Of Guardians, Cynics, and Pragmatists
A Typology of Privacy Concerns and Behavior

Eva-Maria Schomakers, Chantal Lidynia, Luisa Vervier and Martina Ziefle
Human-Computer Interaction Center, RWTH Aachen University, Campus-Boulevard 57, Aachen, Germany

Keywords: Online Privacy, Privacy Paradox, Privacy Typology, Privacy Calculus, Privacy Cynicism, User Study, Privacy Concern.

Abstract: Online privacy is one of the most discussed topics in the digital era. User concerns about online privacy can be a barrier to the use of digital services. Different approaches, mostly from a social science perspective, try to understand user concerns, attitudes, and behaviors in the online context. Especially the so-called privacy paradox, the discrepancy between high privacy concerns and contradicting low privacy protection behavior, has been of interest. This phenomenon has been explained in different ways: users performing a privacy calculus, making affective decisions, or being overwhelmed, resigned by the complexity of online threats and protective measures. Complementing these theories, we hypothesize that different user types approach privacy differently. A survey (N=337) investigates the privacy attitudes, behaviors, and experiences of German internet users. With a cluster analysis, three distinct types of users were identified: the "Privacy Guardians," highly concerned and taking much privacy protective actions, the "Privacy Cynics," concerned but feeling powerless and unable to protect their privacy, and the "Privacy Pragmatists," showing the least concerns which they weigh against benefits. These user groups need different tools and guidelines for protecting their privacy.

1 INTRODUCTION

Searching for information, chatting with friends, customers, or colleagues, shopping, doing sports, studying, navigating, connecting with peers, listening to music, watching TV: These are only a few examples of typical online activities. In 1988, Mark Weiser first used the term "ubiquity of computing" to describe connected computers being everywhere and used in all areas of life. To him, it was a vision of the future, but today, we have almost reached this point. Especially due to the ever increasing use of connected devices also raises the amount of data each individual generates. Well aware, users are then faced with the task of handling online information adequately, knowing how to interact and also knowing about protective measures to uphold their privacy, use these accordingly, and ensure that their data only reaches those they intended to have access. However, the wish for, knowledge about, and actual application of the available measures rarely coincides in "normal" internet users.

There are many studies demonstrating the discrepancy between the privacy protective behaviors of internet users and their strong reported concerns about their online privacy (e.g., Beresford et al., 2012; Taddicken, 2014), corroborating the well-known gap between behavior and attitudes (Ajzen and Fishbein, 1977). Within social science research, many attempts to unscramble this so-called privacy paradox have been made, e.g., by describing privacy decisions as an individual weighing of risks and benefits, the so-called privacy calculus (Dinev and Hart, 2006). However, as humans normally do not act logically but rather affectively, not all users seem to act rationally according to the calculus.

The present study asks the question, whether users differ in their approaches to online privacy behavior and attitudes. Maybe some users rationally weigh benefits and barriers, but others have a more emotional consideration of pro- and contra-using motives or might even follow a situational approach. Possibly, some are not aware of the risks or do not know how to protect their privacy online. Others could know those privacy risks very well and still do not protect information adequately. In this explorative approach, we collect users' behaviors and attitudes regarding their online usage patterns and, using

Schomakers, E., Lidynia, C., Vervier, L. and Ziefle, M.
Of Guardians, Cynics, and Pragmatists.
DOI: 10.5220/0006774301530163
In *Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security (IoTBDS 2018)*, pages 153-163
ISBN: 978-989-758-296-7

cluster analysis, generate profiles of different user types and their attitudes towards privacy, their concerns, and their actual behavior regarding the protection of their privacy.

2 RELATED WORK

To gain a basic understanding of the investigated theoretical concepts, an overview of the meaning of online privacy is presented at first. The concepts ‘privacy concern’ and ‘privacy paradox’ are then described in more detail before existing privacy typologies are outlined shortly.

2.1 Online Privacy

What is it we are talking about? Although privacy is a topic in most debates and discourses about emerging technologies, the Internet of Things, and related policies as well as codes of conduct, the concept itself has been proven difficult to define (cf. Solove 2006, 2008). Many attempts have been made, though. Warren and Brandeis (1890) began by declaring privacy as a right, especially a right to be left alone. With the definition of privacy as the control over information about oneself (Westin 1968), the aspect of informational privacy is put into focus. But this is not the only dimension of privacy. For Burgoon (1982, 1989), for example, privacy means the active limitation of access to one’s physical, psychological, interactional, and informational self. As Finn et al. (2013) expand on Burgoon’s work, they restructure the previous suggestions by addressing the informational self as privacy of data and image as well as privacy of communication. Especially in the digital age, or information age, its aspect of protecting one’s information and data is ubiquitous. Koops et al. (2017) propose a two-level approach that includes eight privacy dimensions (bodily, spatial, communicational, proprietary, intellectual, decisional, associational, and behavioral) and, on the second level, informational privacy as a possible part of the other types of privacy.

2.2 Privacy Concerns and the Privacy Paradox

As Koops et al.’s (2017) two-level approach shows, nowadays data collection in connection to the ubiquity of connected devices can endanger privacy in all its dimensions, as our lives are increasingly more online. Correspondingly, users are concerned (Baruh et al., 2017). Research has been studying informational privacy concerns as indicator and measurement of privacy attitudes in the past centuries, for detailed reviews, see, for example, Buchanan et al. (2007) or Smith et al. (2011). This research shows quite clearly that most people are very concerned. Nevertheless, they still generate tons of data as they surf the web, use apps, reward cards, etc. It could even be shown that for a little reward or instantaneous gratification like a piece of chocolate, they give their passwords to a stranger (Happ et al., 2016) and, on the other hand, are unwilling to invest 1 Euro extra to ensure more privacy within an online transaction while buying DVDs (Beresford et al., 2012). So obviously, there is a discrepancy between the attitude of people and their actual behavior - the ‘privacy paradox.’

To understand the privacy paradox, different theories have been proposed by researchers. For example, the theory of the privacy calculus postulates that users perform a calculus between the risks for privacy and the benefits they gain (e.g., Dinev and Hart 2006, Xu et al., 2011). Other authors criticize that privacy decisions are affected by bounded rationality, meaning cognitive limitations and limited information access, as well as cognitive biases; for example, previous experiences and (successful) strategies will guide behavior in new situations (e.g., Acquisti and Grossklags, 2005, Kehr et al., 2013). After interviewing German internet users about their internet use, Hoffmann et al. (2016) proposed the term “Privacy Cynicism” as a coping strategy of internet users for the complex online world to explain privacy paradoxical behavior:

> “Privacy cynicism allows users to take advantage of online services without trusting providers while aware of privacy threats by forming the conviction that effective privacy protection is out of their hand.” (p. 7)

2.3 User Diversity

To understand motives and possible barriers to the use of online services or technologies in general, it is important to understand the rationale and mental models of (potential) users when using the internet. But as user diversity is a key feature of novel human-computer interaction in general (Ziefle and Jakobs, 2010) and online behaviors in particular (Karim et al., 2009; Ziefle et al., 2015), it is more than reasonable to assume that there is no “one type of internet user.” As manifold as the individuals are the possible influences on their attitudes and behaviors. Individual differences in personality traits, knowledge and experiences, self-efficacy in privacy protection, desire for privacy, and awareness of privacy issues, to name but a few, all play a part in guiding one's concerns and behaviors (e.g., Li, 2011).

User typologies are used to segment users with similar characteristics into homogenous groups. Several privacy-related typologies have been derived by researchers. One of the first and most influential typologies is the Privacy Segmentation Index by Alan Westin (Sheehan, 2002) which categorizes users according to the level of their concern as either privacy fundamentalists (high privacy concern), pragmatists (moderate privacy concern), or unconcerned. In several studies, this typology has been used to explain privacy behavior or attitudes with varying degrees of success (Woodruff et al., 2014; Jai and King, 2016; Sheehan, 2002; Hoofnagle and King, 2008; Baruh and Cemalcilar, 2014).

Smit et al. (2014) also segmented internet users based on concern. In their study, the group of highly concerned users applied the most privacy protective measures while showing the least knowledge about cookies and online behavioral advertising. In contrast, the low concern group showed the most knowledge regarding cookies and advertising practices but utilized the least privacy protection. Baruh and Cemalcilar (2014) derived a typology of social network users showing that privacy protective measures and willingness to disclose information to different receivers can be partly explained by differing privacy attitudes. Lankton et al. (2017) based their typologies of social network users on the privacy management behavior and showed that this corresponds to privacy concern. These findings indicate that privacy attitudes can, in contrast to the phenomenon of the privacy paradox, in a way influence privacy protection behavior if one accounts for different user types.

These approaches either used differences with respect to privacy concerns to create the clusters and then analyzed the relationship of these clusters to privacy behavior, or vice versa. We hypothesize that users do not only differ in their levels of privacy concern and behaviors but also in the relationship between both variables. To test this, we follow an explorative approach towards forming a user typology based on both privacy concerns (attitudinal level) and reported protective behaviors (behavioral level). We question whether the privacy paradox and explanatory theories, like the privacy calculus, are universal for all users or, rather, if users differ in their approach to privacy.

3 RESEARCH METHODOLOGY

The present study pursues the intention of identifying different types of internet users regarding the interplay of their privacy concerns and protective behaviors. These clusters (formed by cluster analysis) will then be examined for statistically meaningful differences in other privacy-related attitudes, experiences, personality traits, and demographic characteristics.

To identify, evaluate, and measure these clusters, a quantitative approach in form of an online questionnaire was conducted. In the following, the questionnaire will be described, followed by the chosen statistical methods. Finally, the sample will be characterized.

3.1 The Questionnaire

The survey consisted of five parts. Starting with demographic factors in part one (age, gender, education level), variables regarding the person were assessed in a second part. These included experience with privacy violations, awareness of privacy issues, privacy self-efficacy, and the big five personality traits in the shortened version by Rammstedt et al. (2012), with the personality dimensions extraversion, agreeableness, openness, neuroticism, conscientiousness. Part three examined the users' privacy attitudes: privacy concern, trust in online, and need for privacy. Protection behavior as well as the usage of widespread online services was surveyed in part four. Additionally, single items regarding reasons not protect privacy were evaluated by the participants. The items are listed in table 1.

Table 1: List of Items (items listed without source are self-developed).

Privacy Protection Behavior
I use every option that I know to protect my online privacy (e.g., deleting cookies, anti-virus software).
I specifically search for more options to protect my online privacy.
I use the default settings of my devices and applications without changing them.
I use the default settings of my devices and applications without installing additional software to protect my privacy.
Privacy Concern
In general, I am concerned about my privacy when I am using the internet. (~ Joinson, 2006)
I do not see risks when providing data in the internet. (~ Xu et al. 2008))
With some type of information collected in the internet I do not feel comfortable. (~ Dinev at al., 2009)

Table 1: List of Items (items listed without source are self-developed) (cont.).

Need for Privacy
Compared to others, I am more sensitive about the way online companies handle my personal information. *(Li, 2014)*
I have nothing to hide, so I am comfortable with people knowing personal information about me. *(Morton 2013)*
Compared to others, I see more importance in keeping personal information private. *(Li, 2014)*
Trust in Online Companies *(McKnight, 2002)*
I feel that most online companies would act in a customers' best interest.
If a customer required help, most online companies would do their best to help.
Most online companies are interested in customer well-being, not just their own well-being.
Experience *(adapted from Li, 2014)*
I believe that my online privacy was invaded by other people or organizations.
I have had bad experiences with regard to my online privacy before.
I experienced misuse of data from friends or family.
Privacy Self-Efficacy *(adapted from* Beier, 1999)
I know most privacy settings of the applications I use.
Because I have had no problems with privacy settings so far, I am confident for future privacy tasks.
I do not read privacy policies because I do not understand them.
I always change my privacy settings when I start using a new device or application.
I feel helpless with privacy settings and measures, so I do not change anything.
Awareness
I follow the news and developments about privacy issues and privacy violations. *(Xu et al., 2008)*
I cannot comprehend the relevance of the issue privacy because I do not care about it.
I pay closer attention to privacy issues and privacy violations since they have become so prominent in media.
Statements
Privacy protection does not work. Whoever wants to can still access my data.
I feel comfortable providing data on the internet because I get rewards (e.g., individualized advertisement, information from friends).
I do not have enough time to keep informed and apply privacy protection.
Privacy protection has become so complex that I do not know how to protect my privacy anymore.

All items had to be rated on a 5-point Likert scale ranging from "I do not agree" (1) to "I agree" (5). The only exception was the use of online services for which we offered a 'yes' or 'no' answering option ("I use this kind of service" or "I do not use this kind of service.")

To assess the reliability of the scales, Cronbach's α was calculated. Two scales showed moderate reliability (Cronbach's α between .6 and .7). As the scales consists of only 3 items each, including reversely coded items, and because of the exploratory nature of this study, these were still deemed acceptable.

The survey was rolled out twice. In December 2016, it was distributed online by an independent market research company (N=200), and five months later, more participants were acquired through personal networks (N=145). In the second round, the survey was conducted online as well as in paper-pencil form to also reach people who use the internet less often. Still, using the internet at all was a prerequisite to be included in the sample.

No statistical differences between the two samples could be discovered with respect to the demographic, attitudinal, or behavioral variables. Completing the questionnaire took about 20 minutes.

3.2 Statistical Analysis

In order to identify possible user profiles, both sample polls were first aggregated and then a two-step cluster approach (cf. Hair et al., 2010) was conducted to identify clusters of internet users who differ in their attitudes and behaviors regarding online privacy. The scales 'general privacy concern' and 'privacy protection behavior' were used to segment users. First, a hierarchical cluster analysis was conducted to identify outliers and determine the optimal number of cluster. A three-cluster solution was then run as k-means cluster analysis to determine the final clusters (with randomly selected seed points). Cluster stability was assessed by rerunning the analysis. Cross-classification proved a very good cluster stability.

For validation and interpretation, ANOVA procedures were used on the segmentation variables, as well as the other attitudinal variables. Chi Square tests were calculated for categorical variables.

3.3 Sample Description

The questionnaire was completed by N=345 German internet users. After the exclusion of outliers, N=337 were used for analysis. Gender is equally distributed across the sample (50.7% women). The participants were aged between 13 and 78 years (*M* = 43.5, *SD* = 15.2) and people with different educational background were included (37.1% completed a college education or higher). Age groups were formed to be comparable to other user typologies regarding privacy attitudes and behaviors (e.g., Sheehan, 2002; Woodruff et al., 2014). For a detailed description of the demographic characteristics, see Table 2.

Table 2: Demographic characteristics of the aggregated sample (N=337).

Demographic characteristics		Percentage of respondents
Age [years]	mean (SD)	43.5 (15.22)
	14-24	14.5%
	25-34	18.1%
	35-44	17.5%
	45-54	21.4%
	55-64	19.6%
	65 +	8.9%
Gender	women	50.7%
	men	49.3%
Education level	No college	62.9%
	College or higher	37.1%

4 RESULTS

The presentation of the results begins with the detailed description of the three identified clusters. Findings with regard to the segmentation variables "privacy concern" und "protection behavior" are presented as well as findings regarding other privacy attitudes and the agreement to reasons to not actively protect one's privacy. Secondly, the demographic characteristics of the clusters are compared before differences in personality traits as well as the usage of online services are outlined.

The clusters differ significantly regarding the segmentation variables (Welch's $F_{\text{Privacy\_Concern}}$ (2, 216) = 366.8, p < .001; $F_{\text{Protection\_Behavior}}$ (2, 334) = 262.67, p < .001), validating a good distinctness between the identified clusters. Mean values of the segmentation variables are depicted in Figure 1. In order to distinguish the three clusters, we labeled them the "Privacy Guardians," "Privacy Cynics," and "Privacy Pragmatists," respectively. Detailed descriptions of each user profiles follow in the next sections.

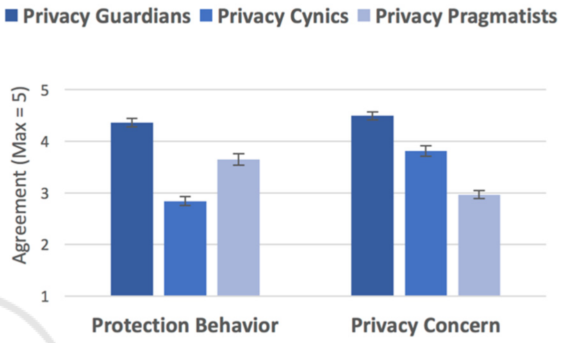

Figure 2: Mean values of overall scores of privacy protective behavior and privacy concern of the three clusters (with 95% confidence intervals, N=337).

4.1 The Privacy Guardians

The first cluster reports the highest privacy protection behavior (*M* = 4.36, *SD* = 0.48) as well as the highest level of privacy concern (*M* = 4.49, *SD* = 0.45) compared to both other groups (min = 1; max = 5, cf. Figure 2. Apart from the high privacy concern, this cluster shows generally strong privacy attitudes (see Figure 1). Compared to the other clusters, members report to have the highest need for privacy (*M* = 4.27, *SD* = 0.74) and being the most aware of privacy issues (*M* = 3.99, *SD* = 0.7). At the same time, they indicate to have made the most bad experiences with privacy violations online (*M* = 3.19, *SD* = 1.07) and show the lowest level of trust into online companies (*M* = 2.47,

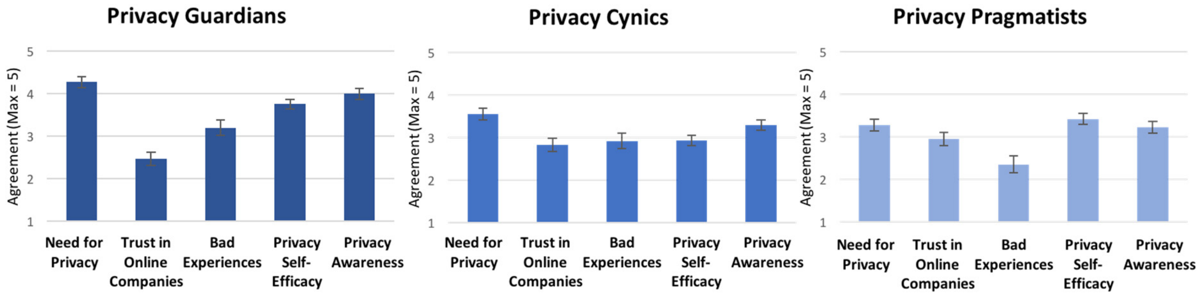

Figure 1: Mean values of overall scores of privacy attitudes of the clusters (with 95% confidence intervals, N=337).

SD = 0.93). Also, they report to be confident in their abilities to protect their online privacy (*M* = 3.75, *SD* = 0.64).

These privacy attitudes paint the clear picture of people who value privacy highly and have a high motivation to protect it. In addition to these privacy attitudes, several single items regarding reasons for not protecting privacy have been rated by the participants (see Figure 3). Corresponding to the high valuation of privacy, the cluster members mostly reject these statements. Especially the statements that “benefits repay for data collection” and that there is “not enough time for privacy protection” are rejected strongly (*M* = 1.64, *SD* = 0.97; and *M* = 1.83, *SD* = 0.94). Still, cluster members moderately agree that privacy protection is too complex and may be ineffective (*M* = 3.16, *SD* = 1.14; and *M* = 2.67, *SD* = 1.19), which seems counterintuitive as members of this cluster report a high level of privacy self-efficacy.

This cluster has been labelled “The Privacy Guardians” because of the strong concern and need for privacy that result in taking effort and time for privacy protective measures - and not accepting any reasons for inactivity in that regard.

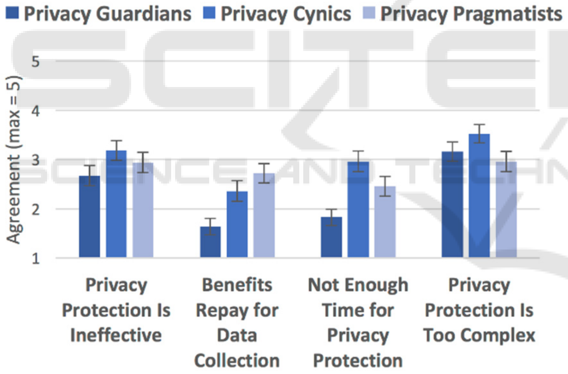

Figure 3: Mean agreement to reasons not to protect privacy for all three clusters (with 95% confidence intervals, N=337).

4.2 The Privacy Cynics

The second cluster shows the lowest privacy protection behavior compared to the others (*M* = 2.84, *SD* = 0.46) but still reports a moderately high privacy concern (*M* = 3.81, *SD* = 0.51). Here, the privacy paradox is perfectly illustrated and in full effect.

Regarding the other privacy attitudes, this group reports mostly average values that are in-between the other two clusters: This cluster shows a moderately high need for privacy (*M* = 3.55, *SD* = 0.71), moderately low trust in online companies (*M* = 2.83, *SD* = 0.8), moderate experiences with privacy violations (*M* = 2.92, *SD* = 0.92), and moderate awareness of privacy issues (*M* = 3.3, *SD* = 0.63). The group stands out only with a low level of privacy self-efficacy compared to the other clusters (*M* = 2.94, *SD* = 0.61). Correspondingly to the low self-efficacy, cluster 2 agrees the most to privacy protection being ineffective, too complex, and too time-consuming.

In line with the privacy paradox phenomenon, the low self-efficacy in terms of protecting behaviors and the higher agreement with the statements for not protecting privacy indicate that members of this cluster may not feel able to protect their privacy. On the other hand, this cluster seems to not put the most effort into privacy protection, as privacy is important but not that much. Also, they do not feel overly uncomfortable with providing data on the internet because they are rewarded with benefits like free services (cf. the moderate agreement to “benefits repay for data collection”).

Only moderately low trust in online companies, moderate awareness of privacy issues, moderately high privacy concern, and the feeling of privacy protection being, on one hand, too complex and therefore the own abilities not enough, and, on the other hand, ineffective anyhow: these characteristics match the description of privacy cynicism found in Hoffmann et al. (2016). Hence, the cluster was named “The Privacy Cynics.”

4.3 The Privacy Pragmatists

Cluster 3 shows the least privacy concern (*M* = 2.97, *SD* = 0.41) but a moderately high privacy protection behavior (*M* = 3.65, *SD* = 0.57). This is complemented by a moderately high privacy self-efficacy (*M* = 3.43, *SD* = 0.65).

In the other privacy related scales, the third cluster shows moderate and comparatively less pronounced attitudes: Members report the lowest need for privacy (*M* = 3.27, *SD* = 0.76), the least bad experiences (*M* = 2.35, *SD* = 1.01), and a moderate awareness (*M* = 3.22, *SD* = 0.71). Trust in online companies is the highest compared to the other clusters (*M* = 2.94, *SD* = 0.81).

The evaluation of the reasons for not protecting privacy can give some hints into understanding these attitudes and behaviors. This cluster agrees moderately to some of these reasons but does not perceive privacy protection as that complex, time-consuming, and ineffective as the Privacy Cynics, confirming the reported moderately high privacy self-efficacy.

The level of privacy concern of this cluster is the lowest compared to the other clusters, but it is still present. Even the most unconcerned do not reject concern completely (Min = 1.67 on a scale of 1 to 5) and only 11.3% (rather) reject privacy concerns on average (mean value lower than the midpoint of the scale). Of these rejecters, 97.4% were grouped into this cluster. This group feels somewhat comfortable with online data collection because of the benefits for the users; thus, weighing benefits and privacy concern against each other. Therefore, many parallels can be drawn to the description of privacy pragmatists in Westin's typology: moderate concern and pondering privacy and benefits (Sheehan, 2002). Accordingly, this cluster is labelled "The Privacy Pragmatists."

4.4 Demographic Characteristics

Table 2 depicts the demographic characteristics of the individual. The clusters are almost equal in size. The Privacy Guardians are significantly older than the Privacy Cynics and Privacy Pragmatists (*F(*2, 334) = 10.58, *p* < .001) and most of the participants older than 55 years belong to this cluster (61%). 43% of the youngest participants (< 25 years old) belong to the Privacy Cynics cluster. More Privacy Guardians are female than male; in contrast, more Privacy Pragmatists are male. The Privacy Guardians tend to be higher educated, but the differences in education level and gender distribution are not statistically significant.

Table 3: Demographic characteristics of the clusters (percentage of members within the cluster).

	Privacy Guardians (38%)	Privacy Cynics (31%)	Privacy Pragmatists (31%)
Age [years]			
mean (SD)	47.55 (14.38)	38.55 (15.12)	43.38 (14.99)
14-24	8.5%	20.4%	16.2%
25-34	13.2%	26.2%	16.2%
35-44	15.5%	19.4%	18.1%
45-54	22.5%	18.5%	23.8%
55-64	21%	9.7%	15.2%
65 +	9.3%	6.8%	10.5%
Gender			
women	55.8%	50.5%	44.8%
men	44.2%	49.5%	55.2%
College education or higher			
no	58.9%	62.1%	68.6%
yes	41.4%	37.9%	31.4%

4.5 Differences in Personality Traits

Additionally to the privacy related attitudes, personality traits of the participants were assessed (cf. Figure 4). The Privacy Guardians are significantly more open (*M* = 3.62, SD = 0.95, *F*(2, 334) = 8.04, *p* < .001) and more conscientious than the other two groups (*M* = 3.83, *SD* = 0.72, *F*(2, 334) = 6.03, *p* < .01). Especially high conscientiousness fits into the picture of those carefully and thoroughly guarding their privacy. More openness to learn how to protect privacy can be helpful in this regard, too. As the technologies and algorithms change quickly, new approaches to privacy protection need to be learned. The clusters did not show any differences in the other big five personality traits of neuroticism, agreeableness, and extraversion.

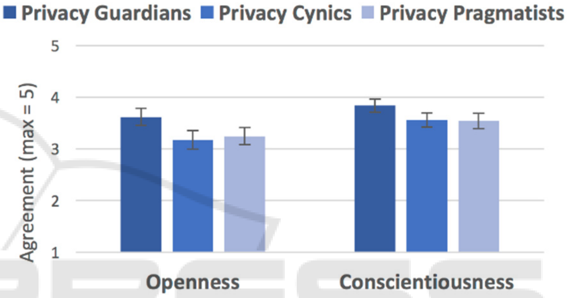

Figure 4: Mean values of personality traits of the three clusters (with 95% confidence intervals, N=337).

4.6 Differences in the Use of Widespread Online Services

Online privacy cannot only be managed by applying protective measures like installing software, using add-ins, or adjusting privacy settings. Not using online services that collect data is another valid privacy management strategy. Figure 5 depicts the usage of different online services, split by the clusters. Surprisingly, significantly more Privacy Guardians shop online than do Privacy Pragmatists ($\chi^2(2)$ = 11.33, *p* < .01). At the same time, more Privacy Pragmatists than Privacy Guardians use Social Media ($\chi^2(2)$ = 6.57, *p* < .05). But those differences are rather small and in the usage of other online services, no differences could be revealed. After all, most online services are widely used, showing that this sample does not refrain from using the beneficial services of the internet despite moderate to high privacy concerns.

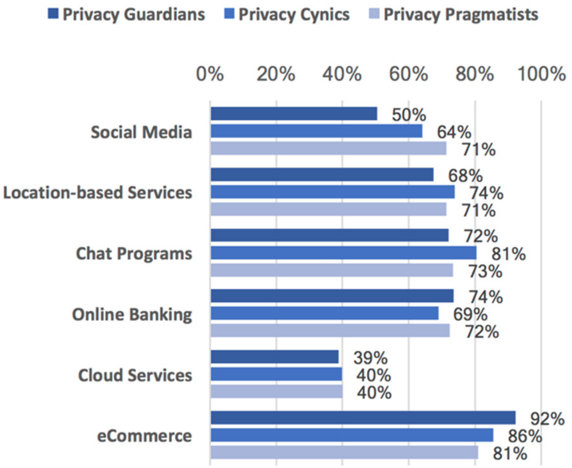

Figure 5: Percentage of participants that use various online services divided by clusters (N=337).

5 DISCUSSION

Employing an explorative approach to reveal user profiles with regard to online behaviors, users have been segmented into clusters that differ in the interplay of privacy concerns and protective behavior. Three clusters could be identified in a two-step cluster analysis.

The first cluster, labelled "The Privacy Guardians," reported strong valuation of and concerns for privacy as well as above average privacy protective behavior. "The Privacy Pragmatists," in contrast, show moderate concerns and a moderately high protection behavior. They reported to be confident in their abilities to protect their privacy but do not value privacy as high as the other clusters. Privacy Pragmatists weigh benefits and concerns of internet use against each other and can, thus, be compared to the privacy pragmatist segments of Westin's studies (cf. Sheehan, 2002).

Hoffmann et al. (2016) coined the term "privacy cynicism" for a coping strategy of concerned but low-skilled internet users, who deem privacy protection as ineffective. The described characteristics are fully prevalent in the second cluster, therefore named the "Privacy Cynics." This is also the only cluster, in which a paradoxical relationship between high privacy concern and low privacy protection behavior can be observed. Especially the low confidence in their own abilities to protect their privacy is distinctive for this group.

The evaluation of single statements regarding reasons to not employ privacy protection are helpful in understanding the clusters. The Privacy Cynics seemed overwhelmed by the complexity of the matter. Therefore, this type of user would benefit greatly from easy-to-understand guidelines and easy-to-use measures to aid in the protection of their privacy without missing out on the benefits online services. As this was also the youngest cluster in our sample, it is necessary to provide the right education in online etiquette and offering tools as early as possible, perhaps already in school, together with the means of a responsible use of online services and digital devices, referred to as digital citizenship (Ribble et al., 2004).

Hoffmann et al. (2016) describe privacy cynicism as state of resignation, of feeling powerless, in order to explain disparities between privacy concerns and awareness of privacy threats without a corresponding privacy protection behavior. In our present study, privacy self-efficacy as well as privacy protection behavior in general were assessed. For a complete picture, knowledge about privacy protection and concrete privacy management strategies need to be included in the study of Privacy Cynics, to examine whether the moderately low privacy self-efficacy actually corresponds to a low knowledge and less (effective) privacy protection strategies, or if the perception of privacy protection being ineffective leads to a disparaging of the own skills.

Similarly, the scale of privacy protection used in this study assesses a very general *"I do use privacy protective measures"* in opposite to concrete measures taken by the participants. Previous studies showed that there is not "the one approach" to privacy protection but rather different privacy management strategies (e.g., Lankton et al. 2017, Sheehan 2002). These cannot be distinguished in this survey and may differ between and within the clusters.

In many privacy-related typologies, one group of users with high valuation of privacy exists, like the Privacy Guardians in this study. In Westin's studies, they are called the "Privacy Fundamentalists;" Sheehan et al. (2002) labelled this group "Alarmed Internet Users," Baruh and Cemalcilar (2014) "Privacy Advocates," and Milne et al. (2016) dubbed them "Risk Averse." Although these typologies are based on different approaches to studying privacy attitudes, they show many similarities: not only a high concern and value for privacy but also strong protection of their privacy with protective measures and/or a low willingness to disclose information. Privacy Guardians tend to be older, have a higher level of education and reveal a higher proportion of women than the other groups. In the present study, these results can be confirmed.

In spite of their high privacy self-efficacy, the Privacy Guardians partly agree to the statement that privacy protection is ineffective and too complex. Hence, also this group could profit from guidelines and easier-to-use measures, instruments, or tools to enable protection of their online data. Because of the high valuation of privacy and the effort and time, they are willing to put into protection, more advanced tools with more options, as well as more detailed guidelines could address this user group.

The Privacy Pragmatists exhibited the lowest privacy concern in this study, but they are still not unconcerned. A group of unconcerned or indifferent internet users (as in the studies of Westin (Kumaraguru and Cranor, 2005); Sheehan (2002), Baruh and Cemalcilar (2014), and Tsarenko and Tojib (2009)) was not present. All groups reported to be aware of privacy issues and to have a low trust in online companies. The Privacy Pragmatists report to have a high self-efficacy, thus believe that they are able to protect their privacy when it is necessary.

An analysis of personality traits of the clusters showed the Privacy Guardians to be more conscientious and open to new experiences as the Cynics or Pragmatists. Especially a higher conscientiousness fits into the picture of the concerned and determined Privacy Guardians. Openness to learn new privacy protection strategies is also needed for keeping up with the fast changing online tools and threats. But the differences between the groups are small and mostly not significant. It seems that personality does barely, if at all, influence privacy attitudes and behaviors.

The use of widespread online services and social media does not vary much between the groups. Social networks are used by more Privacy Pragmatists than Privacy Guardians, whereas more Privacy Guardians use online shopping. The latter seems paradoxical, but the differences are small, showing that the use of online services alone is not really predictable based on concerns. Privacy management is always a combination of protective measures, general use of services, and how services are used. Not even Privacy Guardians want to be excluded from the online world and its tremendous benefits.

Further investigations of the identified user groups or clusters is needed. While the sample size of this study yielded reliable findings in terms of cluster analyzed user groups, still, more representative samples and more detailed questioning of the privacy protection measures could be helpful to broaden the picture of privacy behaviors. In addition, the role of domain knowledge should be focused, thus exploring the influence of knowledge of privacy threats and possible countermeasures to contribute to educational requirements regarding digital citizenship (Ribble et al., 2004). Regression analyses within the user groups to analyze the predictors of privacy behaviors and concern could help to understand their actions. So far, the group of privacy cynics has only been described in German studies. However, it has been shown that online behaviors and attitudes towards privacy are cultured (Hargittai, 2007; Krasnova and Veltri, 2010). It would therefore be of interest, if the identified user profiles would reveal similar user characteristics in different countries.

6 OUTLOOK

Our research aimed at examining whether internet users differ not only in their level of privacy concern and privacy protection behavior but also in the combination of those variables. We could show that three distinct user group exist: The Privacy Guardians are very concerned, value privacy highly, and try to protect their online privacy by every means. Privacy Pragmatists are confident in their abilities to protect their privacy, but they are not as concerned. The Privacy Cynics is the only group, in which a privacy paradoxical behavior was prevalent. This group matched perfectly the description of privacy cynicism as Hoffmann et al. (2016) defined it: They are resigned, feel powerless, and are overwhelmed by the complexity of the online world and the responsibility to protect their online privacy.

The present research provided valuable insights to understand different user groups and the privacy paradox. In the world of ubiquitous computing, in which individual users are under constant pressure to protect their privacy, appropriate solutions for all users have to be provided. By addressing common denominators, obstacles can be lessened and policies introduced to try and offer a solution that fits most users and not just a small selected few.

ACKNOWLEDGEMENTS

The authors thank all participants for sharing their thoughts and opinions. Furthermore, the research support of Stefan Ahlers is highly appreciated. This research was funded by the German Ministry of Education and Research (BMBF) under the project MyneData (KIS1DSD045).

REFERENCES

Acquisti, A., and Grossklags, J. 2005. Privacy and Rationality in Individual Decision Making. *IEEE Security and Privacy*, *3*(1), 26–33.

Ajzen, I., and Fishbein, M. (1977). Attitude-behavior relations: A theoretical analysis and review of empirical research. *Psychological Bulletin*, 84(5), pp. 888.

Baruh, L., and Cemalcılar, Z., 2014. It is More Than Personal: Development and Validation of a Multidimensional Privacy Orientation Scale. *Personality and Individual Differences*, *70*, 165–170.

Baruh, L., Secinti, E. and Cemalcilar, Z., 2017. Online Privacy Concerns and Privacy Management: A Meta-Analytical Review. *Journal of Communication*, 67(1), pp.26–53.

Beresford, A.R., Kübler, D. and Preibusch, S., 2012. Unwillingness to Pay for Privacy: A Field Experiment. *WZ Discussion Paper, No. SP II 2010-03.*

Beier, G., 1999. Kontrollüberzeugungen im Umgang mit Technik, Report Psychologie. pp. 684–693.

Buchanan, T. et al., 2007. Development of Measures of Online Privacy Concern and Protection for Use on the Internet. *Journal of the American Society for Information Science and Technology*, 58(2), pp.157–165.

Burgoon, J.K., 1982. *Privacy and Communication*, Beverly Hills, CA: Sage.

Burgoon, J.K. et al., 1989. Maintaining and Restoring Privacy through Communication in Different Types of Relationships. *Journal of Social and Personal Relationships*, 6(2), pp.131–158.

Dinev, T., and Hart, P., 2006. An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, 17(1), 61–80.

Dinev, T., Xu, H. and Smith, H.J., 2009. Information Privacy Values, Beliefs and Attitudes: An Empirical Analysis of Web 2.0 Privacy. In *Proceedings of the 42nd Hawaii International Conference on System Sciences*. pp. 1–10.

Finn, R.L., Wright, D. and Friedewald, M., 2013. Seven Types of Privacy. In S. Gutwirth et al., Eds. *European Data Protection: Coming of Age*. Dordrecht: Springer Science+Business Media B.V., pp. 3–32.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., and Tatham, R. L., 1998. *Multivariate data analysis*. Upper Saddle River, NJ: Prentice hall.

Happ, C., Melzer, A. and Steffgen, G., 2017. Trick with treat - Reciprocity increases the willingness to communicate personal data. *Computer in Human Behavior*. 61, 372–377.

Hargittai, E., 2007. Whose space? Differences among users and non-users of social network sites. *Journal of Computer Mediated Communication*, 13(1), pp.276-297.

Hoffmann, C.P., Lutz, C. and Ranzini, G., 2016. Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace,* 10(4), pp.1–18.

Hoofnagle, C. J., and King, J., 2008. *Research Report: What Californians Understand about Privacy Online. Social Science Research Network.*

Jai, T. M., and King, N. J., 2016. Privacy Versus Reward: Do Loyalty Programs Increase Consumers' Willingness to Share Personal Information with Third-Party Advertisers and Data Brokers? *Journal of Retailing and Consumer Services*, *28*, pp. 296–303.

Joinson, A. N., Paine, C. B., Buchanan, T. B., and Reips, U. R., 2006. Measuring Internet Privacy Attitudes and Behavior: A Multi-Dimensional Approach. *Journal of Information Science,* 32(4), 334-343.

Karim, N. S. A., Zamzuri, N. H. A. and Nor, Y.M., 2009. Exploring the relationship between Internet ethics in university students and the big five model of personality. Computers and Education, 53(1), pp. 86-93.

Kehr, F., Wentzel, D., and Mayer, P., 2013. Rethinking the Privacy Calculus: On the Role of Dispositional Factors and Affect. *The 34th International Conference on Information Systems*, (1), 1–10.

Koops, B.-J. et al., 2017. A Typology of Privacy. *University of Pennsylvania Journal of International Law*, 38(2), pp.483–575.

Krasnova, H. and Veltri, N. F., 2010. Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA. In*: 43rd Hawaii International Conference on System Sciences (HICSS), Hawaii, USA*, pp. 1–10.

Kumaraguru, P., and Cranor, L., 2005. *Privacy indexes: A survey of westin's studies*. School of Computer Science, Carnegie Mellon University.

Lankton, N. K., McKnight, D. H., and Tripp, J. F., 2017. Facebook Privacy Management Strategies: A Cluster Analysis of User Privacy Behaviors. *Computers in Human Behavior*, *76*, pp.149–163.

Li, H., Sarathy, R. and Xu, H., 2010. Understanding situational online information disclosure as a privacy calculus*. Journal of Computer Information Systems*, 51(1), pp.62–71.

Li, Y., 2011. Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework. *Communications of the Association for Information Systems*, *28*(28), pp.453–496.

Li, Y., 2014. The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision Support Systems*, 57(1), pp.343-345.

McKnight, D. H., Choudhury, V., and Kacmar, C., 2002. Developing and Validating Trust Measures for E-commerce: An Integrative Typology. Information systems research, 13(3), pp.334-359.

Milne, G.R., Pettinico, G., Haijat, F. and Markos, E., 2016. Information Sensitivity Typology: Mapping the Degree and Type of Risk Consumers Perceive in Personal Data Sharing. *Journal of Consumer Affairs,* pp.1–29.

Morton, A., 2013. Measuring inherent privacy concern and Desire for Privacy: A pilot survey study of an instrument to measure Dispositional Privacy Concern. *Proceedings - BigData 2013*, pp.468–477.

Rammstedt, B., Kemper, C., Beierlein, C. and Kovaleva, A., 2012. Eine kurze Skala zur Messung der fünf Dimensionen der Persönlichkeit: Big-Five-Inventory-10 (BFI-10). *GESIS Working Paper*, 23(2), pp.1–32.

Ribble, M. S., Bailey, G. D., and Ross, T. W. (2004). Digital citizenship: Addressing appropriate technology behavior. *Learning and Leading with technology*, 32(1), pp.6.

Sheehan, K. B., 2002. Toward a Typology of Internet Users and Online Privacy Concerns. *The Information Society*, *18*(1), pp.21–32.

Smit, E. G., Van Noort, G., and Voorveld, H. A. M., 2014. Understanding Online Behavioural Advertising: User Knowledge, Privacy Concerns and Online Coping Behaviour in Europe. *Computers in Human Behavior*, *32*, pp.15–22.

Smith, H.J., Dinev, T. and Xu, H., 2011. Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, 35(4), pp.989–1015.

Solove, D.J., 2006. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154(3), pp.477.

Solove, D.J., 2008. Privacy: A Concept in Disarray. In *Understanding Privacy*. Harvard University Press, pp. 1–11.

Taddicken, M., 2014. The “Privacy Paradox” in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure. *Journal of Computer-Mediated Communication*, *19*(2), 248–273.

Tsarenko, Y. and Tojib, T. R., 2009. Examining customer privacy concerns in dealings with financial institutions. *Journal of Consumer Marketing*, *26*(7), 468–476.

Warren, S.D. and Brandeis, L.D., 1890. The Right to Privacy. *Source: Harvard Law Review*, 4(5), pp.193–220.

Westin, A. F., 1968. Privacy and Freedom. *American Sociological Review*, *33*(1), pp. 173.

Woodruff, A., Pihur, V., Consolva, S., Schmidt, L., Brandimarte, L., and Alessandro, A., 2014. Would a Privacy Fundamentalist Sell Their DNA for $1000... If Nothing bad Happened as a Result? ... The Westin Categories, Behavioral Intentions, and Consequences. In *Tenth Symposium on Usable Privacy and Security*.

Xu, H., Dinev, T., Smith, H. J., and Hart, P., 2008. Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View. *ICIS 2008 proceedings*, Paper 6.

Ziefle, M., and Jakobs, E. M. (2010). New challenges in human computer interaction: Strategic directions and interdisciplinary trends. *4th International Con-ference on Competitive Manufacturing Techno-logies*. University of Stellenbosch, pp. 389-398.

Ziefle, M.; Halbey, J. and Kowalewski, S. (2016). Users' willingness to share data in the Internet: Perceived benefits and caveats. *Proceedings of the International Conference on Internet of Things and Big Data (IoTBD 2016)*, pp. 255-265.