Predicting teens' privacy management and attitude towards data protection on social media

Abstract

This study contributes to ongoing debates on the protection of teens' privacy on social media. While ample research is focused on teens' privacy management, less is known about their attitude towards data protection. Drawing from cross-sectional survey data (N = 1113), this study examines whether predictors of privacy management, namely privacy literacy, privacy concern and perceptions of data control also predict teens' attitude towards data protection. Structural equation modeling indicates that all three factors positively predict this facet of privacy. No significant differences were found in the strength of predictors for boys versus girls for privacy management, although the findings do suggest some gender differences for attitude towards data protection that call for further research.

Key words. Data protection, privacy, privacy management, data control, privacy literacy, teens

Predicting teens' privacy management and attitude towards data protection on social media

In May 2018 the General Data Protection Regulation (GDPR) entered into force in Europe. The GDPR aims to increase awareness and transparency about the ways data are collected and used in social media and other data-driven platforms and technologies, thereby enhancing individual control over personal data.[1] The GPDR has proven to be impactful for organizations handling personal data, but much remains to be seen about how it impacts individuals, especially young persons. One aspect in which such individual impact might be observed, is in the attitude one develops towards data protection.

Research on how people value institutional or governmental data protection is limited and mostly focused on adults. According to the Eurobarometer survey, 67% of the Europeans above the age of 16 have heard of the GDPR, and 71% of them have heard about their national data protection authority.[2] Bauer et al. hypothesized that the implementation of the GDPR in Europe would increase individuals' trust in data collectors.[3] Based on a panel survey and survey experiment among adults in Germany, however, no evidence was found to support this hypothesis. Strycharz et al. investigated individual knowledge and perceptions of the adult population toward the GDPR in The Netherlands.[4] While general awareness and knowledge about the data legislation was found, participants also showed reactance against the GDPR, and were doubtful about its effectiveness. Similarly, a survey report carried out by Deloitte in 8 European countries revealed that 58% of their adult respondents found the GDPR to have only limited or no effect on the ways organizations handle personal information.[5]

The findings in the literature on adults thus suggest limited awareness and knowledge of data protection. Research on young people is mostly missing. Teens specifically, are portrayed as vulnerable for online privacy risks, as they are considered as reckless and unconcerned with regard to their privacy management behavior.[6] Empirical research, however, presents a more nuanced image, showing that teens do care about privacy.[7] While teenagers' privacy management has been extensively studied[8], however, little is known about their attitude towards data protection in the context of social media.

This is unfortunate, as the dominant focus on teens' (lacking) privacy management might forego the possibility that teens perhaps most of all want their privacy to be protected by the companies handling their data. It is also relevant to know whether factors commonly known to predict teenagers' privacy management also predict their attitude towards data protection, as this knowledge may support the implementation and reinforcement of regulations such as the GPDR, in turn benefitting teens' privacy and thereby our future society.

Drawing from the findings of a large-scale survey study (N = 1113), we examine and compare the predictors of teens' privacy management and attitudes towards data protection, including privacy literacy[9,10] and privacy concern.[7,11,12]

Theoretical Background and Hypotheses

Explaining privacy management and attitude towards data protection

The individual management of personal information and access control on social media platforms are important components of privacy. Several authors have argued, however, that we should be careful to not equate these behaviors with privacy altogether, as privacy is as much a matter of what society deems appropriate to protect.[13,14,15] Nonetheless, a control-rhetoric is especially present when discussing teens' social media practices. On the topic De Wolf & Joye argued how "Privacy is seen as a matter of individual control, and young people are viewed as unconcerned. When arguing that young people do not care about privacy because they lack control over their personal information, it is also assumed that privacy equals control and vice versa."[6] We find it striking that in these discussions the role of institutional data protection is often not addressed. As this aspect may be crucial, it is important to also investigate how young people think and feel about it.

While privacy management, or personal privacy management[7], encompasses how individuals managing their data and privacy, attitude towards data protection investigates how people value the institutional protection of their personal data. A fundamental difference between the concepts is that privacy management emphasizes individual responsibility, for instance by using privacy controls

provided by service providers, while attitude towards data protection investigates how people value a regulatory framework that protects their privacy and/or facilitates their privacy management (e.g. one's right to object to receiving direct marketing or the right to control personal data if it is wrong).

To understand teens' attitude towards data protection and its predictors, we build on the premises of the privacy calculus model[16] and the protection motivation theory (PMT)[17] – because it is not always straightforward for end-users to calculate risks and benefits. [18]

The privacy calculus model argues that people balance how much they disclose about themselves based on a cost-benefit trade-off.[16] People share more information when the benefits (e.g., free access to a platform) outweigh the costs (e.g., privacy concerns). An important premise of the privacy calculus model is that people are rational beings who can calculate risks and benefits to achieve their desired degree of privacy. Similar to privacy management, data protection can be seen as an outcome that teenagers, and people in general, desire as rational agents. Both contribute to the greater good of safeguarding one's privacy.

Because it is not always straightforward for end-users to calculate risks and benefits, however, the PMT underlines the importance of investigating predispositions that might explain interindividual differences, including both coping and threat appraisals.[17,19,20] Coping appraisal, or the cognitive evaluation of one's capacity to execute the necessary responses (=self-efficacy) as well as the effectiveness of these responses (=response efficacy), are especially relevant in this regard. Privacy literacy is defined "as a combination of factual or declarative ('knowing that') and procedural ('knowing how') knowledge about online privacy."[9] Perceived behavioral control or perceived controllability refers to "whether people believe that they have volitional control over performances of behavior".[21] Privacy researchers have used this concept as a starting point to investigate perceived data control,[22,23] or the extent to which people believe that they have meaningful control over personal data. Following PMT, we treat privacy literacy as a component of self-efficacy and perceived data control as an

important component of response efficacy that may influence privacy management and attitude towards data protection.

In addition to a coping appraisal the PMT also delineates threat appraisals that are likely to influence attitudes towards behavior.[19] These are more focused on how individuals deal with threats and risks. Privacy concern, or one's "belief about the risks and potential negative consequences associated with sharing information"[8], is often regarded as a critical factor explaining privacy management behavior.[7,8,11] It may also predict teenagers' attitude towards data protection, as more concerned teens may also have a more outspoken opinion on companies' institutional responsibility to protect their privacy.

Figure 1 gives an overview of the variables. Below we further define the variables and discuss how we expect these to be related to privacy management and attitude towards data protection. It should be noted, as both privacy management and data protection are ways to protect one's privacy, we do not expect major differences in their relationship with the independent variables.

-- Insert Figure 1 --

Hypotheses

Prior research found a discrepancy between teens' privacy concerns and their behaviors (cfr. Privacy paradox)[24], motivating scholars to research the role of privacy literacy as a predictor of privacy management.[25] Echoing the PMT, privacy management and attitude towards data protection could be explained by one's factual, declarative and procedural knowledge about privacy. After all, Bartsch and Dienlin found that privacy literacy and privacy management positively relate to one another: people who change their privacy settings more frequently show higher levels of privacy literacy and vice versa.[10]

Other research focusing on differences between young adults found that while different age groups are comparable in terms of their privacy literacy, their privacy protective behaviors do differ.[26] In addition, higher levels of privacy literacy make users feel safer when using social media. Similar results

were found by Park,[27] Masur et al.,[28] and Baruh et al.[8]. We expect a positive relationship between privacy literacy and privacy management, and privacy literacy and attitude towards data protection.

H1. Privacy literacy positively predicts privacy management (H1a) and attitude towards data protection (H1b).

PMT considers the perceived effectiveness of protective behavior to be a good predictor for protective attitudes and behaviors.[20] Perceived control positively predicts the perceived security an individual experiences.[29] Therefore, we could argue that teens are less eager to value data protection when they already feel more in control. After all, Bartsch and Dienlin found that users who report a higher perceived control report greater safety in terms of their online privacy.[10] Hajli and Lin also found that perceived control positively predicted an individuals' intention to share information confirming that some deem their data to be protected enough.[30] Nevertheless, teens may also perceive data protection as complementary to their control over personal data. In short, we expect a relationship between perceived data control and attitude towards data protection but do not yet specify its direction.

H2a. Perceived data control positively predicts privacy management (H2a) and relates to attitude towards data protection (H2b).

PMT also argues that how concerned individuals are about a privacy issue is a good predictor for protective attitudes and behaviors. Hence, privacy concern is likely to influence privacy management and attitude towards data protection. Dienlin and Trepte indeed found privacy concern to be a positive, but weak predictor for attitudes towards privacy behavior.[31] Equally, Kokolakis[32] and Baruh et al.[8] found that privacy concerns are positively related to protective measures use. Blank et al.[33], who focused on young people and their privacy on SNS, found that young people are more likely to take privacy protective action than older people. Therefore, we expect teenagers to be rational in their behaviors and attitudes and predict a positive relationship between privacy concern and the two dependent variables.

H3. Privacy concern positively predicts privacy management (H3a) and attitude towards data protection (H3b)

Studies have found that women experience more online privacy breaches and express more privacy concerns than men.[34] This is also true for young women. Considering how they are more likely to be the victim of privacy violations such as video voyeurism and revenge porn, Marwick argues to be mindful of the structural gender inequality between men and women.[35] When looking at the privacy behavior of women it is therefore not surprising to see how they are more likely to have a private profile and are more cautious to whom they allow access to their personal information.[12,34,36] How women value data protection in comparison to men is currently unknown, as well as what explains changes in their attitude towards data protection.

RQ1. "Do boys and girls differ in their privacy management and attitude towards data protection, and are there gender differences in the factors predicting these variables?"

Methods

Data Collection and Sample

The data were collected in schools in October and November 2019 as part of a larger study on teenagers' digital media lives. In accordance with European and national regulation, parental consent was obtained for all teenagers younger than 16 years using a paper-and-pencil form. Consent from the participating teenagers was collected prior to starting the online Qualtrics questionnaire, which they completed during class hours. In total we collected responses from 4255 teens, of whom 1113 were asked to fill in questions with concern to privacy management and attitude towards data protection. This subsample of 1113 teens was representative for age, gender and school track for [omitted]. The sample consisted of 51% girls and 49% boys, who were between 10 and 20 years old (M=16.05, SD=2.08). Our sample consists of mainly heavy social media users, with 81,9% of them using Facebook, TikTok or Instagram at least daily. About one in four teens in our sample (26,8%) indicated to have

previously heard of the GPDR, while 73,2% were ignorant of the data legislation. As no differences were found between both groups (except for a minor difference with concern to privacy literacy) we did not split up the sample in the result section.

Measures

An exploratory factor analysis (EFA) was conducted with a promax rotation. The KMO measure ensured an adequate sample for the analysis (KMO=.878). The Bartlett's test for sphericity (χ^2=15313.30, p<.001) indicated a good correlation structure for factor analysis. Using a cut-off point of .60, and a minimal eigenvalue of 1, the minimum residual factor analysis yielded the expected 5 factors as the best fit for our data. All items fitted their expected factor, but three items did not meet our .60 factor loading cut-off point. Two items from privacy management and one item from privacy literacy were, therefore, excluded from our analysis. The results of the exploratory factor analysis is shown in Table 1.

--Table 1--

Table 2 shows a detailed description of the study measures. All items used a 5 point-Likert scale. To operationalize *privacy management* we made use of the five-item personal privacy management scale of De Wolf.[7] Three items were retained with factor loadings ranging from .694 to .755 (α = .76, M=3.64, SD=.96).

The five-item *attitude towards data protection* measure investigates how data protection is valued. We formulated specific items that measure how important various elements of GDPR legislation are regarded. The factor loadings for data protection attitudes ranged between .770 and .883, all items were retained (α = .92, M=3.64, SD=.93).

To measure *privacy literacy* we used the privacy literacy scale of Bartsch and Dienlin[10], which focuses on the knowledge that people have to delete or deactivate their account or to restrict access

to profile information among other things ("knowing how").[9] Four items were retained with factor loadings ranging between .688 and .790 (α = .89, M=3.80, SD=.89).

To measure *perceived data control* we used four items from Xu's perceived data control scale[37], which was initially used in the context of location-based services, but later also applied in the context of social media.[12,38] As the factor loadings of the items for data control ranged between .845 and .895, all items were retained (α = .93, M=2.93, SD=1.08; 1 = totally disagree, 5 = totally agree).

To measure *privacy concern* we used the privacy concern scale of Xu and colleagues.[38] Factor loadings of the items ranged between .776 and .901, and were thus all retained (α = .91, M=3.18, SD=1.04).

-- TABLE 2 --

Analysis

To address the study objectives, we analyzed the proposed model using AMOS to construct our structural equation model (SEM). We checked the goodness-of-fit of the measurement model and the structural model with the TLI, CFI and RMSEA indices.

Results

Model

The goodness of fit indices of the measurement model exceeded the cutoff value of 0.95 for the TLI and CFI indices and were lower than the .06 cutoff for RMSEA, indicating a good fit (CFI= 0.963, TLI=0.957, RMSEA = 0.030).[39] The model-fit of the general model, as presented in figure 1, also showed good fit (CFI= 0.968, TLI=0.962, RMSEA = 0.051) . A Harman's single factor test showed no indication of a substantial common method bias in our data.[40] At most 27.7% of the variance was accounted for by one factor, moreover, there were no very high correlations (>.90) present between any pair of constructs in our data.

In Table 3, we included the correlations between the study variables. There are significant correlations between most of the variables. The strongest correlations were found between data protection attitude and privacy management (.312***), data protection management and privacy concern (.305***), and privacy management and perceived data control (0.296***). Privacy concern did not correlate with perceived data control or privacy literacy. All other variables correlated to some extent (see table 3).

-- TABLE 3 --

Predictors for Privacy Management and Attitude towards Data Protection

All predictors significantly predicted privacy management as well as attitude towards data protection. For privacy management, privacy concern was the strongest predictor ($\beta = .255, p < .001$), followed by perceived data control ($\beta = .210, p < .001$) and privacy literacy ($\beta = .205, p < .001$). 27% of the variance of privacy management was explained by all three predictors, supporting H1a, H2a and H3a. Only 17% of attitude towards data protection was explained with privacy concerns as the strongest predictor ($\beta = .249, p < .001$), followed by privacy literacy ($\beta = .166, p < .001$) and data control ($\beta = .107, p < .001$), supporting H1b, H2b and H3b. Teens' privacy management and their attitude towards data protection were also significantly and positively related (r = .111, p < .001).

Comparing the Predictors of Privacy Management Attitude towards Data Protection Between Girls and Boys

Independent samples t-tests revealed that boys and girls did differ in terms of their privacy management (t(1111)=4.140, p<.001) and attitude towards data protection (t(1111)=2.772, p<.01). When comparing the models between boys and girls, the predictors for privacy management mostly aligned. A multi-group analysis comparing the models of boys and girls revealed no significant differences in terms of the predictors of privacy management (see table 4).

For the predictors of attitude towards data protection however, the multi-group analysis revealed significant differences (see table 4). Privacy concern ($\beta = .222, p < .001$) and perceived data control ($\beta = .153, p < .001$) predicted 16% of the variance, while privacy literacy was no significant predictor of attitude towards data protection for girls. For boys, 17% of the attitude towards data protection was explained by privacy concern ($\beta = .264, p < .001$) and privacy literacy ($\beta = .226, p < .001$), while perceived data control was no significant predictor. Apart from the difference in which predictors were significant for each gender, no significant differences were found between the constrained model for privacy concern between boys and girls. Overall, the results show a difference between the model to predict attitude towards data protection but no difference between the model to predict privacy management between boys and girls.

-- TABLE 4 --

Discussion

Scope and Findings

The bulk of the work on teens' privacy in the context of social media investigates their (individual) privacy management.[7,8] Although this is valuable, we also find it necessary to investigate whether and how teens want to be protected. Building further on the privacy calculus model[16] and the PMT[17] we argued how both privacy management and data protection are adequate protective responses. We then hypothesized three main predictors of these responses, namely privacy literacy, perceived data control, and privacy concern.

Overall, the findings of our study show how attitude towards data protection is explained in a similar way as privacy management, with privacy literacy, perceived data control and privacy concern as positive predictors. In line with most other studies[8,11], privacy concern was found the strongest predictor of privacy management, but also of attitude towards data protection. Privacy literacy and perceived data control have a somewhat stronger role in predicting privacy management than in predicting attitude towards data protection. This might be explained by the fact that privacy

management requires concrete actions of an individual, whereas data protection is less dependent on individuals and largely guaranteed for them. Finally, we found no substantial differences between the predictors of privacy management between boys and girls. Privacy literacy plays a somewhat more important role in explaining the attitude towards data protection of boys than of girls, whereas for perceived data control it is the other way around.

Limitations and Recommendations

Our research suggests that cognitions, attitudes and behaviors in relation to privacy cluster together. However, there are likely relevant between-person differences that require deeper investigation. We advise future research endeavors to further focus on explaining attitude towards data protection and actual data protection behaviors (for example, ask a particular service provider to access one's data or rectify certain data), while also taking into account other factors that are typically included in PMT models such as perceived severity and vulnerability.[17]

This study explored a limited set of independent variables. Knowing that privacy behaviors are highly contextual[14] and contingent on cultural, social, economic, political, and technological factors, a comparative privacy research framework[42] would be valuable to implement. Such an approach would allow to see how different structures, cultures, and/ or actors (like peers or parents) influence teens' attitude towards data protection. Finally, the field of behavioral economics has demonstrated how teens are prone to judgement errors and decision-making biases when managing their privacy.[42] For example, teens tend to incur long-term costs (e.g., intrusive profiling) in exchange for small immediate benefits (e.g., coupons) in privacy decision making. It could be that such a present-bias also affect the attitude towards data protection. For example, being irritated by cookie alerts (small costs) versus overall transparency of service providers and the ways they handle personal information (long-term benefits).

References

1. European Commission. 'Joint Statement by First Vice-President Timmermans, Vice-President Ansip, Commissioners Jourová and Gabriel ahead of Data Protection Day'; 2019.
2. European Commission. Special Eurobarometer 487a: The General Data Protection. Regulation.https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/86886 ; 2019.
3. Bauer P, Gerdon F, Keusch F Did the GDPR increase trust in data collectors? Evidence from observational and experimental data. *Information, Communication & Society*, 2021; DOI: 10.1080/1369118X.2021.1927138
4. Strycharz J, Ausloos J, Helberger N. Data protection or data frustration? Individual perceptions and attitudes towards the GDPR. *Eur. Data Prot. L. Rev* 2020; 6: 407-421.
5. Deloitte. A New Era for Privacy: GDPR Six Months On. https://www2.deloitte.com/bg/en/pages/legal/articles/gdpr-six-months-after-implementation-2018.html ; 2018.
6. De Wolf R, Joye S. "Control responsibility" A critical discourse analysis of Flemish newspapers on privacy, teens and Facebook. *International Journal of Communication* 2019; 13: 5505-5524.
7. De Wolf R. Contextualizing how teens manage personal and interpersonal privacy on social media. *New Media & Society* 2020; 22: 1058-1075.
8. Baruh L, Secinti E, Cemalcilar Z. Online privacy concerns and privacy management: a meta-analytical review. *Journal of Communication* 2017*; 67*: 26–53.
9. Trepte S, Teutsch D, Masur P K, et al. Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale" (OPLIS) In: Gutwirth S, Leenes R, & de Hert P, eds. *Reforming European data protection law.* Springer. 2015, pp. 333-365

10. Bartsch M, Dienlin T. Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior* 2016; 56: 147-154.
11. Choi H, Park J, Jung Y. The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior 2018;* 81: 42-51.
12. De Wolf R, Willaert K, Pierson, J. Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook. *Computers in Human Behavior* 2014; 35: 444-454.
13. Solove D J. Conceptualizing Privacy. *California Law Review* 2002; 90: 1087-1155.
14. Nissenbaum H. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford Law Books; 2010.
15. Cohen J. What Privacy is for. *Harvard Law Review* 2013; 126: 1904-1933.
16. Laufer R S, Wolfe M. Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of social Issues* 1977; 33: 22-42.
17. Rogers R W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology* 1975; 91: 93–114.
18. Boerman S, Kruikemeier S, Borgesius Zuiderveen F J. Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel data. *Communication Research* 2021; 48: 953-977.
19. Jansen J, Veenstra S, Zuurveen R, Stol W. Guarding against online threats: Why entrepreneurs take protective measures. *Behaviour & Information Technology* 2016; 35: 368–379.
20. Jansen J , Schaik P. Comparing three models to explain precautionary online behavioural intentions. *Information and Computer Security* 2017; 25: 165–180.
21. Ajzen I. Nature and operation attitudes. *Annu. Rev. Psychol* 2001; *52*: 27-58.
22. Xu H, Teo H H, Tan B C Y. Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. *Information Systems Research* 2012; 23: 1342-136.

23. Zarouali B, Poels K, Ponnet K. "Everything under control?": Privacy control salience influences both critical processing and perceived persuasiveness of targeted advertising among adolescents. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 2018; *12*: Article 5

24. Barnes S B. A privacy paradox: Social networking in the United States. *First Monday* 2006; *11*. Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/1394

25. Masur P K. How Online Privacy Literacy Supports Self-Data Protection and Self-Determination in the Age of Information. *Media and Communication* 2020; 8: 258-269.

26. Kezer M, Sevi B, Cemalcilar Z, Baruh L. Age differences in privacy attitudes, literacy and privacy management on Facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 2016; 10: article 2.

27. Park Y J. Digital literacy and privacy behavior online. *Communication Research* 2013; 40: 215-236.

28. Masur P K, Teutsch D, Trepte S. Entwicklung und Validierung der Online-Privatheitskompetenzskala (OPLIS) [engl. Development and validation of the online privacy literacy scale]. *Diagnostica* 2017; 63: 256-268.

29. Zhang J, Yan L, Song Y. "The Role of Consumers' Perceived Security, Perceived Control, Interface Design Features, and Conscientiousness in Continuous Use of Mobile Payment Services." *Sustainability* 2019; 11, 6843.

30. Hajli Nick, Lin X. "Exploring the Security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information." *Journal of Business Ethics* 2016; 133: 111–23.

31. Dienlin T, Trepte S. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European journal of social psychology* 2015; 45: 285-297.

32. Kokolakis S. "Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon." *Computers & Security* 2017; 64: 122–34.

33. Blank G, Bolsover G, Dubois E. "A New Privacy Paradox: Young People and Privacy on Social Network Sites." *SSRN Electronic Journal* 2014. https://doi.org/10.2139/ssrn.2479938.

34. Fogel J, Nehmad E. Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior* 2009; 25: 153-160.

35. Marwick A E. Scandal or sex crime? Gendered privacy and the celebrity nude photo leaks. *Ethics and Information Technology* 2017; 19: 177-191

36. Lewis K, Kaufman J, Christakis N. The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication* 2008*; 14*: 79-100.

37. Xu H. The effects of self-construal and perceived control on privacy concerns. *Proceedings of the 28th Annual International Conference on Information Systems,* Montréal, Canada, 2007: Paper 125.

38. Xu H, Dinev T, Smith J. Information privacy concerns: linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems* 2011; 12: 798-824.

39. Hu L T, Bentler P M. Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural equation modeling: a multidisciplinary journal* 1999; 6: 1-55.

40. Rodríguez-Ardura I, Meseguer-Artola A. How to prevent, detect and control common method variance in electronic commerce research. *Journal of theoretical and applied electronic commerce research* 2020; *15*: 1-5.

41. Masur P K, Epstein D, Quinn K, Wilhelm C, Baruh L, Lutz C. A Comparative Privacy Research Framework.2021, December https://doi.org/10.31235/osf.io/fjqhs

42. Acquisti A, Brandimarte, L, Loewenstein G. Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age. *Journal of Consumer Psychology* 2020; 30: 736-758.

Table 1
Exploratory factor analysis

	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5	Construct
I consider it important that the GDPR protects my personal data	**0.747**	0.020	0.009	0.027	0.033	
I consider it important that companies tell my how they use my personal data	**0.863**	0.031	-0.004	-0.041	-0.019	
I consider it important that those who process my personal data are supervised	**0.896**	0.020	-0.030	-0.002	-0.032	Data Protection Attitude
I consider it important that those who misused my personal data are punished	**0.812**	-0.014	-0.021	0.011	0.025	
I consider it important that citizens receive information on how their data are collected and processed	**0.864**	0.018	0.030	0.004	-0.041	
I believe I have control over what organizations access my personal information via social media	-0.022	**0.829**	-0.001	0.011	0.047	
I believe I have control over what information I provide to organizations via social media	0.080	**0.875**	0.001	0.000	-0.012	
I believe I have control over the ways organizations use my personal information via social media	-0.025	**0.911**	0.009	-0.002	-0.007	Data Control
I believe I have control over the information I share with organizations via social media	0.050	**0.887**	-0.011	-0.007	-0.006	
I am concerned my online information could be abused	0.032	-0.042	**0.828**	0.032	0.038	
I am concerned that others will find personal information	-0.032	-0.018	**0.871**	-0.007	0.040	
I am concerned that my online information will be used for unforeseen goals	0.007	-0.011	**0.904**	-0.000	-0.012	Privacy Concern
I am concerned that others will post embarrassing information of me	-0.018	0.056	**0.810**	-0.035	-0.069	

Table 1
Exploratory factor analysis

	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5	Construct
I know how to delete or deactivate my account	0.086	-0.057	0.040	**0.685**	-0.002	
I know how to restrict access to profile information	0.140	-0.073	0.021	**0.747**	0.046	
I know how to make my profile not accessible via Google **(excluded)**	-0.173	0.062	-0.034	**0.528**	-0.014	
I know how to control if others tag my name on pictures	-0.005	-0.005	-0.054	**0.766**	-0.008	Privacy Literacy
I know how to restrict access to my contact information	-0.000	0.063	0.022	**0.787**	-0.040	
I adjusted my settings, so others have to ask permission when tagging me in a picture **(excluded)**	-0.102	0.022	0.002	-0.003	**0.477**	
I am careful when accepting friend requests	0.100	-0.043	-0.055	0.006	**0.693**	
In general, I make use of privacy settings to manage my privacy	0.096	-0.022	-0.011	0.038	**0.709**	Privacy Management
I untag myself from photos I do not find appropriate **(excluded)**	0.003	0.040	0.091	0.048	**0.481**	
I make sure only friends can see my profile on social media	-0.030	0.005	-0.033	-0.090	**0.752**	

Note. Applied rotation method is promax.

Table 2

Description of the Study Measures

	M	SD	Cronbach's alpha	Factor loading of the items
Perceived data control	2.93	1.08	.93	
I believe I have control over what organizations access my personal information via social media				.845
I believe I have control over what information I provide to organizations via social media				.892
I believe I have control over the ways organizations use my personal information via social media				.892
I believe I have control over the information I share with organizations via social media				.895
Privacy management	3.64	.96	.76	
I adjusted my settings, so others have to ask permission when tagging me in a picture (**excluded)**				.437
I am careful when accepting friend requests				.694
In general, I make use of privacy settings to manage my privacy				.755
I untag myself from photos I do not find appropriate (**excluded**)				.554
I make sure only friends can see my profile on social media				.682
Privacy literacy	3.80	.89	.84	
I know how to delete or deactivate my account				.688
I know how to restrict access to profile information				.766
I know how to make my profile not accessible via Google (**excluded**)				.501
I know how to control if others tag my name on pictures				.752

I know how to restrict access to my contact information				.790
Data protection attitude	3.64	.93	.92	
I consider it important that the GDPR protects my personal data				.770
I consider it important that companies tell my how they use my personal data				.851
I consider it important that those who process my personal data are supervised				.883
I consider it important that those who misused my personal data are punished				.809
I consider it important that citizens receive information on how their data are collected and processed				.868
Privacy concern	3.18	1.04	.91	
I am concerned my online information could be abused				.858
I am concerned that others will find personal information				.869
I am concerned that my online information will be used for unforeseen goals				.901
I am concerned that others will post embarrassing information of me				.776

Table 3

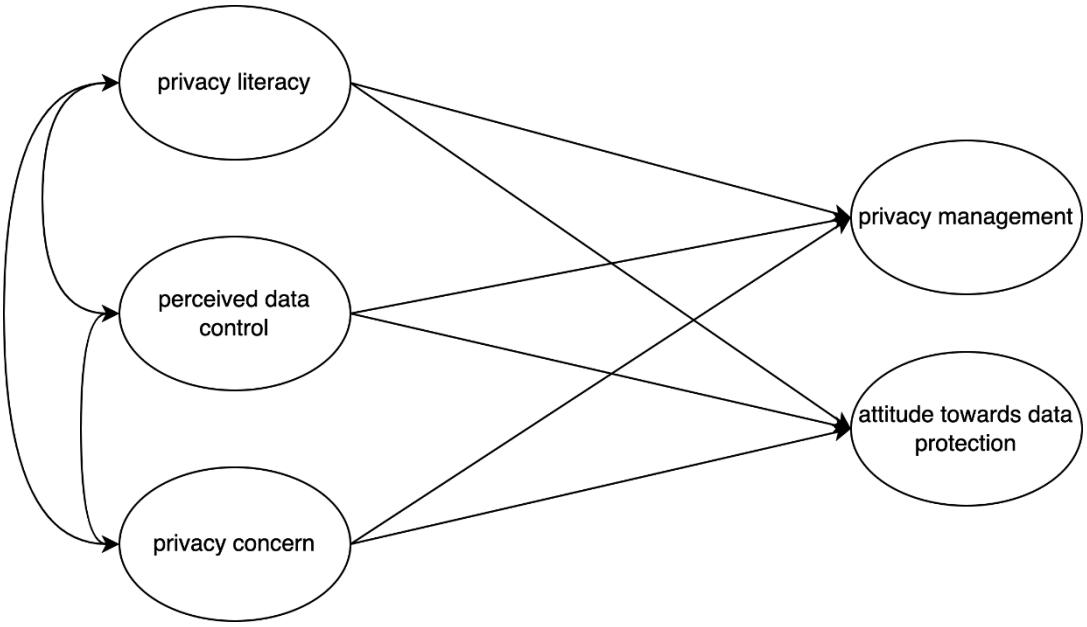
Correlations between study variables

	(1)	(2)	(3)	(4)
(1) Perceived data control				
(2) Privacy management	.296***			
(3) Privacy literacy	.270***	.230***		
(4) Data protection attitude	.190***	.312***	.200***	
(5) Privacy concern	(ns)	.290***	(ns)	.305***

Table 4

Predictive Value of Predictors by Gender

From	To	β(all)	β (girls)	β (boys)	Significance difference between girls & boys
Privacy Literacy	Privacy Management	.205***	.195***	.221***	n.s.
Perceived Data Control	Privacy Management	.210***	.207***	.200***	n.s.
Privacy Concern	Privacy Management	.255***	.227***	.264***	n.s.
Privacy Literacy	Data Protection Attitude	.166***	n.s.	.226***	Only significant for boys
Perceived Data Control	Data Protection Attitude	.107***	.153***	n.s.	Only significant for girls
Privacy Concern	Data Protection Attitude	.249***	.222***	.269***	n.s.
Explained Variance					
R^2 (Privacy Management)		.27	.22	.29	
R^2(Data Protection Attitude)		.17	.16	.17	


privacy literacy
perceived data control
privacy concern
privacy management
attitude towards data protection