Digital Inequalities in Online Privacy Protection: Effects of Age, Education, and Gender

Moritz Büchi, Noemi Festic, Natascha Just and Michael Latzer
University of Zurich

Repeated data-breach revelations like the 2018 *Cambridge Analytica* scandal go hand in hand with increasing concerns about the protection of personal data on the Internet and discussions about adequate privacy and data governance. Contemporary information societies are marked by datafication (van Dijck, 2014) and combine a set of distinctive features, among them big data as a new asset class and new algorithmic methods of extracting economic and social value from it (Latzer, Hollnbuchner, Just, & Saurwein, 2016). The volume and scope of data collection is continuously expanding, and small and big personal data are increasingly at the core of various business models. They are being traded on a large scale and have essentially become a currency in multi-sided Internet platform markets with which users pay—knowingly or unknowingly—for zero-priced goods (Just, 2018). This unprecedented availability of data and the sophisticated methods of harnessing it result both in calls to get over privacy by proclaiming a post-privacy era (Heller, 2011) and claims to provide adequate levels of data and privacy protection. From an institutional perspective the governance of privacy or data comprises a mix of interwoven actors and instruments (Bennett & Raab, 2003; Latzer, Just, Saurwein, & Slominski, 2003). This mix ranges from *top-down* command-and-control regulation at the one end, like the EU General Data Protection Regulation (Regulation (EU) 2016/679), to *bottom-up* user self-help at the other end. The latter refers, for example, to ways of generally and deliberately limiting the disclosure of personal data or of actively managing this disclosure with a myriad of PETs—privacy enhancing technologies—or by using fake identities (Preibusch, 2015).

The impotence of the state to guarantee full-fledged protection in global online networks in general (Roßnagel, 1997), and the legacy of the conventional liberal privacy paradigm with focus on individualistic conceptions of privacy in particular (Bennett & Raab, 2003; Regan, 1995), both suggest a more prominent role for user self-help in this governance mix.

In fact, being online has become a societal standard and prerequisite for functioning in society by facilitating, among other things, social interactions and relationship building (Ellison, Vitak, Steinfield, Gray, & Lampe, 2011). A complete refusal of data disclosure is therefore not an option in this new data-driven age (Hargittai & Marwick, 2016), especially if Internet users wish to profit from the various advantages of using the Internet. As a consequence, the individual balancing of the benefits and risks of disclosing personal data as well as self-protection become more important. While some empirical studies show that active privacy protection varies from one person to another (Latzer, Büchi, & Just, 2015a), a digital-inequality perspective on the wider distribution of privacy protection across societies is largely missing. In particular, work has not explored digital inequalities in the extent to which people actively protect their privacy online, and the factors that explain the different dimensions of privacy self-help protection on the individual level. Such an understanding is necessary, however, to comprehend better who gets what level of data protection, and to identify whether or not there are systematically disadvantaged and vulnerable social groups. Such knowledge may, in turn, feed back into policy-making with the aim of remedying structural inequalities—a consideration that has not received adequate attention in data or privacy protection policies thus far.

This chapter contributes to a more nuanced understanding of differences in self-help privacy protection based on nationally representative survey data and includes Internet skills as an important digital inequality variable. Individuals' self-help is only one means of privacy governance among many, and uncovering its specifics says little about the overall extent of privacy protection that is accorded to a particular person or society at large. However, by conceptually analyzing online privacy as a social value (instead of mainly as an individual one) within a digital inequalities framework, and by empirically exposing sociodemographic and Internet-usage-related predictors of self-help privacy protection, one is able to locate digital inequalities with regard to active online privacy protection, and to uncover the factors that inhibit or facilitate adequate self-protection.

In line with digital inequality research, it is likely that disadvantaged Internet users with lower digital skills or education in general are more vulnerable to privacy violations. At the same time questions have been raised as to whether a privacy divide will necessarily map neatly into a digital divide (Bennett & Raab, 2003), as those who are socioeconomically better off may be presumed to be particularly vulnerable to data extraction and profiling for economic reasons. Little research has been done on (sociodemographic) predictors of online privacy protection, particularly drawing on population-level data. This chapter contributes to closing this gap and empirically addresses the following questions: What explains variance in individuals' privacy protection behavior online? How is individuals' privacy protection behavior influenced by sociodemographic attributes, by the amount of people's overall Internet use and their Internet skills, as well as by their attitudes towards personal information and past privacy breaches?

This chapter first provides a brief overview of existing research on online privacy with a focus on protective behavior. It then outlines the relevance of researching online privacy protection from a digital inequalities perspective. Privacy is fundamentally seen as a common, public and collective value (Regan, 1995) whose unequal distribution may be a societal problem. Its protection and social distribution are therefore not only a regulatory issue but essentially an issue of social policy (Bennett & Raab, 2003). The empirical part describes the methods and results. A discussion of the findings and their implications concludes the chapter.

Protection of Online Privacy

The expectation that Internet use yields personal, economic or social advantages is often complemented by important assumptions about its opposite effects (van den Hoven, 2008). Experiencing privacy breaches first-hand can have real-life consequences. These can take the form of tangible outcomes like job loss or feelings of embarrassment due to personal information becoming publicly available against one's will. But even the perception of or potential for insufficient privacy protection, for instance due to the mere possibility of surveillance, can have negative effects in that people may be deterred from exercising their freedoms online – a phenomenon also described as chilling effects (e.g., Penney, 2017). Such incidents or feelings are sometimes presumed to induce stress or to affect an individual's subjective well-being negatively (Reinecke & Oliver, 2017). Negative privacy experiences and general awareness about the importance of privacy online appear, however, in discord with actual privacy protection behavior, and evidence of its predictors and their strength varies.

Inconsistent user behavior regarding online privacy has, for example, been extensively and repeatedly researched, in particular for social media, within the framework of the *privacy paradox* (e.g., Barnes, 2006; Norberg, Horne, & Horne, 2007; Taddicken, 2014). This holds that Internet users tend to share large amounts of personal information online, despite simultaneously claiming to care or be worried about the security of their data.

Hargittai and Marwick (2016) summarize three main causes for this phenomenon reported in existing literature: a general lack of understanding of possible risks or dangers, deficits regarding appropriate skills to protect personal privacy, and the social relevance of sharing information, among other things, for socialization or employment purposes. In focus group interviews with 40 young adults, their own research shows how feelings of resignation and pragmatic, cynical attitudes provide further explanations for why Internet users' privacy concerns do not immediately translate into protective behavior or less disclosure (Hargittai & Marwick, 2016). Similarly, *privacy fatigue*, conceptualized by Choi, Park, and Jung (2018) as composed of emotional exhaustion and cynicism, was shown to result in a greater intention to provide personal information and to be a more important predictor of privacy behavior than privacy concerns for a sample of 324 Internet users.

Research reveals that people are not generally ignorant, but that they continuously and actively negotiate the scope and amount of personal information they share in order to protect and express themselves against variables that affect their privacy (Young & Quan-Haase, 2013). For example, in a longitudinal panel study of 5076 early adopters, Facebook users expanded their privacy-seeking behavior and withheld increasing amounts of personal data over time, sharing less with "stranger" profiles in the network (Stutzman, Gross, & Acquisti, 2012). At the same time, they tended to share increasing amounts of personal information with profiles that were connected to their own, which meant that they also, and potentially unknowingly, shared increasing amounts of data with "silent listeners" such as Facebook, third parties and advertisers.

Altogether, existing literature on online privacy has predominantly revealed privacy concerns and attitudes as well as experienced privacy breaches as predictors of privacy protection (Baruh, Secinti, & Cemalcilar, 2017). Drawing on the same data set as this chapter, Büchi, Just and Latzer (2017) showed, for example, that past experiences with privacy breaches strongly predicted current protective behavior. Also, in accordance with privacy paradox research, caring about privacy, i.e. strong privacy attitudes, did not automatically lead to strong self-protection. The main result, however, was that general Internet skills were a key predictor of users' privacy behavior.

The mixed and sometimes contradicting results of existing research can be attributed to differing definitions or operationalizations of privacy concerns and protective behaviors (Kokolakis, 2017). For instance, privacy behavior is commonly measured through the amount or scope of information that individuals disclose online rather than actual protection measures they actively pursue. Privacy must therefore always be viewed against specific contexts and varies greatly with changing circumstances (Acquisti, Brandimarte, & Loewenstein, 2015).

Digital inequalities in privacy protection

From its inception, the idea of privacy protection has been predicated on a liberal democratic model, essentially on an individualistic conception of privacy as a special type of "right to be let alone" (Warren & Brandeis, 1890, p. 193). While this individualist privacy paradigm is increasingly being questioned in research, among other things, with a recognition of its social value (Regan, 1995; Bennett & Raab, 2003; Nissenbaum, 2010; Solove, 2015), there is still a tendency in policy-making and regulation to remain loyal to this legacy. An example of this is the above-mentioned EU data-protection regulation, which came into effect in May 2018. It particularly aims at allowing citizens better control of their data by introducing, among other things, a new right to data portability or strengthened rights to request the erasure of data. However, privacy in general, and the risks and harms incurred by privacy violations in particular, affect people differently as individual privacy needs vary by social identity and situation—an issue that this new regulation, for example, does not account for. While it contains comprehensive obligations regarding reciprocal communication between the various stakeholders involved in data protection, the encouragement of awareness-raising activities, codes of conduct and certification mechanisms, there is no provision that accounts for scrutinizing likely disparities among the people this regulation is intended to protect. Such knowledge, however, could assist in detecting inequalities in privacy and data protection and allow adjusting public policies accordingly.

To discuss online privacy protection in line with digital-inequality scholarship is therefore precisely to rethink this traditional conception of privacy (protection): from a primary emphasis on its importance to individuals to an acknowledgement of its broader importance to societies at large and the likely consequences this entails for policy-making.

Systematically or structurally marginalized groups can be assumed to experience privacy (protection) differently from privileged groups within a society (Marwick & boyd, 2018; Matzner et al., 2016). Increasingly, individuals are required to provide personal data as a precondition for employment, the receipt of social services, or the avoidance of negative financial consequences (Marwick & boyd, 2018). For example, automated assessment methods are increasingly used to determine the "employability" of job candidates (O'Neil, 2016). Their social media data is used to calculate their fit for a specific position based on personality type analyses from likes and shares on social media profiles or the assessment of a candidate's network connections to determine their social capital (Madden, Gilman, Levy, & Marwick, 2017).

Various studies have started investigating online privacy for such disadvantaged groups. For instance, privacy concerns have been found to be among the top five reasons for Internet nonuse among members of disadvantaged public housing communities in a major US city—a pattern that is in contrast with general population data that report such concerns as the least-mentioned reason (Li, Chen, & Straubhaar, 2018). Further, for Internet users in these communities, age was the only sociodemographic factor significantly and negatively related to digital privacy-protection skills and to the conduct of digital activities that can compromise privacy (i.e., activities like online purchases, online banking, or the use of social online networks that involve self-disclosure of personal information and that enhance quality of life).

It is particularly these disadvantaged groups that are most dependent on the decisions made based on their data and who are likely to be unaware of data-collection practices (Matzner et al., 2016) or have inadequate skills to manage their own information disclosure on the Internet (Li et al., 2018). Older individuals and women have been shown to have lower levels of technical skills of privacy control, whereas education had no effect (Park, 2013). Park's (2013) analysis of a probability sample of 419 American Internet users surveyed in 2008 revealed age as the most important sociodemographic predictor of information control behavior, suggesting that older users are a particularly vulnerable group in connection with privacy online. Also, men tended to have higher technical privacy skills and have greater confidence in their own privacy protection behavior (Park, 2015). For a representative sample of 3000 American adults, Madden et al. (2017) detected low-income individuals as a specifically vulnerable group that reports being unconfident about their understanding of privacy policies, their ability to manage privacy settings, and report difficulties in finding tools and strategies that would help them protect their data online. These results are particularly alarming, because such vulnerable population groups are specifically targeted by data-driven surveillance practices. Such disadvantaged groups are then also particularly vulnerable to potential errors or biases embedded in data-driven, algorithmic systems that make automated decisions.

Privacy protection behavior has also been (implicitly) researched in relation to digital inequalities and the privacy paradox. This has often been regarded as a generational particularity, distinguishing young people's behavior. Recent research, however, suggests that if such a privacy paradox exists, generational divides or differences do not suffice to explain it (Hargittai & Marwick, 2016; Madden, Lenhart, Cortesi, & Gasser, 2013). Drawing on a sample of American college students surveyed about their privacy practices on Facebook, Tufekci (2012) found that negative experiences and general concerns drive self-protective measures.

This chapter now scrutinizes what inhibits privacy protection and thereby focuses on the amount of Internet use, general Internet skills, privacy attitudes, and experienced privacy breaches as predictors for self-help protection behavior and specifically investigates differences based on sociodemographic variables (age, gender, education).

[Figure 1 here]

The model shown in Figure 1 conceptualizes online privacy protection as dependent on two groups of variables. First, to explain privacy-related behavior, *experience* with privacy violations and *attitudes* regarding the protection of potentially sensitive personal data are considered relevant (Chen, Beaudoin, & Hong, 2016; Kokolakis, 2017). Besides these variables that are directly related to privacy, more general measures at the level of Internet usage, *skills* and *amount*, are expected to influence online privacy protection behavior (Park, 2013; Litt & Hargittai, 2014). Second, sociodemographic variables potentially affect the level of self-help online privacy protection as well as its Internet-usage-related predictors. The conceptual model specifically indicates that online privacy is sensitive to inequalities. Variables such as education have traditionally been associated with digital disadvantage; for example, less educated users have been shown to have lower Internet skills (Hargittai, 2008; Van Deursen & Van Dijk, 2010). Such socially determined differences in skills then potentially assert themselves in manifold outcomes, not least in the level of online privacy.

The basic relationships proposed in the model combined with existing empirical work reviewed above leads us to test the following hypotheses. The first set concerns the relationship between privacy-protection behavior and Internet-use-related variables:

Online privacy protection is positively predicted by:

H1a: Privacy breach experiences

H1b: Online privacy attitudes

H1c: General Internet skills

H1d: Amount of Internet use

Further, based on research on digitally disadvantaged groups:

H2a: Age negatively predicts amount of Internet use and general Internet skills.

H2b: Being female negatively predicts amount of Internet use and general Internet skills.

H2c: Higher levels of education positively predict amount of Internet use and general Internet skills.

Additionally, the sociodemographic variables are expected to directly influence privacy protection consistent with digital inequality:

Higher levels of online privacy protection will be associated with:

H3a: Lower age

H3b: Higher education

H3c: Being male

Method

Representative Survey Data

We collected nationally-representative survey data (*N*=1121) in 2015 as part of the World Internet Project – Switzerland survey. This survey measures various aspects of Internet use and in 2015 included a module on privacy-related questions to test the proposed hypotheses of this study. Respondents were interviewed via landline or mobile phones. In this general Swiss population survey, to ensure representativeness, we constructed sampling quotas based on age, gender, region, and employment status (Latzer et al., 2015a). Analyses reported below exclude non-users of the Internet, resulting in an effective sample of 970 Internet users. This sample comprised 48% women, 36% had a tertiary education degree, and the median age was 45 years.

Data Analyses

The conceptual model presented in Figure 1 was translated into a statistical model comprising exogenous variables, mediators, and an outcome variable. The analysis thus relied on path modeling. The analytical procedure towards testing the tenability of the hypotheses was first to estimate a saturated version of the model, i.e., all exogenous variables predicted all mediators and the outcome, and all mediators predicted the outcome. In a second step, non-significant paths were removed in favor of model parsimony. We used the lavaan package in the statistical software R (Rosseel, 2012) with robust maximum likelihood estimation. We tested the adequacy of the multi-item measures with confirmatory factor analysis and assessed model fit conventional criteria in the structural equation modeling literature (Schermelleh-Engel, Moosbrugger, & Müller, 2003; Hu & Bentler, 1999).

Measures

In addition to the variables individually described below, respondents indicated their age and gender. Education was recorded using five categories. The variable was subsequently recoded into three categories, with low education serving as reference group: low (primary or secondary school), medium (vocational school, A levels degree or high school graduation), and high education (university, university of applied sciences). All other measures used multiple items (see appendix, Table A2). For online privacy protection, privacy-breach experience, online privacy attitudes and general Internet skills, we calculated mean indices for use in the path model.

Online privacy protection. The measure for individual self-help privacy protection on the Internet was constructed by adapting four items from the Pew Research Center's Internet & American Life Project (Rainie, Kiesler, Kang, & Madden, 2013) and a Eurobarometer survey on data protection (European Commission, 2011). Respondents answered on a four-point frequency scale ranging from 1 = *never* to 4 = *frequently* as to how regularly they change privacy settings, provide fake information about themselves online, manage cookies or monitor which information is available about them online. Managing cookies was the most prevalent online privacy protection measure.

Privacy breach experience. To determine whether respondents had suffered privacy violations, they were directly asked whether their privacy had been violated, their data had been abused, they had received abusive e-mails, or had been asked for banking or personal details in the past year. All four questions were answered on a binary scale where 0 = *no* and 1 = *yes*. Male Internet users reported having been subject to privacy breaches more often than female respondents. Overall, being asked for banking or personal details online was the most common privacy breach experience in the sample, with 36% of the respondents reporting this negative experience.

Online privacy attitudes. To measure individuals' privacy attitudes, we adapted four items from the Pew Research Center's Internet & American Life Project (Rainie et al., 2013). Respondents were asked about how important they think it is that only they or those they have authorized know the search queries they perform online, their location when they use the Internet, the websites they visit, and their communication partners on the Internet. The information deemed most sensitive by respondents was the identity of their interlocutor.

General Internet skills. Internet skills were measured applying a validated survey instrument for general populations (Van Deursen, Helsper, & Eynon, 2014). Originally, five different types of Internet skills were included: operational, information navigation, social, creative, and mobile. Respondents were asked to rate their ability to perform five Internet-use-related tasks by rating their agreement with statements on a five-point Likert scale (see appendix, Table A2). For operational skills (being able to open downloaded files), 73% of the sample indicated the highest level of agreement, indicating very little variation and a ceiling effect. This item was thus excluded from subsequent analyses and we proceeded with a four-item measure of general Internet skills.

Amount of Internet use. A composite variable for the amount of Internet use (Blank & Groselj, 2014) was constructed by summing the frequency (6-point scale) of engaging with a set of 37 diverse Internet applications such as checking facts, playing games, reading news, comparing products, or messaging (see Latzer, Büchi, & Just, 2015b for details on the different uses surveyed). The theoretical range of the variable was 0–185; the empirical range was 3–132 (*M* = 51, *SD* = 20).

Results

CFA of the latent multi-item measures for general Internet skills, online privacy attitudes, privacy breach experience, and online privacy protection produced a well-fitting model with (see appendix, Figure A1). Bivariate correlations among the Internet-use-related variables revealed that skills and privacy-breach experience are positively associated with use (see appendix, Table A1).

[Figure 2 here]

The paths specified in the statistical model, derived from the conceptual model developed above, fit the empirical relationships among the variables very well. Figure 2 provides a graphic representation of the main estimated paths and Table 1 lists all parameter estimates. Based on these results, we evaluate the hypotheses.

The first set of hypotheses held that privacy protection would be positively predicted by four Internet-use-related variables. The model lends clear support to these hypotheses: privacy-breach experience (*H1a*), online privacy attitudes (*H1b*), general Internet skills (*H1c*), and amount of Internet use (*H1d*) all had significant and positive effects. For example, an increase of one on the 5-point Internet skills scale was associated with a .15 increase in the level of self-help privacy protection on a 4-point scale (see Table 1)

[Table 1 here]

The second set of hypotheses concerned the effects of socio-demographic attributes on Internet-use-related variables. Older age was strongly and negatively associated with lower levels of Internet use and skills, thus *H2a* was supported. The standardized estimates for the effect of age on Internet use and skills were by far the strongest in the model. *H2b* held that being female negatively predicts the level of Internet use and skills. The results support both parts of the hypothesis as being female negatively predicted the amount of Internet use and Internet skills. *H2c* suggested a negative effect of education on the level of Internet use and skills. Medium education (vs. low and high) and high education (vs. low and medium) both significantly predicted the amount of Internet use as hypothesized (see Table 1).

The third set of hypotheses pertained to the direct effects of socio-demographic variables on the frequency of performing privacy protective actions. *H3a* was supported with age negatively affecting online privacy protection. *H3b* was only partially supported; high education had a weak but significant effect, whereas the coefficient for medium education was not significant. *H3c* was rejected because gender was not directly associated with online privacy protection (see Table 1).

Additionally, the following paths that we had not explicitly hypothesized were retained in the path model given their significant estimates. Online privacy attitudes were positively predicted by being female and having high education. Experiencing privacy breaches was predicted positively by education and being male.

At 40%, the variance (R^2) explained in the outcome variable (online privacy protection) was very high. The general Internet usage variables (amount and skills) were strongly dependent on sociodemographics (R^2 of 26% and 23%, respectively), whereas the explained variance in the privacy-related mediators was comparably low (R^2 of 7% for privacy breach experience and 1% for privacy attitudes).

Discussion and Conclusion

Understanding what factors inhibit privacy protection may provide a basis for improvements in privacy practice and policy. To this end, this chapter uniquely conceptualized online privacy from a digital inequality perspective. It provides nationally representative data from Switzerland for an explanatory model of self-help online privacy protection. Using multi-indicator variables and path modeling, the results reveal distinct pathways to online privacy relevant for digital inequality and corresponding policies. The results show that pro-privacy attitudes, experiences of privacy breaches, the amount of Internet use, and general Internet skills all related to increased privacy-protective behaviors. Amount of use and skills were themselves highly dependent on sociodemographic attributes with younger, male, and more educated users reporting higher values. Additionally, lower age and higher education were directly associated with higher frequency of privacy protection. Older age was directly linked to lower self-help privacy protection. Age also exhibited a strong indirect negative relationship with privacy protection via amount of Internet use and Internet skills. Low-use and low-skilled older Internet users thus represent a social group particularly vulnerable to experiencing negative Internet outcomes.

While educational reforms have started to include digital skills development in schools—for example by addressing safe social network site use—skills training for older Internet users remains challenging, and informal social support plays a major role (Courtois & Verdegem, 2016; König, Seifert, & Doh, 2018). Furthermore, and independent of age, digital inequalities in online privacy are also salient with regards to Internet skills and level of education.

To the extent that self-help measures of online privacy protection prove effective, the analysis shows that digital inequalities in Internet use carry over to relevant outcomes, in this case the protection of personal data. Because privacy and control over one's personal data relate to social power and discrimination, inequalities emerging from online behavior on top of long-standing forms of social inequality are problematic. In addition to deeply rooted social inequalities, digital inequalities, in particular in Internet skills, warrant attention. Privacy breaches are one important way in which Internet use and related variables can negatively affect individuals' well-being and ultimately feed back into life chances and social stratification. Accordingly, it is an area where existing inequalities are of concern and need to be addressed both by policy and future research.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9). http://journals.uic.edu/ojs/index.php/fm/article/view/1394/1312

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication, 67*(1), 26–53. https://doi.org/10.1111/jcom.12276

Bennett, C. J., & Raab, C. D. (2003). *The governance of privacy: Policy instruments in global perspective*. Burlington, VT: Ashgate.

Blank, G., & Groselj, D. (2014). Dimensions of Internet use: Amount, variety, and types. *Information, Communication & Society, 17*(4), 417–435. https://doi.org/10.1080/1369118X.2014.889189

Büchi, M., Just, N., & Latzer, M. (2017). Caring is not enough: The importance of Internet skills for online privacy protection. *Information, Communication & Society, 20*(8), 1261–1278. http://dx.doi.org/10.1080/1369118X.2016.1229001

Chen, H., Beaudoin, C. E., & Hong, T. (2016). Protecting oneself online: The effects of negative privacy experiences on privacy protective behaviors. *Journalism & Mass Communication Quarterly, 93*(2), 409–429. https://doi.org/10.1177/1077699016640224

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy protection. *Computers in Human Behavior, 81,* 42–51. https://doi.org/10.1016/j.chb.2017.12.001

Courtois, C., & Verdegem, P. (2016). With a little help from my friends: An analysis of the role of social support in digital inequalities. *New Media & Society, 18*(8), 1508–1527. https://doi.org/10.1177/1461444814562162

Ellison, N. B., Vitak, J., Steinfield, C., Gray, R., & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environment. In S. Trepte & L. Reinecke (Eds.), *Privacy online* (pp. 19–32). Berlin, Heidelberg, DE: Springer Verlag. https://doi.org/10.1007/978-3-642-21521-6_3

European Commission (2011). Special Eurobarometer 359: Attitudes on data protection and electronic identity in the European Union. Retrieved from http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

Hargittai, E. (2008). The digital reproduction of inequality. In D. Grusky (Ed.), *Social stratification* (pp. 936–944). Boulder, CO: Westview Press.

Hargittai, E., & Marwick, A. (2016). "What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication, 10*, 3737–3757.

Heller, C. (2011). *Post-privacy*. Munich, DE: C.H. Beck.

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling, 6*(1), 1–55. https://dx.doi.org/10.1080/10705519909540118

Just, N. (2018). Governing online platforms: Competition policy in times of platformization. *Telecommunications Policy*. https://doi.org/10.1016/j.telpol.2018.02.006

Kokolakis, S. (2017). Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

König, R., Seifert, A., & Doh, M. (2018). Internet use among older Europeans: An analysis based on SHARE data. *Universal Access in the Information Society.* https://doi.org/10.1007/s10209-018-0609-5

Latzer, M., Büchi, M., & Just, N. (2015a). Vertrauen und Sorgen bei der Internet-Nutzung in der Schweiz 2015. Themenbericht aus dem World Internet Project – Switzerland 2015. University of Zurich, Zurich. Retrieved from http://mediachange.ch/media//pdf/publications/Vertrauen_Sorgen_2015.pdf

Latzer, M., Büchi, M., & Just, N. (2015b). Internet-Anwendungen und deren Nutzung in der Schweiz 2015. Themenbericht aus dem World Internet Project – Switzerland 2015. University of Zurich, Zurich. Retrieved from http://mediachange.ch/media//pdf/publications/Anwendungen_Nutzung_2015.pdf

Latzer, M., Hollnbuchner, K., Just, N., & Saurwein, F. (2016). The economics of algorithmic selection on the Internet. In J. Bauer & M. Latzer (Eds.), *Handbook on the economics of the Internet* (pp. 395–425). Cheltenham, Northhampton, UK: Edward Elgar.

Latzer, M., Just, N., Saurwein, F., & Slominski, P. (2003). Regulation remixed: Institutional change through self and co-regulation in the mediamatics sector. *Communications & Strategies, 50*(2), 127–157.

Li, X., Chen, W., & Straubhaar, J. (2018). Concerns, skills, and activities: Multilayered privacy issues in disadvantaged urban communities. *International Journal of Communication, 12*, 1269–1290.

Litt, E., & Hargittai, E. (2014). A bumpy ride on the information superhighway: Exploring turbulence online. *Computers in Human Behavior, 36*, 520–529. https://dx.doi.org/10.1016/j.chb.2014.04.027

Madden, M., Gilman, M., Levy, K., & Marwick, A. (2017). Privacy, poverty, and big data: A matrix of vulnerabilities for poor Americans. *Washington University Law Review, 95*(1), 53–125.

Madden, M., Lenhart, A., Cortesi, S., & Gasser, U. (2013). Teens and mobile apps privacy. Washington, DC: Pew Research Center. Retrieved from http://www.pewinternet.org/2013/08/22/teens-and-mobile-apps-privacy

Marwick, A. E., & boyd, d. (2018). Understanding privacy at the margins. *International Journal of Communication, 12*, 1157–1165.

Matzner, T., Masur, P. K., Ochs, C., & von Pape, T. (2016). Do-it-yourself data protection – empowerment or burden? *Law, Governance and Technology Series, 24,* 277–305. https://doi.org/10.1007/978-94-017-7376-8_11

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

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. doi:10.1111/j.1745-6606.2006.00070.x

O'Neil, C. (2016). *Weapons of math destruction: how big data increases inequality and threatens democracy*. New York, NY: Crown.

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

Park, Y. J. (2015). Do men and women differ in privacy? Gendered privacy and (in)equality in the Internet. *Computers in Human Behavior, 50*, 252–258. https://doi.org/10.1016/j.chb.2015.04.011

Penney, J. W. (2017). Internet surveillance, regulation, and chilling effects online: a comparative case study. *Internet Policy Review*, *6*(2), 1–39. https://doi.org/10.14763/2017.2.692

Preibusch, S. (2015). Privacy Behaviors After Snowden. *Communications of the ACM*, *58*(5), 48–55. https://doi.org/10.1145/2663341

Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013). Anonymity, privacy, and security online. Washington, DC: Pew Research Center. Retrieved from http://pewinternet.org/Reports/2013/Anonymity-online.aspx

Regan, P. M. (1995). *Legislating privacy: Technology, social values, and public policy.* Chapel Hill, NC: University of North Carolina Press.

Reinecke, L., & Oliver, M. B. (2017). *The Routledge handbook of media use and well-being: International perspectives on theory and research on positive media effects.* London, UK: Routledge.

Rosseel, Y. (2012). lavaan: An R package for structural equation modeling. *Journal of Statistical Software, 48*(2), 1–36.

Roßnagel, A. (1997). Globale Datennetze: Ohnmacht des Staates — Selbstschutz der Bürger: Thesen zur Änderung der Staatsaufgaben in einer „civil information society“. *Zeitschrift für Rechtspolitik, 30*(1), 26–30.

Schermelleh-Engel, K., Moosbrugger, H., & Müller, H. (2003). Evaluating the fit of structural equation models: Tests of significance and descriptive goodness-of-fit measures. *Methods of Psychological Research Online, 8*(2), 23–74.

Solove, D. J. (2015). The meaning and value of privacy. In B. Roessler & D. Mokrosinska (Eds.), *Social dimensions of privacy: Interdisciplinary perspectives* (pp. 71–81). Cambridge, UK: Cambridge University Press. https://doi.org/10.1017/CBO9781107280557

Stutzman, F., Gross, R., & Acquisti, A. (2012). Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of Privacy and Confidentiality, 4*(2), 7–41.

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. https://doi.org/10.1111/jcc4.12052

Tufekci, Z. (2012). Facebook, Youth and Privacy in Networked Publics. In *Proceedings of the Sixth International AAAI Conference on Weblogs and Social Media*. Dublin, Ireland: AAAI Press. Retrieved from https://www.aaai.org/ocs/index.php/ICWSM/ICWSM12/paper/view/4668

Van den Hoven, J. (2008). Information technology, privacy, and the protection of personal data. In J. Van den Hoeven & J. Weckert (Eds.), *Information technology and moral philosophy* (pp. 301–321). Cambridge, UK: Cambridge University Press.

Van Deursen, A., & Van Dijk, J. (2010). Internet skills and the digital divide. *New Media & Society, 13*(6), 893–911. https://doi.org/10.1177/1461444810386774

Van Deursen, A., Helsper, E. J., & Eynon, R. (2014). Measuring digital skills: From digital skills to tangible outcomes project report. Retrieved from www.oii.ox.ac.uk/research/projects/?id=112

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society, 12*(2), 197–208.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193–220.

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook. *Information, Communication & Society, 16*(4), 479–500. https://doi.org/10.1080/1369118X.2013.777757

Table 1

Parameter Estimates of the Path Model

		Unstandardized	SE	*z*	*p*	Standardized
Regressions						
protection	←					
	use	0.006**	0.001	5.217	<.001	0.179
	attitudes	0.111**	0.016	6.895	<.001	0.171
	skills	0.15**	0.024	6.147	<.001	0.201
	experience	0.158**	0.018	8.583	<.001	0.237
	age	-0.01**	0.001	-8.26	<.001	-0.247
	educ.high	0.085*	0.038	2.228	0.026	0.057
use	←					
	age	-0.573**	0.031	-18.614	<.001	-0.5
	female	-6.841**	1.114	-6.138	<.001	-0.169
	educ.med	4.982**	1.666	2.99	0.003	0.123
	educ.high	9.613**	1.793	5.362	<.001	0.231
attitudes	←					
	female	0.173*	0.071	2.418	0.016	0.077
	educ.high	0.203**	0.073	2.789	0.005	0.088
skills	←					
	age	-0.027**	0.002	-16.583	<.001	-0.479
	female	-0.179**	0.056	-3.216	0.001	-0.092
	educ.med	0.338**	0.082	4.114	<.001	0.173
	educ.high	0.625**	0.085	7.38	<.001	0.31
experience	←					
	female	-0.381**	0.067	-5.646	<.001	-0.175
	educ.med	0.221*	0.098	2.248	0.025	0.101
	educ.high	0.552**	0.103	5.379	<.001	0.246
Covariances						
use	↔					
	skills	6.653**	0.541	12.294	<.001	0.448
	experience	4.555**	0.616	7.392	<.001	0.25
	attitudes	1.945**	0.647	3.007	0.003	0.101
skills	↔					
	experience	0.147**	0.028	5.255	<.001	0.163
attitudes	↔					
	skills	0.083*	0.033	2.536	0.011	0.087
	experience	0.186**	0.036	5.187	<.001	0.159

Note. χ^2 (5, N = 970) = 6.00, p = 0.307, χ^2 / df = 1.20, CFI = .999, TLI = .996, RMSEA = .014, SRMR = .010. See Figure 2 for graphic representation. * p < .05. ** p < .01.

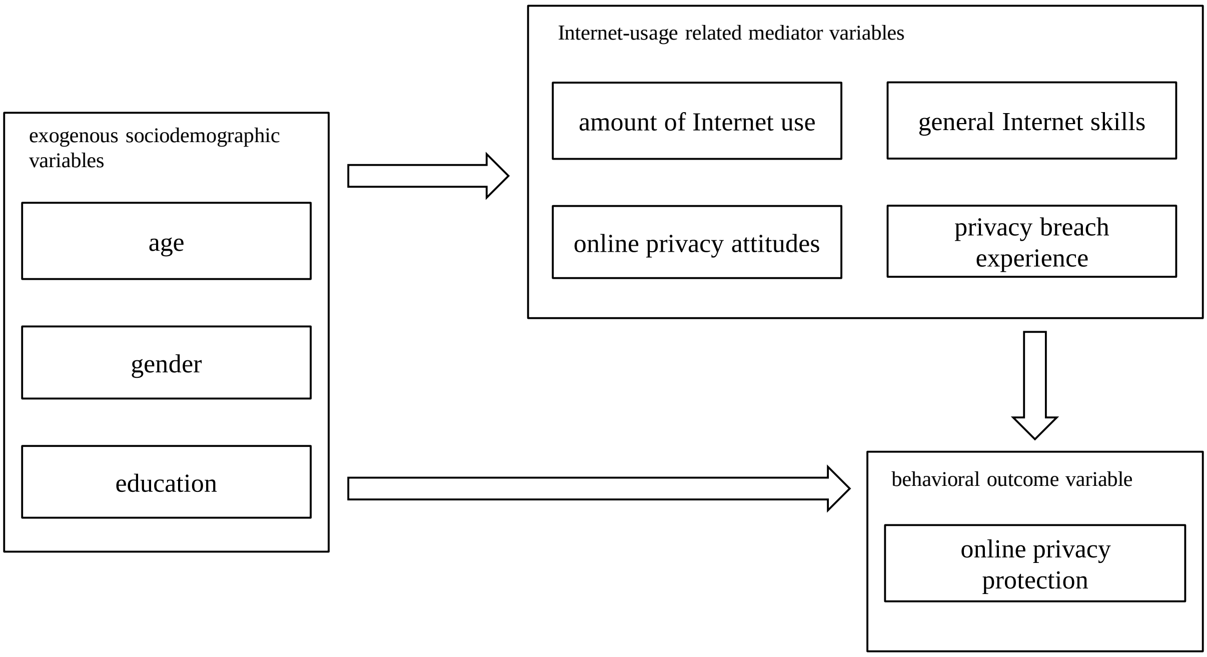
Internet-usage related mediator variables
amount of Internet use
general Internet skills
online privacy attitudes
privacy breach experience
exogenous sociodemographic variables
age
gender
education
behavioral outcome variable
online privacy protection

Figure 1. Conceptual model to explain online privacy protection.

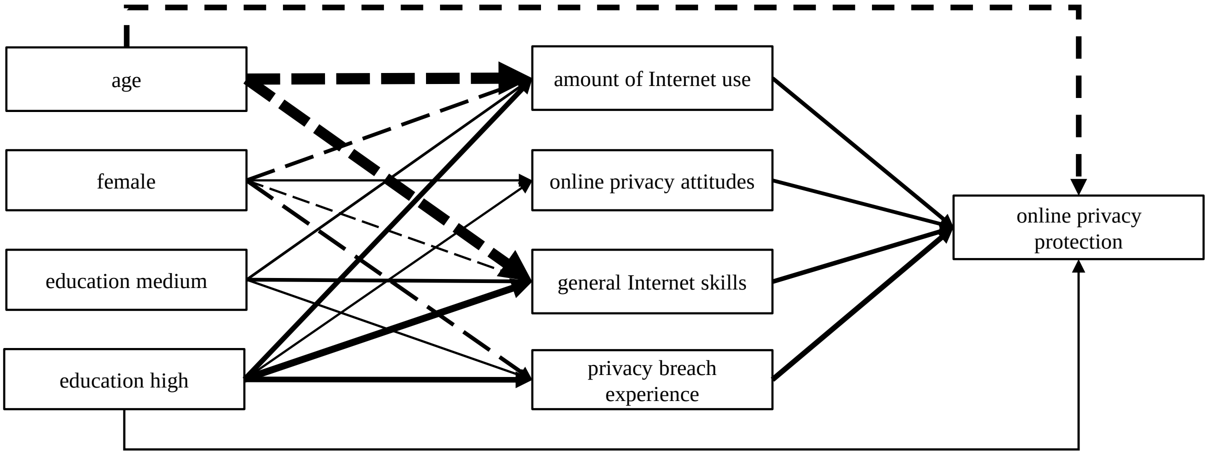

Figure 2. Path model (empirical test of the conceptual model presented in Figure 1). Solid lines indicate positive significant regression coefficients; dashed lines indicate negative significant regression coefficients. Line width is scaled to the standardized regression estimate, i.e. thicker lines indicate stronger effects. Covariances among the exogenous variables and among the mediators are not shown but were also modeled. See Table 1 for full model results.

Appendix

Table A1

Means, standard deviations, and zero-order correlations of the variables in the path model

Variable	*M*	*SD*	1	2	3	4	5	6	7	8
1. age	44.39	17.62								
2. female	0.48	0.50	-.01							
3. education high	0.38	0.49	.18**	-.10**						
4. education medium	0.47	0.50	.01	.10**	-.73**					
5. amount of Internet use	51.30	20.29	-.46**	-.17**	.07*	-.06*				
6. online privacy attitudes	3.77	1.12	-.01	.07*	.08*	-.04	.09**			
7. general Internet skills	3.70	0.98	-.42**	-.10**	.10**	-.07*	.58**	.09**		
8. privacy breach experience	1.07	1.09	.02	-.19**	.19**	-.09**	.26**	.16**	.19**	
9. online privacy protection	2.01	0.73	-.40**	-.08*	.10**	-.07*	.49**	.25**	.47**	.35**

Note. * *p* < .05. ** *p* < .01.

Table A2

Measurement item details

Latent variable	Item	Wording	Scale	M (SD)
General Internet Skills	infnavskill	*I find it easy to decide on the best keywords for web search.*	5-point	3.9 (1.0)
	creativeskill	*I know how to create and upload content.*	5-point	3.0 (1.6)
	mobileskill	*I know how to download apps to a mobile device.*	5-point	3.9 (1.5)
	socialskill	*I know how to change who I share content with.*	5-point	3.4 (1.5)
Online Privacy Attitudes	searchhist	*How important is it for you that only you or people you authorize know which search queries you perform?*	5-point	3.5 (1.4)
	location	*…where you are located when using the Internet?*	5-point	3.6 (1.4)
	visit	*…which websites you visit?*	5-point	3.7 (1.4)
	emailto	*…with whom you communicate over the Internet?*	5-point	3.9 (1.4)
Privacy Breach Experience	infabuse	*Thinking of the past year, did you feel that your personal data was passed on or abused?*	binary	0.31 (0.46)
	abusemail	*…have you ever received obscene or abusive e-mails?*	binary	0.29 (0.45)
	netscam	*…been contacted by someone online asking for bank or personal details in the past year*	binary	0.36 (0.48)
	breach	*Have you ever had your privacy violated online?*	binary	0.11 (0.31)
Online Privacy Protection	settings	*Do you change settings so that content is only visible to specific people?*	4-point	1.9 (1.2)
	fakename	*Do you use fake information online such as a fake name?*	4-point	1.5 (0.90)
	cookies	*Do you block, delete, or deactivate cookies?*	4-point	2.7 (1.2)
	monitor	*Do you monitor which information is available about you online?*	4-point	2.0 (0.98)

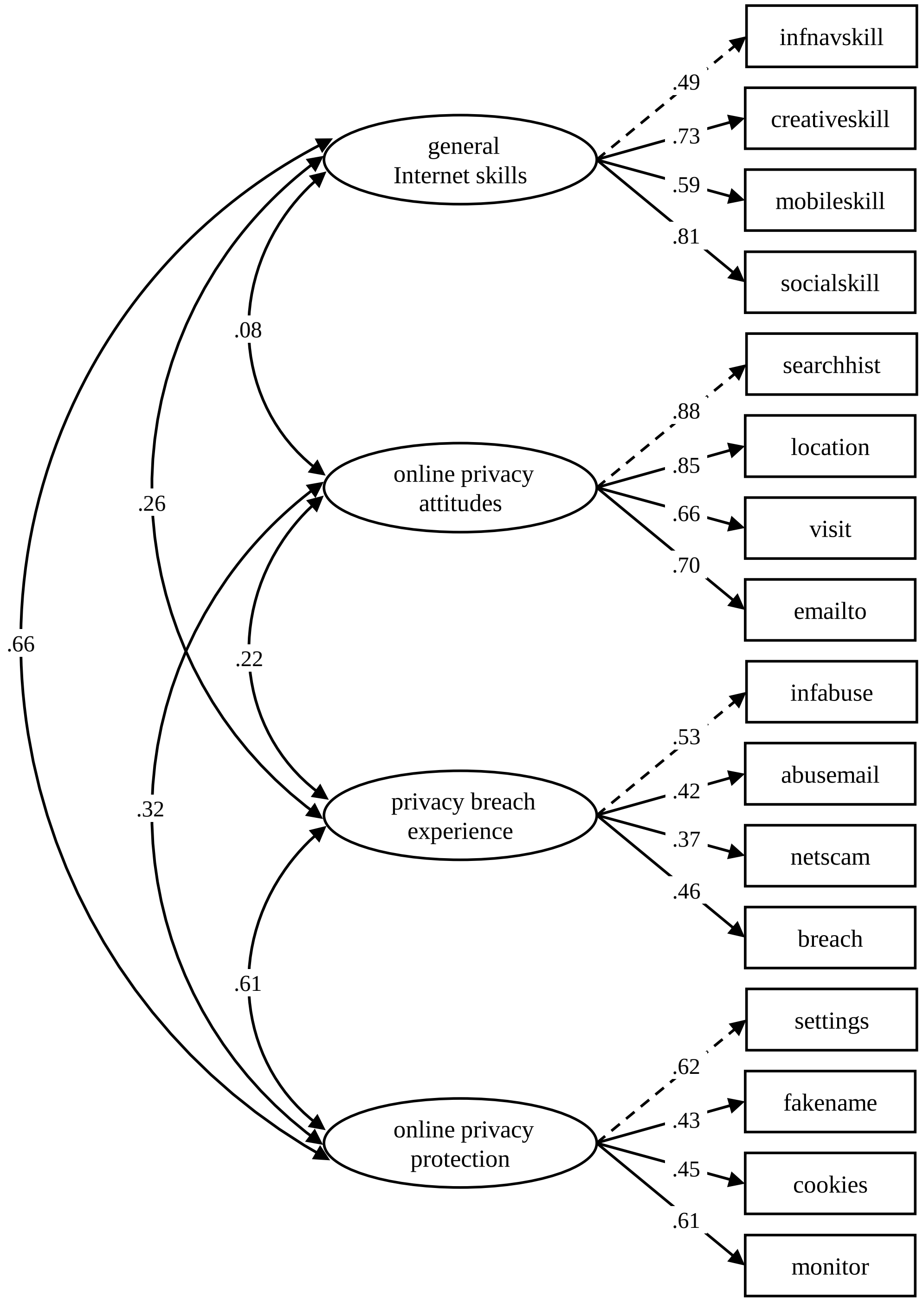

Figure A1. Confirmatory factor analysis for the correlated four-factor latent measurement model. See Table A2 for item details. Standardized coefficients are shown; dashed lines indicate reference items (unstandardized factor loading fixed to 1). Model fit: χ^2 (98, N = 970) = 180.81, p < 0.001, χ^2 / df = 1.85, CFI = .976, TLI = .971, RMSEA = .030, SRMR = .032.