2010). Hence, the government and other people are more likely to be perceived as a threat, which should render anonymity a resource. As a consequence, people with lower honesty and humility might desire more privacy as a means to mitigate their felt risk (Altman, 1976). For example, studies have found that surveillance can reduce cheating behaviors (Corcoran & Rotter, 1987; Covey, Saladin, & Killen, 1989). Covey, Saladin, and Killen (1989) for example asked students to solve an impossible maze. In the high surveillance condition, the experimenter stood in front of the students and closely monitored their behavior. In the low surveillance condition, the experimenter remained behind the students where he or she could not see the students. Results showed greater cheating among students in the low surveillance condition, suggesting that in situations with less privacy, people show more honesty (i.e., fewer cheating behaviors). Next, in a longitudinal sample with 457 respondents in Germany (Trepte, Dienlin, & Reinecke, 2013), people who felt they needed more privacy were also less authentic (and therefore, arguably, also less honest and sincere) on their online social network profiles (r = -.48) and less authentic in their personal relationships (r = -.28).

In conclusion, we could imagine that lack of honesty may indeed relate to an

increased felt need for privacy, especially when it comes to government surveillance.

Emotionality. Next, it seems possible that the need for privacy is also related to people's level of emotionality. Emotionality is captured by the facets fearfulness, anxiety, dependence, and sentimentality. General anxiety measures for example whether people are afraid of negative events or whether they are easily frightened. With regard to interpersonal privacy, one could argue that people who are anxious are more likely to consider social interactions a risk or threat [especially with strangers or weak ties; Granovetter (1973)], which is why anxious people might desire more privacy. Somewhat related, prior empirical research has shown that people who are more concerned about their privacy are also more likely to withdraw online, for example by deleting posts or untagging themselves from linked content (Dienlin & Metzger, 2016). On the other hand, one could argue in favor of the opposite: People who are more anxious may desire *less* privacy from others (especially their strong ties), as a means to cope better with their daily challenges.

Concerning the need for privacy from government surveillance, we could imagine that people who are more anxious desire less privacy. Despite the fact that only 18% of all Americans trust their government "to do what is right" (Center, 2017), almost everyone agrees that "it's the government's job to keep the country safe," while most people are also satisfied with the government's job [pewresearchcenterDistrustHowAmericans2015]. Hence, for anxious individuals, the government might be seen as a resource rather than a threat. It therefore seems plausible that people who are in general more anxious are also more likely to consent to government surveillance, given that such surveillance promises to prevent crime or to reduce the likelihood of terrorist attacks. Therefore, people who are more anxious might desire less privacy from government surveillance and, for the same reasons, also less anonymity.

Extraversion. Extraversion is comprised of the facets social self-esteem, social boldness, sociability, and liveliness. Arguably, extraversion is the factor that should correspond most closely to need for privacy. This especially pertains to sociability, which

captures whether people prefer to spend their time alone or with company. It seems plausible that people who are more sociable are also more likely to think of other people as a resource, which is why they should generally desire less interpersonal privacy and less anonymity (e.g., Buss, 2001). Put differently, given that privacy is a voluntary withdrawal from society (Westin, 1967), we expect that people who are less sociable, more reserved, or more shy should have a greater need for privacy from others.

This rationale is supported by several empirical studies: People who score higher on the personality meta-factor *plasticity*, which is a composite of the two personality factors extraversion and openness, have been shown to desire less privacy (Morton, 2013); people who describe themselves as introverted thinkers are more likely to prefer social isolation (Pedersen, 1982); and introverted people are more likely to report invasions of privacy (Stone, 1986).

Finally, Pedersen (1982) showed that three dimensions of need for privacy relate to self-esteem: Respondents who held a lower self-esteem were more reserved ($r = .29$), needed more anonymity ($r = .21$), and preferred solitude ($r = .24$).

Agreeableness. Agreeableness is captured by the facets forgiveness, gentleness, flexibility, and patience. It is not entirely clear whether or not agreeableness relates to need for privacy. Notably, it has been found that people who are more agreeable are also moderately less concerned about their privacy (Junglas, Johnson, & Spitzmüller, 2008). Because need for privacy and privacy concerns are closely related, it seems possible that more agreeable people desire less privacy.

Conscientiousness. Conscientiousness consists of the facets organization, diligence, perfectionism, and prudence. Arguably, all facets are about being in control, about reducing potential risks, and avoiding future costs. And because privacy is much about control, it seems likely that an individual's felt need for privacy relates to their general tendency to avoid risks, to deliberate, and to plan ahead carefully. If other people are considered a threat, people who are risk averse might desire more interpersonal privacy.

The most cautious strategy to minimize risks of information disclosure would be to keep as much information as possible private. Somewhat related, empirical studies report that people who consider their privacy at risk are less likely to disclose information online (e.g., Bol et al., 2018). Moreover, conscientious people are slightly more concerned about their privacy (Junglas, Johnson, & Spitzmüller, 2008). But as above, especially with regard to privacy from government surveillance, risk averse people could also desire *less* privacy, so that the government is able to avert potential threats. In sum, think that it is most plausible that people who are more risk averse also desire more privacy in all three contexts measured in this study.

Openness to Experiences. Openness to experiences comprises the facets aesthetic appreciation, inquisitiveness, creativeness, and unconventionality. Openness to experience is also considered a measure of intellect and education. More educated people have more knowledge about how to protect their privacy (Park, 2013), which could be the result of an increased need for privacy. Junglas, Johnson, and Spitzmüller (2008) reported that openness to experience is positively related to privacy concern, supporting this reasoning.

On the other hand, openness is by definition the opposite of privacy, and people who are more open to experience news aspects might proritize privacy, for example when it comes to testing a new social medium. Many new digital practices such as online interaction, purchases, or information seeking pose a risk to privacy. People who are less open to new experiences might not care so much about the potential benefits but rather what could be lost, prioritizing privacy.

Socio-demographic variables. Finally, it has often been shown that socio-demographic variables such as sex, age, education, and affluence can relate to the need for privacy. For example, in a study with 3.072 people from Germany, women desired more informational and physical privacy, while man needed more psychological privacy (Frener, Wagner, & Trepte, 2021). In a nationally representative study of the US and Japan, in both countries people who were older and who had higher income levels reported

more privacy concerns. As reported above, more educated people possess also more privacy knowledge (Park, 2013).

Method

This section describes how we determine the sample size, data exclusions, the analyses, and all measures in the study.

Sample

Participants will be collected from the professional online survey panel Prolific. The sample will be representative of the US regarding age, gender, and ethnicity. The study received IRB approval from University of Vienna. We calculated that participation will take approximately 15 minutes. We will pay participants $ 2.56 for participation, equaling an hourly wage of $ 9,81.

To determine sample size, we ran a priori power analyses. The final analyses will be conducted using structural equation modeling, for which exact power analyses are difficult to obtain. We hence conducted tentative power analyses using two-sided bivariate correlations. Hence, power analysis are not exact but only a rough guide to get a better idea of the required minimum sample size.

We based our power analysis on a smallest effect size of interest (SESOI). We only consider effects at least as great as $r = .10$ as sufficient support for our theoretical rationales (Cohen, 1992). Because we adopt an exploratory perspective, we do not want to miss potentially existing effects. We opted for a balanced alpha and beta error approach, because we consider both errors to be equally relevant. In conclusion, in our study we assume an alpha error of 10% and a beta error of 10%, representing a power of 90%. Hence, we will use two inference criteria: Effects need to show a p-value below $p = 10\%$ and an effect size of at least $r = .10$. Together, power analyses revealed a minimum sample size of $N = 782$.

We will individually check responses for patterns such as straight-lining or missing of inverted items, making sure to remove only clear cases. We will automatically exclude participants who miss two attention checks. Participants who miss one attention check will be checked carefully regarding response patterns. We will remove participants if they should report ages below the minimum participation age of 18 years. We will exclude respondents if they answer less than 50% of all questions. The remaining missing responses will be imputed using predictive mean matching. We will remove respondents with exceedingly fast responses, namely below three standard deviations of the medium response time.

Data Analyses

The factorial validity of the measures and the hypotheses will be tested with structural equation modeling (SEM). If Mardia's test shows that the assumption of multivariate normality is violated, we will use the more robust Satorra-Bentler scaled and mean-adjusted test statistic (MLM) as estimator. We will test each scale in a confirmatory factor analysis. To avoid overfiting the models to the data, we will use more liberal fit criteria (CFI $>$ .90, TLI $>$ .90, RMSEA $<$. .10, SRMR $<$ .10) (Kline, 2016). If the models' fit is below the criteria, we will first inspect modification indices, potentially allowing covariance or cross-loadings if theoretically plausible. If these changes do not yield sufficient fit, we will drop malfunctioning items. If fit is still subpar, we will conduct exploratory factor analyses (EFA) to asssess the underlying factor structure. EFAs will be run using maximum likelihood estimation and oblimin rotation (Osborne & Costello, 2004, p. 7). If more than one dimension was revealed, we will implement bifactor model solutions.[1] Bifactor models retain a general measure of the variable, and it is not necessary

[1] Bifactor models implement one factor that explains the variance in all items (the so-called general factor or g-factor). In addition, at least two additional factors are implemented that explain the variance in a subset of the items. The general factor and the specific factors are orthogonal. Bifactor models are nested within hierarchical models. For more information on bifactor models, see Kline (2016), p. 319. Note that

to introduce novel subdimensions. If no adequate bifactor model can be found, we will proceed by deleting items with low loadings on the general factor and/or the specific factors. If also after deletion of individual items no bifactor solution should emerge, using a subset of the items we will extract a single factor with sufficient factorial validity.

To answer our research question, we will analyze the variables' bivariate relations. To assess better the variables' potential causal effect, we will also ran a multiple structural regression model. Because we were interested in a complex model (overall, eight predictors and three outcomes) but the sample was comparatively small, we simplified the model. To this end, instead of a fully latent structural regression model we conducted a partially latent structural regression model, in which the predictor variables were modeled as single indicators while controlling for measurement error (Kline, 2016, p. 214). To get high-quality single indicators of the predictors, we computed the average of the model predicted values / latent factor scores, which we extracted from the CFAs. If the CFAs showed a unidimensional solution, we used the model predicted values for this latent factor; if the CFAs produced a multidimensional solution, we used the model predicted values for the general latent factor.

Finally, combining several items into a latent factors helps to reduce and condense information, while partialing out error. At the same time, and although above we explicated our analysis pipeline, this approach still maintains several researcher degrees of freedom. We hence emphasize that we will adapt the models only to achieve satisfactory factorial validity and not to cherry-pick significant material. To provide a broader picture, in the online supplementary material (OSM) we will also share the results of the unaltered factors and how the personality factors predicted reach need for privacy item individually.

---

we will not specify a bifactor model of need for privacy, because we are explicitly interested in the relations between the personality facets and the three dimensions of need for privacy.

Measures

All items were answered on a 7-point Likert scale ranging from 1 (*strongly disagree*) to 7 (*strongly agree*).[2] A list of all the items that were used (including deleted ones), results of CFAs/EFAs, as well as item statistics and their distribution plots can be found or will later be reported in the OSM.

Need for privacy. Although there exist several operationalizations of need for privacy (Buss, 2001; Frener, Wagner, & Trepte, 2021; Marshall, 1974; Pedersen, 1979), we are not aware of a scale that is both encompassing and up-to-date. Hence, we use both extant scales and newly developed ad-hoc scales, some of which were already pretested. Ad-hoc scales were tentatively validated. We (a) collected qualitative feedback from three different privacy experts, (b) tested and adapted the items using four established readability indices (i.e., Flesch–Kincaid reading grade, Gunning Fog Index, Coleman Liau Index, and the Dale–Chall Readability Formula; see, e.g., Patalay, Hayes, & Wolpert, 2018), and (c) like Frener, Wagner, and Trepte (2021) will assess convergent validity by collecting single-item measures of privacy concern and privacy behavior, for which we expect to find small to moderate relations.

Overall, we will collect 32 items measuring need for privacy, with eight subdimensions consisting of four items each. Three subdimensions were adopted from Frener, Wagner, and Trepte (2021) – namely psychological, informational, and physiological privacy – which build on Burgoon's Burgoon (1982) privacy theory. Because Frener, Wagner, and Trepte (2021) could not successfully operationalize the dimension of social privacy, we also measured a social privacy dimension, which in a prestudy showed satisfactory fit. We then measured need for privacy on a societal level. The first subdimension was government surveillance, which represents the extent to which people want the government to abstain

[2] Note that the HEXACO inventory normally uses 5-point scales. Because we were not interested in comparing absolute values across studies, we used 7-point scales to have a uniform answer format for all items, which in addition likely increase meaningful variance.

from collecting information about them. The second dimension was anonymity, which captures the extent to which people feel the need to avoid identification. Both scales were pretested and showed good factorial validity. Third, we measured need for privacy from companies using four self-designed items. Finally, we self-developed also a general measure of need for privacy.

Personality. Personality will be measured using the HEXACO personality inventory. The inventory consists of six factors with four dimensions each, including the additional meta scale "altruism." We will predict need for privacy first using the factors and then using the facets.

References

Altman, I. (1975). *The environment and social behavior*. Monterey, CA: Brooks Cole.

Altman, I. (1976). Privacy: A conceptual analysis. *Environment and Behavior*, *8*(1), 7–29. https://doi.org/10.1177/001391657600800102

Bansal, G., Zahedi, F. M., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, *49*(2), 138–150. https://doi.org/10.1016/j.dss.2010.01.010

Bol, N., Dienlin, T., Kruikemeier, S., Sax, M., Boerman, S. C., Strycharz, J., ... Vreese, C. H. (2018). Understanding the effects of personalization as a privacy calculus: Analyzing self-disclosure across health, news, and commerce contexts. *Journal of Computer-Mediated Communication*, *23*(6), 370–388. https://doi.org/10.1093/jcmc/zmy020

Burgoon, J. K. (1982). Privacy and communication. *Annals of the International Communication Association*, *1*, 206–249.

Buss, A. H. (2001). *Psychological dimensions of the self*. Thousand Oaks; Calif: Sage Publications.

Center, P. R. (2017). Public trust in government: 1958-2017. {InternetDocument}. Retrieved from http://www.people-press.org/2017/12/14/public-trust-in-government-1958-2017/

Cohen, J. (1992). A power primer. *Psychological Bulletin*, *112*(1), 155–159. https://doi.org/10.1037/0033-2909.112.1.155

Corcoran, K. J., & Rotter, J. B. (1987). Morality-conscience guilt scale as a predictor of ethical behavior in a cheating situation among college females. *The Journal of General Psychology*, *114*(2), 117–123. https://doi.org/10.1080/00221309.1987.9711061

Covey, M. K., Saladin, S., & Killen, P. J. (1989). Self-monitoring, surveillance, and incentive effects on cheating. *The Journal of Social Psychology*, *129*(5), 673–679.

https://doi.org/10.1080/00224545.1989.9713784

Dienlin, T. (2014). The privacy process model. In S. Garnett, S. Halft, M. Herz, & J. M. Mönig (Eds.), *Medien und Privatheit* (pp. 105–122). Passau, Germany: Karl Stutz.

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs—Analyzing self-disclosure and self-withdrawal in a representative U.S. sample. *Journal of Computer-Mediated Communication*, *21*(5), 368–383. https://doi.org/10.1111/jcc4.12163

Frener, R., Wagner, J., & Trepte, S. (2021). Development and validation of the need for privacy scale (NFP-S). Denver, CO, digital conference.

Granovetter, M. S. (1973). The strength of weak ties. *American Journal of Sociology*, *78*(6), 1360–1380.

Hosman, L. A. (1991). The relationships among need for privacy, loneliness, conversational sensitivity, and interpersonal communication motives. *Communication Reports*, *4*(2), 73–80. https://doi.org/10.1080/08934219109367527

John, O. P., & Srivastava, S. (1999). The big five trait taxonomy: History, measurement, and theoretical perspectives. In L. A. Pervin & O. P. John (Eds.), *Handbook of personality: Theory and research* (2. ed., pp. 102–138). New York, NY: Guilford Press.

Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: An empirical study in the context of location-based services. *European Journal of Information Systems*, *17*(4), 387–402. https://doi.org/10.1057/ejis.2008.29

Kline, R. B. (2016). *Principles and practice of structural equation modeling* (4th ed.). New York, NY: The Guilford Press.

Lee, K., & Ashton, M. C. (2018). Psychometric Properties of the HEXACO-100. *Assessment*, *25*(5), 543–556. https://doi.org/10.1177/1073191116659134

Marshall, N. J. (1974). Dimensions of privacy preferences. *Multivariate Behavioral Research*, *9*(3), 255–271. https://doi.org/10.1207/s15327906mbr0903_1

Masur, P. K. (2018). *Situational privacy and self-disclosure: Communication processes in online environments*. Cham, Switzerland: Springer.

Masur, P. K., Teutsch, D., & Dienlin, T. (2018). Privatheit in der Online-Kommunikation. In W. Schweiger & K. Beck (Eds.), *Handbuch Online-Kommunikation* (2nd ed.). Wiesbaden, Germany: Springer VS. https://doi.org/10.1007/978-3-658-18017-1_16-1

Morton, A. (2013). Measuring inherent privacy concern and desire for privacy - A pilot survey study of an instrument to measure dispositional privacy concern. In *International Conference on Social Computing (SocialCom)* (pp. 468–477). https://doi.org/10.1109/SocialCom.2013.73

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford University Press.

Omarzu, J. (2000). A disclosure decision model: Determining how and when individuals will self-disclose. *Personality and Social Psychology Review*, *4*(2), 174–185. https://doi.org/10.1207/S15327957PSPR0402_5

Osborne, J. W., & Costello, A. B. (2004). Sample size and subject to item ratio in principal components analysis. *Practical Assessment, Research & Evaluation*, *9*(11).

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research*, *40*(2), 215–236. https://doi.org/10.1177/0093650211418338

Patalay, P., Hayes, D., & Wolpert, M. (2018). Assessing the readability of the self-reported Strengths and Difficulties Questionnaire. *BJPsych Open*, *4*(2), 55–57. https://doi.org/10.1192/bjo.2017.13

Pedersen, D. M. (1979). Dimensions of privacy. *Perceptual and Motor Skills*, *48*(3), 1291–1297. https://doi.org/10.2466/pms.1979.48.3c.1291

Pedersen, D. M. (1982). Personality correlates of privacy. *The Journal of Psychology*, *112*(1), 11–14. https://doi.org/10.1080/00223980.1982.9923528

Petronio, S. (2010). Communication privacy management theory: What do we know about family privacy regulation? *Journal of Family Theory & Review*, *2*(3), 175–196.

https://doi.org/10.1111/j.1756-2589.2010.00052.x

Schwartz, B. (1968). The social psychology of privacy. *American Journal of Sociology*, *73*(6), 741–752.

Sevignani, S. (2016). *Privacy and capitalism in the age of social media*. New York; London: Routledge Taylor & Francis Group.

Solove, D. J. (2007). 'I've got nothing to hide' and other misunderstandings of privacy. *San Diego Law Review*, *44*, 745–772.

Stone, D. L. (1986). Relationship between introversion/extraversion, values regarding control over information, and perceptions of invasion of privacy. *Perceptual and Motor Skills*, *62*(2), 371–376. https://doi.org/10.2466/pms.1986.62.2.371

Trepte, S., Dienlin, T., & Reinecke, L. (2013). *Privacy, self-disclosure, social support, and social network site use. Research report of a three-year panel study* ({UnpublishedWork}). Retrieved from http://opus.uni-hohenheim.de/volltexte/2013/889/

Trepte, S., & Masur, P. K. (2017). Need for privacy. In V. Zeigler-Hill & T. K. Shackelford (Eds.), *Encyclopedia of Personality and Individual Differences* (pp. 1–4). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-28099-8_540-1

Westin, A. F. (1967). *Privacy and freedom*. New York, NY: Atheneum.

Contributions

Conception and design: TD, MM. Data acquisition: TD. Code: TD. Analysis and interpretation of data: TD, MM; First draft: TD; Revisions & Comments: TD & MM.

Funding Information

During the conception and data collection of the prestudy, TD was funded by The German Academic Scholarship Foundation (German: Studienstiftung des deutschen Volkes), which financially supported a research stay at UCSB. During some time working on the article and while at University of Hohenheim, TD was funded by the Volkswagen

Foundation (German: Volkswagenstiftung), grant "Transformations of Privacy." TD is now funded by a regular and not-tenured assistant professorship at University of Vienna. MM is funded by a regular and tenured full professorship at UCSB.

Competing Interests

Both authors declare no competing interests.

Supplementary Material

All the stimuli, presentation materials, participant data, analysis scripts, and a reproducible version of the manuscript can be found or will be shared as online supplementary material on the open science framework (https://osf.io/7ncpk/). The paper also has a companion website where all materials can be accessed ().

Data Accessibility Statement

The data will be shared on the open science framework (https://osf.io/7ncpk/).