On the Relationship between IT Privacy and Security Behavior: A Survey among German Private Users

Tom Biselli
Science and Technology for Peace and Security (PEASEC), Technical University of Darmstadt, Deutschland, Deutschland

Christian Reuter
Science and Technology for Peace and Security (PEASEC), Technical University of Darmstadt, Deutschland, Deutschland

On the Relationship between IT Privacy and Security Behavior: A Survey among German Private Users

Tom Biselli, Christian Reuter

Technical University of Darmstadt,
Science and Technology for Peace and Security (PEASEC), Darmstadt, Germany
{biselli, reuter}@peasec.tu-darmstadt.de

Abstract. The relevance of adequate privacy and security behavior in the digital realm is higher than ever. However, the exact relationship between privacy and security behavior is rarely discussed in the literature. This study investigates this relationship and the role of socio-demographic factors (gender, age, education, political ideology) in such behavior. Results of a survey among German private users (N=1,219) show that privacy and security behavior are only weakly correlated and not similarly influenced by socio-demographic factors. While security behavior significantly differs between age and education groups (younger and less educated show less security behavior), no such differences exist for privacy behavior. Additionally, political ideology has no influence on privacy and security behavior. Thus, this study sheds light on the concepts of privacy, security and corresponding behavior and emphasizes the need for a fine-grained differentiation if either privacy or security behavior is to be improved.

Keywords: security, privacy, behavior, relationship

1 Introduction

The advancing digitalization leads to the ever-increasing pervasion of the internet into the daily lives of individuals. In this context, individuals increasingly share sensitive data and use software to facilitate their everyday life. This has implications both with regard to privacy and security in the realm of information technology[1]. The Deutsche Telekom (Europe's largest telecommunications company) hereby reported 46 million attacks on their honeypots in 2019 [1], an increase of 12 million attacks compared to 2018. In addition, the Federal Criminal Police Office (Bundeskriminalamt) reported around 87,000 incidents of cybercrime with a particularly growing focus on mobile malware and an associated financial loss of around 60 million euros [2].

Apart from such illegal activities that reveal the need for enhanced security, the advancing digitalization also fuels an increased interest of private companies and state institutions to increasingly collect private data about individuals. Companies are mainly interested in better understanding their customers in order to offer individualized products and enable personalized advertising. State actors, on the other hand, are expanding their surveillance activities in cyberspace to prevent or solve crimes, in the context of

[1] In this paper, privacy and security thus always refer to IT privacy and IT security.

16th International Conference on Wirtschaftsinformatik,
March 2021, Essen, Germany

which the interests of individuals who value their privacy are potentially affected. Negative consequences of increased collection of private data could be observed in the case of Cambridge Analytica, where data was analyzed and misused for political purposes and thus used in a completely different context than originally intended by the user [3].

In this digital environment, individuals should therefore have an interest in maintaining their privacy and security through appropriate protective behavior. In line with this, a representative study by the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) in 2017 showed that 97% of German internet users consider security to be very important [4]. However, only a third of those surveyed specifically inform themselves about security. Further studies have confirmed that there is a growing security awareness among private individuals, especially with regard to the widespread use of smartphones [5, 6]. Similarly, users usually highly value their privacy but often do not act accordingly, a phenomenon also known as the *privacy paradox* [7, 8]. Thus, there is a general concern to support users in both their privacy and security needs. Privacy and security behavior have a common basis, as they both deal with threats in a digital world. By avoiding public WIFI-spots, for example, one can avoid both security risks and unwanted access to private data. However, the one does not necessarily go hand in hand with the other. Performing regular updates of the operating system of one's computer might be an effective security behavior, but does not prevent the provider from collecting private data. Therefore, the exact relationship between privacy and security remains of high importance. If both privacy and security behavior is to be effectively enhanced, it must be understood how both are related, whether they are conceptually similar or different and whether different factors similarly influence privacy and security behavior. Only on the basis of a better understanding of this can it be ensured that appropriate interventions and software are developed which support users in their need for both privacy and security.

To address this issue, an online study representative for the German population (with regard to age, gender, state, income and education) with 1,219 participants was conducted. In the following sections related work is presented (section 2), followed by the hypotheses (section 3) and the methods applied (section 4). After the illustration of the results (section 5) the findings are discussed in a broader context (section 6) and conclusions are drawn (section 7).

2 Related Work

Theoretical conceptualizations. The causes of existing insufficiencies and possibilities for improving both privacy and security behavior are being studied intensively. IT security in general refers to the protection of computer systems from theft and damage of hardware, software and information as well as the disruption of services they are supposed to provide [9]. A good conceptualization of this protection is provided by the so called CIA triad: secure IT systems should therefore maintain confidentiality, integrity and availability [10]. *Confidentiality* hereby refers to the prevention of unauthorized viewing, *integrity* to the unauthorized modification and *availability* to the preservation

of access [10]. Based on these definitions, security does not necessarily cover the privacy domain, but may incorporate it to some extent. There is a particular overlap in the factor confidentiality, since unauthorized viewing is associated with both unauthorized access as a security breach and with the possible exposure of sensitive information about individuals as a privacy breach. Integrity and availability, on the other hand, tend to describe factors that can be distinguished from privacy more easily.

Privacy in general refers to the prevention of exposure of sensitive information about (groups of) individuals. This includes, among other things, the nondisclosure of behavior, communications and descriptive personal data [11]. The general understanding of the term "privacy" today is still quite close to Westin's widely known definition in 1967, which described privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" [12]. However, preserving privacy in the rapidly changing digital environment is much more difficult today, which may be one reason why there is still no general agreement on the exact scope of the term privacy. Since the focus in this study is on the exposure of sensitive information in the realm of information technology, we refer to privacy in the IT context throughout this manuscript.

Based on these conceptualizations, privacy and security can both be seen as essential protections which are related to a certain degree - especially in the factor confidentiality, which describes the unauthorized viewing of data and is relevant for both privacy and security. Nevertheless, they can also vary widely in which specific elements they protect. While security refers to protection in a more general way, privacy refers specifically to the protection of personal, informational data.

Previously, the technology threat avoidance theory (TTAT) has been introduced as a possible framework to better understand personal motivations when facing IT threats [13, 14]. The TTAT hereby tries to conceptualize the cognitive processes taking place when individuals appraise threat and seek solutions with the goal to avoid technology-related threats. Although the TTAT does not explicitly distinguish between privacy and security, both represent essential areas in which IT-threats can be avoided. TTAT posits that, when confronted with IT threats, the two processes *threat appraisal* and *coping appraisal* take place and determine the answer to the threat [14]. While both privacy and security have their common ground in representing IT-related threats, they could also differ in those processes. For example, security threats such as ransomware often have immediate negative effects for users while privacy threats often have negative consequences only at a later stage and also on a societal rather than individual level (as in the Cambridge Analytica case). Thus, depending on whether the threat is a security or privacy threat, the threat appraisal could differ and result in different behavior. Taken together, the TTAT provides a framework on the basis of which it can be expected that privacy and security behavior are related to a certain extent, but nevertheless differ in specific aspects of the corresponding behavior.

Empirical conceptualizations. In order to find relevant literature, we used several databases (IEEE Xplore, Web of Science, ACM Digital Library), looking for the combination of the search terms privacy, security and relationship. After initially including

several studies containing both privacy and security even without a specific conceptualization of their relationship in order to illustrate the problem, we proceeded to only include studies making some kind of statement about the presumed relationship. This approach revealed that despite the reported differences on a theoretical level, privacy and security (and corresponding behavior) are often used together without a finer distinction. They are hereby treated as quite identical with the (mostly implicit) assumption, that they describe a common construct. In this context one study, for example, argues for the importance of usable privacy and security and how social processes play a major role in a number of privacy and security related behaviors [15]. However, instead of explicitly conceptualizing the relationship between security and privacy, both terms are mainly used in combination. Similar cases with a lack of disentangling privacy from security behavior can be seen throughout the literature [16–18]. Only few studies explicitly justify the approach to treat both privacy and security as closely related. For example, in one instance it is explicitly argued that they are indeed closely related and might be best conceptualized as two dimensions of a single construct [19].

Apart from studies that cover privacy and security as closely related or without an explicit conceptualization, some voices argue for a finer distinction between privacy and security, and define these concepts more explicitly in distinction to each other [20–23]. Bansal, for example, distinguishes privacy and security via developing a scale with dimensions which are unique to security concerns and show no overlap to privacy concerns, such as data integrity, authentication and improper access during transmission [24]. Pavlou also explicitly distinguishes information privacy concerns and information security concerns as distinct antecedents of purchasing behavior in an online environment representing uncertainty factors [25]. Finally, Oetzel and Krumay distinguish privacy and security conceptually and based on a content analysis of company websites, even though they acknowledge that some relationship exists between the concepts to a certain degree [26]. One group of studies explicitly examines the relationship between privacy and security attitudes and find that they are not equally influenced by individual characteristics, with the correlation between privacy and security attitudes being only weak [27, 28].

Finally, some studies rather use a hierarchical approach to conceptualize privacy and security, although sometimes only implicitly. In one study, influencing factors on privacy and security behavior are discussed without a clear distinction between the two concepts [17]. Implicitly, however, privacy is treated as a subcategory of security concerned with the protection of access to personal data. The subsumption of privacy into the security domain is confirmed by further studies which define information privacy as a part of the broader construct web security [29] and generally as being part of a security framework [30]. The other direction of a hierarchical relationship has also been suggested, e.g. in the sense that the problem area of improper access to data as a security concern can also be considered as a part of the superordinate category privacy [31]. An overview of the most commonly proposed relationships is provided in Figure 1.

Influencing factors on privacy and security behavior. In order to better conceptualize the relationship between privacy and security behavior, it is also promising to examine it from different points of view and analyze how factors such as age, gender, education

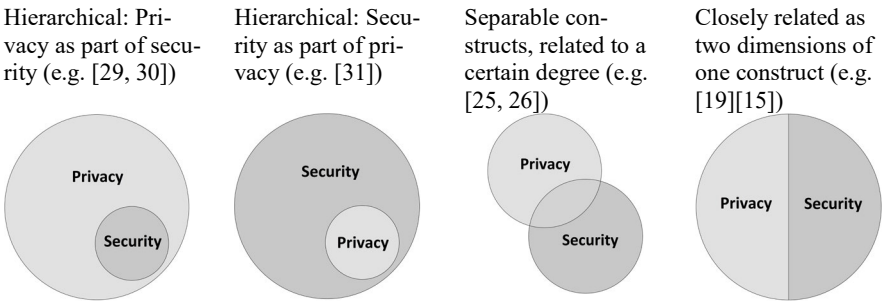

Figure 1. Conceptualizations of the relationship between privacy and security proposed in the literature (inspired by [20]).

and political ideology influence the corresponding behavior. Age and gender, for example, have previously been associated with differences in security behavior. Here, it has mainly been shown that women show less security knowledge, experience and behavior than men [32, 33]. With regard to age, especially younger people below 25 years have been associated with weaker security behavior [34, 35]. As for education, it has previously been shown that those with higher levels of education tend to be more concerned about privacy [36] and show more security awareness [37]. Political ideology has so far mainly been reported as relevant to privacy attitudes and behavior [7, 38, 39]. There is a consensus in this respect that people who see themselves as rather left-wing are more critical of the (predominantly state-organized) data collection on individuals. If the concepts of privacy and security were indeed as closely related as they are often discussed, the moderating factors described should be applicable to each other's behavior. Thus, political ideology should have an influence on security behavior, age and gender should have an influence on privacy behavior and education levels should have similar effects on both privacy and security behavior.

Importantly, privacy and security attitudes and behavior can potentially differ between cultures [40, 41]. Thus, we focus on a sample from Germany providing an opportunity for cross-country comparability in future studies. Private users are thereby of special interest since everyday behavior in the digital realm can have negative consequence for everyone, such as the already described security incidents (e.g. mobile malware) and privacy breaches (e.g. Cambridge Analytica).

Research Gap. Generally, there is no consensus with regard to the relationship between privacy and security and plenty of studies using both terms actually do not conceptualize their relationship at all, but use both in parallel and assume some kind of implicit, close relationship. Importantly, the vast majority of studies trying to conceptualize some kind of relationship focus either on theoretical considerations or on corresponding privacy/security attitudes as opposed to behavior. Thus, there exists a gap with regard to illuminating the relationship between privacy and security behavior. If the ultimate goal is to increase privacy and security behavior, which is a desirable objective as previously outlined, further empirical data on the relationship between them is needed. Especially the question, to what extent privacy behavior goes hand in hand with security behavior, and thus whether both could eventually be improved by similar interventions

and technical implementations has been neglected so far. Accordingly, this study aims to answer the following research question: "*Are privacy and security behavior closely related and similarly influenced by demographic factors and political ideology?"*.

3 Hypotheses

In order to fill the described research gap, this study investigates the relationship between privacy and security behavior of private users in Germany, taking into account demographic factors such as gender, age, education and political ideology. *Private users* are hereby defined as individuals who use information and communication technology, such as computers and the internet for their personal use. Based on the literature review, we do not expect privacy and security behavior to be not related at all and that they would constitute completely separable domains. Instead, we aim at illuminating the relationship between the two by assessing the correlation and influencing factors on corresponding behavior at different levels. Due to the literature describing privacy and security (sometimes implicitly) predominantly as closely related, a correlation and a similar influence of demographic factors and political ideology on both privacy and security behavior is expected. However, no assumptions are made about the expected strength of the correlation, as there is preliminary evidence to suggest that privacy and security may be conceptually more different than often treated in the literature. As demographic factors have previously been shown to influence especially security behavior, these factors should influence privacy behavior in a similar way, if both were conceptually closely related. Similarly, political ideology, which has previously been shown to influence privacy behavior, should also influence security behavior if both were closely related. If there were no similar influence of these factors on the corresponding behavior, this would indicate that the two concepts of privacy and security behavior need to be distinguished more thoroughly. Based on the previously reviewed literature, the following hypotheses are therefore postulated:

- **H1: Privacy behavior and security behavior correlate positively**
- **H2: Demographic factors such as gender, age, and education have a similar influence on both privacy and security behavior**
- **H3: Political ideology has a similar influence on both privacy and security behavior**

4 Method

4.1 Study Design and Participants

To assess privacy and security behavior and their relationship, a representative online survey with German citizens was conducted in May 2019, using LimeSurvey and the

panel provider GapFish (Berlin)[2]. GapFish is certified according to the ISO norm 26362 ensuring the quality of access-panels in market, opinion and social research [42]. The sample (N = 1,219) was matched to the distribution of age, gender, income, region and education according to the general German population [43, 44] during the data collection by the panel provider using corresponding quotas. The sample covers an age-range from 14 to 87 years, of which 52% are women and 48% are men.

The survey included four questions related to security behavior and eight questions related to privacy behavior. The overall survey further included questions on security and privacy knowledge, media use in crisis situations and data misuse which, however, are not part of this study. As the privacy and security behavior questions were posed prior to the other questions, a possible bias through the other questions can be ruled out. Answers to the items were given on a 5-point rating scale by Rohrmann, ranging from *1 – I disagree* to *5 – I strongly agree* [45]. To get more reliable answers, the option *no answer* was provided for all questions and all questions were posed in German.

The items were developed based on the recommendations of the German Federal Office for Information Security (BSI) on how to secure one's computer, smartphone and online generated data [46, 47]. Some survey instruments already exist with regard to privacy and security. However, we found none to be suitable for our specific case, in which we wanted to analyze German private users with regard to their everyday behavior. The Human Aspects of Information Security Questionnaire (HAISQ), for example, aims at evaluating information security threats caused by employees within organizations rather than assessing private users in their everyday life [48] and the Internet Users Information Privacy Concerns (IUIPC) scale focuses on attitudes rather than actual behavior [49]. For the item development we therefore focused on (1) behavioral actions rather than intentions, (2) private users in their everyday-life as opposed to specific (e.g. work-related) contexts and (3) suitable contexts for German private users. The latter was the main motivation to use recommendations of a German institution such as the BSI. The recommendations do not explicitly distinguish between privacy and security behavior but rather touch on both topics. For the purpose of this study, however, the resulting items have been treated as items separately for privacy and security, based on face validity. Since the recommendations do not explicitly distinguish between privacy and security behavior and we wanted to include all recommendations to cover enough topics, an uneven number of items for assessing privacy and security behavior resulted. With regard to their security behavior, the participants had to answer questions such as whether they would install software updates immediately, or use antivirus software. With regard to their privacy behavior, the participants had to answer questions such as whether they inform themselves about the privacy policy of apps before installing them, or avoid online services that require a name or e-mail address (an overview of all items used in the analysis can be found in Figure 2 and 3).

[2] Some of the subsequently analyzed data with regard to security behavior (but not privacy behavior) overlaps with a data analysis of a different published manuscript of our group. However, the focus here is explicitly on the relationship between privacy and security behavior, which was not examined at all in the other study. There, the focus was on the extent to which knowledge about security-relevant issues can predict appropriate security behavior [33].

Because the aim of this study was to evaluate the relationship between privacy and security behavior of the German population with regard to demographics like age and gender, education but also political ideology, corresponding questions were also included in the survey. For the latter, two items were included which asked for the personal opinion regarding the responsibility for data protection on the internet (*state* vs. *company*) since different political ideologies can be expected to yield different answers here (e.g. more left-wing socialist types might expect greater state interference than more right-wing liberal types [50]). In these, participants were asked, whether they think that the state is responsible for data protection on the internet (item 1) and whether they think, that the companies collecting the data are responsible for data protection on the internet (item 2). The items were developed based on theoretical considerations and answers were given on the same 5-point Rohrmann-scale as the other items. Another item asked directly about the political orientation on a left to right spectrum (*left-wing, fairly left-wing, center, fairly right-wing, right-wing*).

4.2 Analysis

The analysis was conducted using the software tools Microsoft Excel and RStudio Version 4.0.2. Answers with the rating *no response* were excluded as missing values from the subsequent analysis. An initial descriptive analysis for the items for both the privacy behavior scale and security behavior scale was conducted. The reliability of the corresponding scales was investigated based on the internal consistency (Cronbach's Alpha). In order to find group differences, participants were grouped into roughly equal age categories (15-29, 30-44, 45-59, > 60). Education levels were grouped into three categories: *low* (no degree and German Hauptschul-degree), *medium* (German Realschul-degree) and *high* (Highschool & University degree). The individual level of privacy and security behavior was determined by calculating the mean across all items of the corresponding scale. The factor *attribution of responsibility for data protection on the internet* was calculated based on the two items with regard to state- or company-responsibility. If a participant reported a higher responsibility for the state than the company, he was grouped in the factor level state and vice versa.

Differences in privacy and security behavior depending on the group factors *gender*, *age* and *education* were analyzed using a multivariate analysis of variance (MANOVA). A separate MANOVA was carried out for the factors *political orientation* and *attribution of responsibility for data protection on the internet* (together representing political ideology) as they can be assigned to a different theoretical framework than the former factors. Since the assumption of multivariate normality and homogeneity of covariance matrices could not be confirmed for the available data, a parametric bootstrap resampling approach with 10,000 iterations was used to calculate the test statistics. This method was implemented using the MANOVA function from the R package "MANOVA.RM" [51].

Subsequent univariate analyses were conducted using factorial analyses of variance (ANOVA) when corresponding assumptions such as normal distribution and homogeneity of variances were fulfilled and robust factorial ANOVAs with trimmed means (trimming level = 0.2) if they were violated [52, 53]. The robust approach also uses

bootstrapping to obtain an empirically derived critical p-value. In this context, no degrees of freedom are reported since an adjusted critical value instead of a critical value based on a known sampling distribution is used. The reported test statistic Q refers to the robust ANOVA test statistic for trimmed means. Subsequent robust post-hoc tests (test statistic: ψ) for disentangling observed main effects are also based on percentile bootstraps for the p values [53]. Because all tests were performed with the same sample, the 5% - alpha level was corrected with the Bonferroni-Holm method [54].

5 Results

5.1 Descriptive Analysis

To evaluate the reliability of the constructed privacy behavior and security behavior scales, the internal consistency of Cronbach's Alpha was analyzed. After two items for the privacy behavior scale and one item for the security behavior scale were rejected and not used for further analyses (due to a low correlation of the item with the overall scale) they showed moderate values of $\alpha_{\text{privacy-behavior}} = .72$ and $\alpha_{\text{security-behavior}} = .65$. The internal consistency is usually considered acceptable from around $\alpha = .70$ [55]. A possible underestimation of α due to few and heterogenous items is a known phenomenon, which can be neglected to a certain degree, since the analysis does not focus on individual scores but on aggregated group scores, which are not strongly affected by measurement errors due to a lower reliability [55].

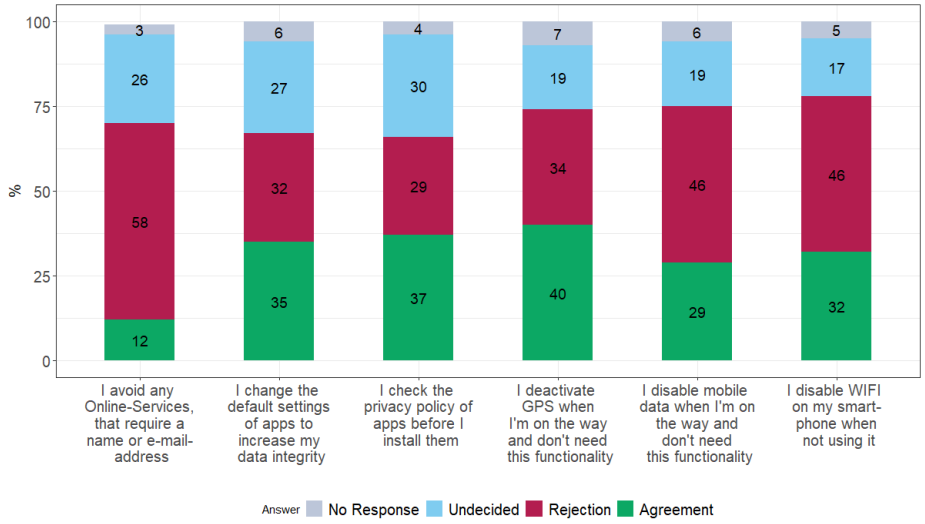

Figure 2. Percentage frequencies for the questions of the *privacy behavior* category, N = 1,219.

A descriptive analysis of the responses gave a nuanced picture of the participants' self-reported privacy behavior. As shown in Figure 2 ("Rejection" combines *"I strongly disagree"* and *"I hardly agree"* answers while "Agreement" combines *"I fairly agree"*

and *"I strongly agree"* answers), agreement and rejection with regard to privacy-related items are mostly balanced with the exception of one item (*"I avoid Online-Services, that require a name/email-address"*) where only 12% of participants agree and 58% disagree. Moreover, a fairly high percentage of participants were undecided about their privacy behavior, with response rates ranging from 17% to 30%.

A descriptive analysis of the responses with regard to security revealed that the majority of participants indicated a rather high level of self-reported security behavior. Figure 3 shows the percentage frequencies for the corresponding *security behavior* items. It becomes apparent that agreement to all security-related items exceeds rejection (70% vs. 18%, 51% vs. 25%, 58% vs. 18%) and also undecided or no response answers (which are all below 20%).

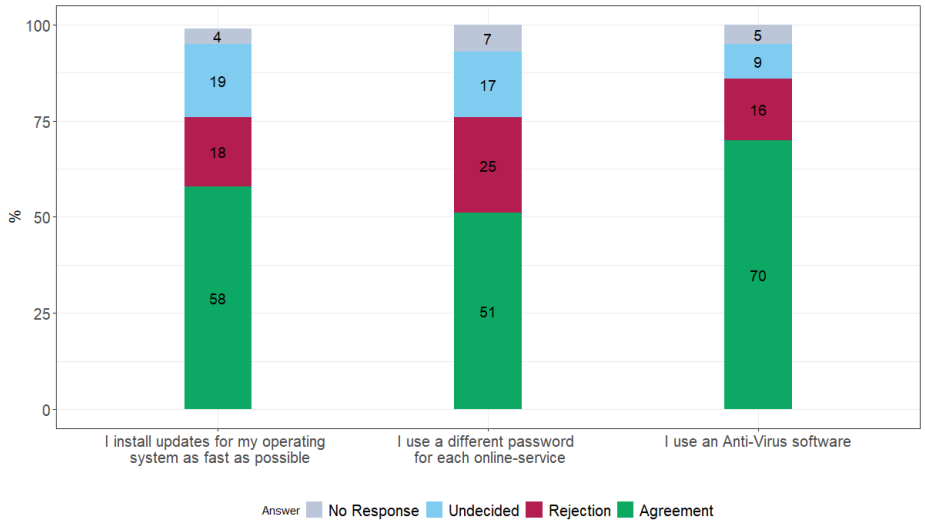

Figure 3. Percentage frequencies for the questions of the *security behavior* category, N = 1.219.

5.2. Hypothesis Testing

H1: Privacy behavior and security behavior correlate. To test H1, a Spearman's rank correlation was calculated with the mean values of privacy and security behavior across the corresponding items. The correlation was weakly positive, $r = .18$, $p < .001$. The overall privacy behavior ($M = 2.81$, $SD = 0.86$) thereby was considerably lower than the overall security behavior ($M = 3.76$, $SD = 1.07$) across all participants.

H2: Demographic factors such as gender, age, and education have a similar influence on both privacy and security behavior. One main goal of the analysis was to assess, whether privacy and security behavior can be considered as conceptually closely related. If that were the case, gender, age and education should have a similar influence on both privacy and security behavior. The corresponding robust MANOVA revealed that while gender did not influence privacy and security behavior at all (Wald-type statistic: $W(df=2) = 0.85$, $p = 0.99$) both age ($W(6) = 32.11$, $p < .001$) and education ($W(4)$

= 21.61, p = .003) influenced privacy and security behavior. To disentangle these effects, univariate ANOVAs were conducted separately for privacy behavior and security behavior. This revealed that age (F(1,995) = 0.07, p = .79) and education (F(1,995) = 2.01, p = .78) did not influence privacy behavior. In contrast, security behavior was significantly influenced by both age (Q = 44.94, p = .01) and education (Q = 12.88, p = .02). Subsequent robust post-hoc comparisons showed that young people below the age of 30 reported significantly less security behavior than those in the age groups 30-44 (ψ = -0.69, p < .001) and 45-59 (ψ = -0.81, p = .001). Furthermore, older people in the age group over 60 reported significantly higher security behavior than those in the age group 30-44 (ψ = -1.08, p < .001), but significantly lower security behavior that those in the age group 45-59 (ψ = -1.20, p < .001) (see Table 1).

Table 1. Table for trimmed mean values (trimming level = 0.2) and standard deviations of the *security behavior* score per age category

	security behavior score	
Age (in years)	**mean value (*M*)**	**standard deviation (*SD*)**
< 30	3.43	1.03
30 - 44	3.75	1.04
45-59	3.93	1.08
>= 60	3.84	1.07

With regard to the level of education, robust post-hoc comparisons revealed that those with a low education reported significantly lower security behavior both compared to those with medium education (ψ = -0.94, p = < .001) and high education (ψ = 1.30, p = < .001) (see Table 2).

Taken together, the results show that contrary to expectations, privacy and security behavior are not similarly influenced by the categories of gender, age and education. While different groups with regard to age and education report significantly diverging security behavior, no such differences are seen for privacy behavior. Thus, the hypothesis could not be confirmed based on the current data.

Table 2. Table for trimmed mean values (trimming level = 0.2) and standard deviations of the *security behavior* score per education category

	security behavior score	
Education	**mean value (*M*)**	**standard deviation (*SD*)**
Low	3.63	1.14
Medium	3.84	0.98
High	3.90	1.03

H3: Political ideology has a similar influence on both privacy and security behavior. Besides the described demographic factors such as gender, age and education, it

was hypothesized that political ideology might have an influence on privacy and security behavior. Again, if privacy and security can be considered as conceptually closely related, political ideology should have a similar influence on privacy and security behavior. The corresponding MANOVA included the factors "attribution of responsibility for data protection on the internet" (*state* vs. *company*) and political orientation (*left*, *rather left*, *center*, *rather right*, *right*). The results showed that neither the data protection attribution ($W(8) = 17.51$, $p = .18$) nor political orientation ($W(4) = 5.56$, $p = .94$) were significantly associated with privacy and/or security behavior.

6 Discussion

Summary of results. The main goal of this study was to quantify the relationship between privacy and security behavior and assess, whether they can be regarded as closely related. We tried to illuminate this relationship from different points of view by examining whether the corresponding behaviors correlate and whether they are similarly influenced by factors such as demographics and political ideology. Only then it would be valid not to disentangle them and explicitly explain their relationship when researching these concepts, as is often the case. However, the present results show that privacy and security behavior are actually only weakly correlated. Furthermore, influencing factors on privacy and security behavior are not consistent. While young people (<30) and those with low education (no degree and German Hauptschul-degree) reported significantly less security behavior than older and more educated people, no such differences could be found for privacy behavior. Political ideology had no influence, neither on privacy nor on security behavior.

Relationship between privacy and security behavior. Based on these results, the notion, that privacy and security are closely linked and those who behave securely necessarily also behave privately must be questioned. This finding stands in contrast to some research, which does not explicitly distinguish between privacy but uses both in parallel [16–18]. Thus, the danger exists that findings which implicitly rather target security improvements might be falsely attributed to privacy improvements when they are only suitable to improve security – and vice versa. This could be relevant, for example, for both the education of children and adults with regard to improving privacy and security behavior and for software developers who need to be aware in which relation they view privacy and security and to what extend one and the other shall be protected.

Especially with regard to the examination of privacy and security behavior as opposed to corresponding attitudes, the findings of this study add to the existing literature. They are hereby in line with findings, that attitudes towards privacy and security also are not similarly influenced by personality characteristics and the correlation between privacy and security attitudes is only weak [27, 28]. Existing evidence, according to which individuals differ in their privacy needs based on their political ideology [38, 39] could not be shown in corresponding behavior. One reason for this could be the fact, that we assessed political orientation on a 5-point scale. Even though it can be argued that too many points can also confuse respondents, there is evidence that a 10-point and

11-point left-to-right scale can lead to a higher validity [56]. Thus, we might have been able to detect corresponding effects if we had used a more fine-grained scale.

In general, up until today there is no consensus on the exact relationship between privacy and security. Sometimes implicitly, sometimes explicitly hierarchical relationships are proposed (privacy as part of security [29, 30, 57], security as part of privacy [31]) both are described as rather separable constructs [25, 26] or as related dimensions of one underlying construct [15, 19]. Since we found at least some correlation between both privacy and security but couldn't identify the common drivers to be demographic factors or political ideology the question then arises where the common ground between privacy and security could lie. As previously outlined, the TTAT might provide a suitable framework for conceptualizing both the similarities and differences between privacy and security. The TTAT makes assumptions about cognitive processes such as threat appraisal and coping appraisal, which determine subsequent behavior in the face of IT-related threats [14]. Threat appraisal hereby includes the *perceived susceptibility* and *perceived severity*, i.e. gravity of consequences associated with an IT threat. While TTAT does not explicitly distinguish between privacy and security related IT threats, the dimension of perceived severity of the corresponding IT threat (security or privacy related) could be one, where privacy and security behavior are differentially influenced. Specifically, only if an individual considers the unregulated collection of personal data as having grave consequences, would he engage in behavior that prevents this, and thus show high privacy behavior. However, since the consequences of a security threat such as a computer virus are usually more immediate, an individual could show high security behavior and at the same time underestimate the consequences of not protecting his privacy, and thus show low privacy behavior. Consequently, there might be a common factor such as avoidance of technology related threats in general, as posited by the TTAT, which explains that privacy and security behavior are correlated, albeit weakly. However, in certain aspects of this common factor, such as the exact threat appraisal via assessing the perceived severity of the IT threat, depending on the core beliefs of an individual, differences in privacy and security behavior might arise. This would explain that factors such as age and education have a differential influence on privacy and security behavior. Given the weak correlation and inconsistent role of demographic factors and political ideology for privacy and security behavior, it is not obvious whether our results rather suggest that privacy and security overlap as distinct concepts, or whether they can rather be seen as two dimensions of a common construct. However, combined with the considerations presented in the light of the TTAT, we suggest that corresponding privacy and security behavior might be best conceptualized as two dimensions of a common construct which, based on TTAT, possibly represents some form of technical threat avoidance.

Limitations. Some limitations of this study need to be considered, before drawing too broad conclusions. First, *(1)* the results are based on the participants' self-reported privacy and security behavior which is not necessarily identical with their actual behavior. The discrepancy between intentions and actual behavior has been reported before [7, 58] and represents a general limitation of the survey methodology. Furthermore, *(2)* the used items can only be seen as an approximation to the surveyed constructs because no

previously validated questionnaire was used. This caveat regarding the validity of the scales was confirmed by a rather low internal consistency, especially with regard to security behavior. The exact wording of items could be refined, e.g. disabling WIFI on one's smartphone could be more relevant in public than at home. In addition, *(3)* relatively few items were used to assess complex privacy and security behavior with many potential influencing factors [59, 60], a problem exacerbated by the elimination of two items due to their low correlation with the corresponding behavior scale. Consequently, the items and should be reviewed and revised. However, since the items were based on recommendations of the German Federal Office for Information Security, they are still considered sufficiently suitable for an approximation to the described topic.

7 Conclusion

In view of ever-increasing threats to privacy and security, methods to improve both privacy and security behavior are being studied intensively. However, an explicit conceptualization of the relationship between privacy and security is often missing, although both terms are usually used in combination. In general, there is no consensus on how best to describe the relationship and the extent to which one goes hand in hand with the other. Based on the results of this study, we found that privacy and security behavior of German private users actually correlate only weakly and is differentially influenced by demographic factors such as age and education. Thus, even though privacy and security are often treated as closely related concepts, it is not necessarily possible to improve security behavior and rely on automatically improving privacy behavior (and vice versa). Instead, a fine-grained differentiation is necessary if privacy or security behavior in particular is to be improved. The results of this study shed light on the relationship in that there might exist a common driver which influences both privacy and security behavior to a certain degree, but which we could not show to be related to demographics and political ideology. Future studies should take a step back from the circumscribed concepts privacy and security and explicitly try to uncover common drivers of those behaviors. Also, the findings of this study should be validated, taking into account the described limitations. Only through such studies and a better understanding of the concepts and the relationship between privacy and security behavior can they be effectively improved and private users empowered to meet the challenges in the digital realm.

Acknowledgements

This research work has been funded by the German Federal Ministry of Education and Research and the Hessian Ministry of Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE and by the Deutsche Forschungsgemeinschaft (DFG) – SFB 1119 (CROSSING) – 236615297 as well as GRK 2050 (Privacy & Trust) – 251805230.

References

1. Knirsch, R.: Telekom legt aktuelle Zahlen zur Cybersicherheit vor [Telekom presents current numbers on cyber security] | Deutsche Telekom, https://www.telekom.com/de/medien/medieninformationen/detail/telekom-legt-aktuelle-zahlen-zur-cybersicherheit-vor-573046, last accessed 2020/07/31.
2. Bundeskriminalamt: Cybercrime Bundeslagebild [Federal situation picture]. (2018).
3. Isaak, J., Hanna, M.J.: User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. Computer. 51, 56–59 (2018).
4. Deutsches Bundesamt für Sicherheit in der Informationstechnik (BSI): Die Lage der IT-Sicherheit in Deutschland [The state of IT security in Germany] 2018. 100 (2018).
5. Reuter, C., Häusser, K., Bien, M., Herbert, F.: Between effort and security: User assessment of the adequacy of security mechanisms for app categories. In: Proceedings of Mensch und Computer. pp. 287–297 (2019).
6. Ben-Asher, N., Kirschnick, N., Sieger, H., Meyer, J., Ben-Oved, A., Möller, S.: On the need for different security methods on mobile phones. In: Mobile HCI - 13th International Conf. on Human-Computer Interaction with Mob. Devices and Services. pp. 465–473 (2011).
7. Acquisti, A., Grossklags, J.: Privacy Attitudes and Privacy Behavior. Econ. Inf. Secur. 165–178 (2006).
8. Alashoor, T., Baskerville, R.: The privacy paradox: The role of cognitive absorption in the social networking activity. In: International Conference on Information Systems: Exploring the Information Frontier, ICIS (2015).
9. Mihajlov, M., Josimovski, S., Jerman-Blazič, B.: A conceptual framework for evaluating usable security in authentication mechanisms - Usability perspectives. In: 5th International Conference on Network and System Security, NSS 2011. pp. 332–336 (2011).
10. Pfleeger, C.P.: Security in computing. Pearson Education India (2009).
11. Pfleeger, S.L., Pfleeger, C.P.: Harmonizing privacy with security principles and practices. IBM J. Res. Dev. 53, 1–12 (2009).
12. Westin, A.F.: Privacy and freedom. Atheneum, New York (1967).
13. Chen, H., Li, W.: Mobile device users' privacy security assurance behavior: A technology threat avoidance perspective. Inf. Comput. Secur. 25, 330–344 (2017).
14. Liang, H., Xue, Y.: Avoidance of information technology threats: A theoretical perspective. MIS Q. 33, 71–90 (2009).
15. Das, S., Kim, T.H., Dabbish, L.A., Hong, J.I.: The Effect of Social Influence on Security Sensitivity. In: SOUPS: Symposium on Usable Privacy and Security. pp. 143–157 (2014).
16. Halevi, T., Lewis, J., Memon, N.: A pilot study of cyber security and privacy related behavior and personality traits. In: WWW Companion - Proceedings of the 22nd International Conference on World Wide Web. pp. 737–744 (2013).
17. Kang, R., Dabbish, L., Fruchter, N., Kiesler, S.: "My data just goes everywhere:" User mental models of the internet and implications for privacy and security. In: SOUPS - Proceedings of the 11th Symposium on Usable Privacy and Security. pp. 39–52 (2015).
18. Redmiles, E.M., Kross, S., Mazurek, M.L.: How Well Do My Results Generalize? Comparing Security and Privacy Survey Results from MTurk, Web, and Telephone Samples. In: IEEE Symposium on Security and Privacy. pp. 1326–1343. Institute of Electrical and Electronics Engineers Inc. (2019).
19. Flavián, C., Guinalíu, M.: Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site. Ind. Manag. Data Syst. 106, 601–620 (2006).
20. Hurlburt, G.F., Miller, K.W., Voas, J.M., Day, J.M.: Privacy and/or security: Take your pick. IT Prof. 11, 52–55 (2009).

21. Ermakova, T., Fabian, B., Kornacka, M., Thiebes, S., Sunyaev, A.: Security and Privacy Requirements for Cloud Computing in Healthcare. In: ACM Transactions on Management Information Systems. pp. 1–29 (2020).
22. Buck, C., Kessler, T., Eymann, T.: Nutzerverhalten als Teil der IT-Security – ein IS-Literaturüberblick [User behavior as part of IT security - an IS literature overview]. In: Wirtschaftsinformatik (WI) Proceedings. pp. 1115–1130 (2015).
23. Maass, M., Walter, N., Herrmann, D., Hollick, M.: On the Difficulties of Incentivizing Online Privacy through Transparency: A Qualitative Survey of the German Health Insurance Market. In: Wirtschaftsinformatik (WI) Proceedings (2019).
24. Bansal, G.: Security concerns in the nomological network of trust and Big 5: First order vs. second order. In: International Conf. on Information Systems, ICIS. pp. 2117–2132 (2011).
25. Pavlou, P.A.: State of the information privacy literature: Where are we now and where should we go? MIS Q. 35, 977–988, (2011).
26. Oetzel, M.C., Krumay, B.: Differentiating privacy and security: A content analysis of B2C websites. In: 17th Americas Conf. on Information Systems, AMCIS. pp. 1891–1900 (2011).
27. Egelman, S., Peer, E.: Predicting privacy and security attitudes. In: ACM SIGCAS Computers and Society. pp. 22–28 (2015).
28. Egelman, S., Peer, E.: Scaling the security wall : Developing a security behavior intentions scale (SeBIS). In: Conference on Human Factors in Computing Systems - Proceedings. pp. 2873–2882 (2015).
29. Kim, M.S., Ahn, J.H.: Comparison of trust sources of an online market-maker in the e-marketplace: Buyer's and seller's perspectives. J. Comput. Inf. Syst. 47, 84–94 (2006).
30. Clarke, R.: Privacy impact assessment: Its origins and development. Comput. Law Secur. Rev. 25, 123–135 (2009).
31. Smith, H.J., Milberg, S.J., Burke, S.J.: Information privacy: Measuring individuals' concerns about organizational practices. MIS Q. Manag. Inf. Syst. 20, 167–195 (1996).
32. McGill, T., Thompson, N.: Gender differences in information security perceptions and behaviour. In: ACIS - 29th Australasian Conference on Information Systems. pp. 1–11 (2018).
33. Herbert, F., Schmidbauer-Wolf, G.M., Reuter, C.: Differences in IT Security Behavior and Knowledge of Private Users in Germany. WI2020 Community Tracks. 168–184 (2020).
34. Jagatic, T.N., Johnson, N.A., Jakobsson, M., Menczer, F.: Social phishing. Commun. ACM. 50, 94–100 (2007).
35. Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F., Downs, J.: Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In: Conference on Human Factors in Computing Systems. pp. 373–382 (2010).
36. O'Neil, D.: Analysis of internet users' level of online privacy concerns. Soc. Sci. Comput. Rev. 19, 17–31 (2001).
37. Öğütçü, G., Testik, Ö.M., Chouseinoglou, O.: Analysis of personal information security behavior and awareness. Comput. Secur. 56, 83–93 (2016).
38. Rykkja, L.H., Lægreid, P., Fimreite, A.L.: Attitudes towards anti-terror measures: The role of trust, political orientation and civil liberties support. Crit. Stud. Terror. 4, 219–237 (2011).
39. Bergström, A.: Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. Comput. Human Behav. 53, 419–426 (2015).
40. Li, Y., Kobsa, A., Knijnenburg, B.P., Carolyn Nguyen, M.-H.: Cross-Cultural Privacy Prediction. In: Proceedings on Privacy Enhancing Technologies. pp. 113–132 (2017).
41. Reuter, C., Ludwig, T., Kaufhold, M.-A., Spielhofer, T.: Emergency services' attitudes towards social media: A quantitative and qualitative survey across Europe. J. Hum. Comput. Stud. 95, 96–111 (2016).

42. ISO 26362:2009: Access panels in market, opinion and social research - Vocabulary and service requirements, https://www.iso.org/standard/43521.html, last accessed 2020/11/09.
43. Destatis: Bildungsstand: Allgemeine Schulausbildung [Educational level: General school education] - Statistisches Bundesamt, https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Bildung-Forschung-Kultur/Bildungsstand/Tabellen/bildungsabschluss-privathaush-allgemeine-schulausbildung-insgesamt.html, last accessed 2020/07/10.
44. Statistisches Bundesamt: Datenreport 2016. Ein Sozialbericht für die Bundesrepublik Deutschland [Data Report 2016: A Social Report for the Federal Republic of Germany] | WZB, https://www.wzb.eu/de/publikationen/datenreport/datenreport-2016, last accessed 2020/07/10.
45. Rohrmann, B.: Empirische Studien zur Entwicklung von Antwortskalen für die sozialwissenschaftliche Forschung [Empirical studies on the development of response scales for social science research]. Zeitschrift für Sozialpsychologie. 9, 222–245 (1978).
46. Bundesamt für Sicherheit in der Informationstechnik: Zehn Maßnahmen zur Absicherung gegen Angriffe aus dem Internet [Ten measures to safeguard against attacks from the Internet], https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Checklisten/Massnahmen_gegen_Internetangriffe.html, last accessed 2020/07/30.
47. Bundesamt für Sicherheit in der Informationstechnik (BSI): Sichere private Nutzung des Internets [Safe private use of the Internet]. (2013).
48. Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., Zwaans, T.: The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Comput. Secur. 66, 40–51 (2017).
49. Malhotra, N.K., Kim, S.S., Agarwal, J.: Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Inf. Syst. Res. 15, 336–355 (2004).
50. Fuchs, D., Klingemann, H.: Das Links-Rechts-Schema als politischer Code: ein interkultureller Vergleich auf inhaltsanalytischer Grundlage [The left-right scheme as political code: an intercultural comparison based on content analysis]. Campus Verl., Frankfurt am Main (1989).
51. Friedrich, S., Konietschke, F., Pauly, M.: Resampling-based analysis of multivariate data and repeated measures designs with the R package MANOVA. RM. R J. 11, 380–400 (2019).
52. Field, A.P., Wilcox, R.R.: Robust statistical methods: A primer for clinical psychology and experimental psychopathology researchers. Behav. Res. Ther. 98, 19–38 (2017).
53. Mair, P., Wilcox, R.: Robust statistical methods in R using the WRS2 package. Behav. Res. Methods. 52, 464–488 (2020).
54. Victor, A., Elsässer, A., Hommel, G., Blettner, M.: Judging a Plethora of p-Values: How to Contend With the Problem of Multiple Testing. Dtsch. Ärzteblatt Int. 107, 50–56 (2010).
55. H. Moosbrugger, Kelava, A.: Testtheorie und Fragebogenkonstruktion [Test theory and questionnaire construction]. Springer-Verlag Berlin Heidelberg, Heidelberg (2012).
56. Kroh, M.: Measuring left-right political orientation: The choice of response format. Public Opin. Q. 71, 204–220 (2007).
57. Bubaš, G., Orehovački, T., Konecki, M.: Factors and predictors of online security and privacy behavior. J. Inf. Organ. Sci. 32, 79–98 (2008).
58. Kokolakis, S.: Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Comput. Secur. 64, 122–134 (2017).
59. Furnell, S., Rajendran, A.: Understanding the influences on information security behaviour. Comput. Fraud Secur. 2012, 12–15 (2012).
60. Leach, J.: Improving user security behaviour. Comput. Secur. 22, 685–692 (2003).