International Journal of Information Management 46 (2019) 142–150

Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt

Internet users' perceptions of information sensitivity – insights from Germany

Eva-Maria Schomakers[a,*], Chantal Lidynia[a], Dirk Müllmann[b], Martina Ziefle[a]

[a] Human-Computer Interaction Center, RWTH Aachen University, Campus-Boulevard 57, 52074 Aachen, Germany
[b] Data Protection Research Institute, Goethe-University Frankfurt/Main, 60629 Frankfurt, Germany

ARTICLE INFO

Keywords:
Information privacy
Perceived sensitivity
Empirical study
Cultural comparison
Privacy attitudes

ABSTRACT

With the ever-increasing collection of user data, online privacy becomes an urgent matter for users and research across borders. The perception of information sensitivity is central to privacy attitudes and behaviors in different usage contexts. In an online questionnaire, n = 592 German internet users evaluated how sensitive they perceive 40 different data types. The German sensitivity evaluations revealed in this study are compared to results from the US and Brazil (Markos et al., 2017), in order to understand the cultural impact on evaluations. Additionally, we analyze how attitudes and demographic characteristics of the German sample influence the perception of sensitivity on an individual level. Some distinct differences in sensitivity perception between Germany, Brazil, and the US can be observed, but the rank orders of sensitivity of data types is very similar between the countries, indicating that there is a consensus on what constitutes sensitivity across nations. On an individual level, disposition to value privacy, risk propensity, and education level influence the perception of sensitivity. The findings contribute to an understanding of how to design information and communication strategies to inform internet users how to manage their data carefully.

1. Introduction

The internet has become a ubiquitous part of daily life. More than two thirds of the population in Western Europe uses smartphones, the utilization of connected devices and online services increases (UM London & eMarketer, 2018). For example, over one billion people connect and socialize on social media, revolutionizing social relationships, information and knowledge sharing, as well as marketing opportunities (AlAlwan, Rana, Dwivedi, & Algharabat, 2017; Kapoor et al., 2018; Shiau, Dwivedi, & Yang, 2017). Thereby, they create large amounts of data, so-called "Big Data", that, in turn, creates manifold opportunities for health care, companies, and society as a whole: Epidemics might be predicted and controlled. Innovative, user-centered products can be developed and novel business services can be identified that create new markets. Driving routes can be calculated in real time in line with energy efficient driving behaviors and a higher road safety – to name just a few opportunities (e.g., Nambiar, Bhardwaj, Sethi, & Vargheese, 2013; Sagiroglu & Sinanc, 2013). These applications of big data mostly depend on users to provide their data. Studies show that users are aware of the increasing amount of data that is collected about them and also about the possible risks associated with the data handling (European Commission, 2015).

In light of the new European General Data Protection Regulation (GDPR) whose provisions are to be applied as of May 2018, the debate about online privacy has accelerated. Privacy concerns are widespread and lead users to rethink their online use and data provision behavior (European Commission, 2015; Li, 2011b). How concerned users are about data collection depends not only on who collects the information and what for, but also what type of information is at stake (e.g., Valdez & Ziefle, 2018). The question arises which information is perceived as sensitive and what determines this perception of sensitivity as the sensitivity of information is perceived differently by every person (e.g., Bergström, 2015) and also differs across countries (e.g., Krasnova, Veltri, ö Günther, 2012).

Markos, Milne, and Peltier, (2017) showed that cultural differences in the evaluation of perceived sensitivity across data types exist. Beyond the differences in data types, the rank order of specific types of information was still very similar, which led the authors to hypothesize a global consensus on the level of sensitivity.

The aim of this research is to provide a European perspective on information sensitivity. Especially in light of the new European General Data Protection Regulation (GDPR), Markos et al.'s assumption of a global data sensitivity consensus needs to be explored. This study contributes a German perspective to the phenomenon.

* Corresponding author.
E-mail addresses: schomakers@comm.rwth-aachen.de (E.-M. Schomakers), dirk.muellmann@kit.edu (D. Müllmann).

https://doi.org/10.1016/j.ijinfomgt.2018.11.018
Received 25 July 2018; Received in revised form 30 November 2018; Accepted 30 November 2018
Available online 18 December 2018

2. Related work

In the following, the concept of information privacy is defined and the importance of sensitivity of information for the understanding of privacy attitudes and behaviors is stressed. Also, individual and cultural influences on privacy perceptions are outlined.

2.1. Information privacy

Privacy is a multidimensional construct reaching into different parts of our lives. Burgoon (1982) defines privacy as the limitation of access to the self and distinguishes between physical, psychological, interactional, and informational privacy. With the often used definition of privacy as control over information about oneself, Westin (1967) focusses on informational privacy. Nowadays, with the online world available (almost) everywhere, information privacy has become an integral part of all other types of privacy as data is collected about users almost all the time (Koops et al., 2017). Correspondingly, worries about information privacy are prevalent (European Commission, 2015). Empirical studies mostly refer to information privacy concerns as measure of the discrepancy between desired and actual state of privacy (Li, 2011b). Privacy concerns can be directed to the online world as whole or to a specific situation (Li, 2011a). Privacy concerns, among other attitudes and context factors, influence behavioral intentions and actual behaviors, e.g., the provision of information and use of technologies (e.g., Li, 2011b; Smith, Dinev, ö Xu, 2011).

2.2. Information sensitivity

As one important contextual factor, the perceived sensitivity of the information that is requested influences privacy concerns (Li, 2011a). The higher the perceived sensitivity of data the higher are the privacy concerns. It has been shown (Rohm ö Milne, 2004) that people are especially concerned about medical data and that individuals who perceive health information to be more sensitive also show a higher concern for health information (Bansal, Zahedi, ö Gefen, 2010). Moreover, when highly sensitive information is at stake, privacy concerns have a stronger negative effect on the willingness to provide information than when the information is low in sensitivity (Mothersbaugh, Foxx, Beatty, ö Wang, 2012).

However, what exactly is sensitive information? This depends, to a large degree, on the perspective. The General Data Protection Regulation ((EU) 2016/679, OJ L 119, 04.05.2016, 1 et seqq.) follows the principle of ban with reservation to permit (cf. Art. 6 Sec. 1 GDPR) concerning the execution of data processing. This means that data processing, by law, is forbidden as long as it is not explicitly allowed, e.g., by the users consent (Art. 6 Sec. 1 lit. a) GDPR). The GDPR only applies to personal data which is defined as any information relating to an identified or identifiable natural person (cf. Art. 4 (1) GDPR). Furthermore, it grants special categories of personal data a higher level of protection, which are seen as particularly sensitive (cf. recital 51 GDPR),. This category is determined as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership as well as genetic and biometric data, health data, or data concerning a person's sex life or sexual orientation (cf. Art. 9 Sec. 1 GDPR).

From the users' perspective, items that are more personally identifying are perceived as more sensitive (Malheiros, Preibusch, ö Sasse, 2013). But as technological developments accelerate, it cannot be assumed that every user knows how data can be linked to identify individuals. Additionally, users' evaluation of risk is highly subjective (Renn, 1989). The perception of risks and the perceived need of Internet security is also considerably impacted by the usage context (Asplund ö Nadjm-Tehrani, 2016). Correspondingly, the definition of information sensitivity as the potential loss associated with the disclosure of that information emphasizes the subjectivity of the sensitivity evaluation (Mothersbaugh et al., 2012). In addition, different types of information are associated with different types of risks (Milne, Pettinico, Hajjat, ö Markos, 2016). For example, credit card numbers are mostly associated with monetary risks, whereas the social network profile relates more to social and psychological risks. Markos et al. (2017) identify an information sensitivity continuum by empirically ranking 52 information types based on their perceived overall sensitivity and link this perception of sensitivity with the willingness to provide that information. In summary, sensitivity of information plays a crucial role for online privacy perceptions and depends on the type of information as well as on individual differences.

2.3. Individual differences

There is not one specific type of user with a fixed set of characteristics. Users vary, for example, in their perceived importance of privacy, how much they trust the parties who handle their personal data, or the way they evaluate risks. These personal characteristics and previous experiences or even current affect, may have an impact on the evaluation of sensitivity.

Privacy disposition reflects the individual need for privacy and represents a personality trait with a strong impact on privacy perception and the perceived sensitivity of information (Li, 2011a). Privacy disposition influences whether a foray into personal space is felt to be an intrusion or not (Xu, Dinev, Smith, ö Hart, 2008). Also, previous experiences with online privacy invasions and the perception of risks are strongly related to privacy perceptions (Li, 2011b; Smith et al., 2011).

Trust plays a very complex role in the context of privacy attitudes and behaviors. Trust beliefs lower information privacy concerns (Li, 2011b). But trust has also been found to be an antecedent to behaviors, to be influenced by privacy concerns, and to play a moderating role between attitudes and behaviors (Kirs ö Bagchi, 2012; Smith et al., 2011). Also, trust is not a one-dimensional concept. McKnight and Chervany (2000) postulate a typology of trust in which the disposition to trust, institution-based trust, trusting beliefs, and trusting intentions are distinguished. For the context of sensitivity of information, especially the concept of institution-based trust seems relevant, as trust into those institutions that handle data in general may influence sensitivity perception of information, independent from context.

Moreover, demographic characteristics like age and gender influence privacy perceptions. Some studies find no direct effect of age on privacy attitudes and data sensitivity perception (e.g., Hoofnagle, King, Li, ö Turow, 2010; Markos et al., 2017), but most report younger age groups to share more information and to be less concerned about information privacy (e.g., Miltgen ö Peyrat-Guillard, 2014; Van den Broeck, Poels, ö Walrave, 2015). Jones, Johnson-Yale, Millermaier, and Perez, (2009) show that young adults distinguish between information types, being concerned about sharing personally identifying information but not about sharing anonymous information. Ziefle and Calero Valdez (2018) report both, age-sensitive and age-insensitive findings in the medical context: very intimate data - e.g., data on mental illnesses - should not be shared in any situation. However, older users were more willing to share data on general health and physical illnesses whenever it contributes to a global benefit for the society.

Women report in most studies that they are more concerned about their information privacy than men (Li, 2011b; Smith et al., 2011). But Bergström (2015) show that differences in the perception of sensitivity based on gender are only prevalent regarding some contexts and information types. When it comes to educational effects, mixed findings are prevailing: A review study revealed no differences in privacy concerns depending on education levels (Li, 2011b), but other studies report that users with lower educational level tend to be less concerned (Blank, Bolsover, ö Dubois, 2014; Rainie, Kiesler, Kang, ö Madden, 2013). Thus, educational and gender differences in sensitivity perception could explain some discrepancies between empirical studies about privacy concerns.

2.4. Cultural differences

Markos et al. (2017) demonstrated differences in the perception of data sensitivity between cultures, in their case between Brazilian and

US American citizens. Brazilians are shown to perceive most information as less sensitive resulting in a higher willingness to provide information. But in comparison between the two perspectives, the rank order of specific types of information was similar, which leads to the hypothesis of a global consensus on the level of sensitivity.

Culture as the "collective programming of the mind that distinguishes the members of one group or category of people from another" (Hofstede, 2011, p. 3) influences thinking, feeling, and behaviors. This is also true for privacy attitudes and online behaviors (e.g., Miltgen ö Peyrat-Guillard, 2014; Trepte et al., 2017; Hossain ö Dwivedi, 2014). Krasnova and Veltri (2010) compare privacy concerns between the US and Germany and find that Germans fear more damage from self-disclosure in online social networks and also see a higher probability of privacy violations than US Americans. In a recent European comparison, Germany lists among the countries whose citizens are less concerned for their online privacy (Potoglou, Dunkerley, Patil, ö Robinson, 2017).

Hofstede (2011) distinguishes six cultural dimensions that represent values varying between cultures. In countries with a large power distance, inequalities and strong hierarchies are accepted and expected. A society is collectivistic if the people are integrated into extended families whereas in individualistic societies, one cares mostly for oneself and the immediate family. Masculine societies associate men with assertiveness and competitiveness whereas in a feminine society, men and women are both seen as modest and caring. Strong uncertainty avoidance leads to a need for clarity and structure while uncertainty is felt as a threat. Long-term oriented countries value perseverance and thrift; in short-term oriented countries, traditions are respected and it is important to save one's face. In indulgent countries, enjoying life and having fun is freely gratified whereas restrained countries have strict social norms controlling the gratification of needs.

Fig. 1 depicts the differences between Germany, the US, and Brazil in Hofstede's cultural dimensions. Especially regarding long-term orientation and indulgence, Germany differs from both the US and Brazil. As indulgence is related to saving one's face, privacy could be of less importance and information could be perceived as less sensitive in Germany as rather restrained country compared to the rather indulgent US and Brazil. But, regarding individualism, Germany scores in between the US and Brazil but still on the individualistic side, whereas individualistic countries stress the right for privacy (Hofstede, 2011).

In comparison between Brazil and the US, Markos et al. (2017) showed that not the cultural dimensions are the best predictor for the perceived sensitivity of information but the country of origin has a greater impact. Thus, the legislative conditions that users are accustomed to may influence their perception of sensitivity. With the first data protection act worldwide adopted in 1970 in the state of Hesse (GVBl. I., 1970, 625 et seqq.), Germany has the longest legal tradition of privacy regulation. Among other factors, it is highly influenced by the countries historical experience of two dictatorships cementing their power through surveillance and control of the citizens. In accordance with the right of informational self-determination, privacy is constitutionally protected by the German Grundgesetz (Art. 2 Sec. 1 in conjunction with Art. 1 Sec. 1 GG; BVerfGE 65, 1). Since 2018, the European Data Protection Regulation creates a coherent level of data protection within the whole European Union leaving only few areas for distinct national data protection laws. Germany's history as a country with high data protection standards may be ambiguous in its influence on the sensitivity perception of Germans: either they perceive most data to be more sensitive or – as it is already protected by law – data is perceived as less sensitive.

3. Method

In an empirical questionnaire approach, 592 German internet users evaluated the perceived sensitivity of 40 different data types. The results are compared to those of Markos et al. (2017) from a Brazilian and a US American sample.

3.1. The selection of information types

A qualitative pre-study was conducted to assess the comprehensibility of the information types by Markos et al. (2017) as well as to identify further sensitive information types. Two focus groups were carried out. After an introduction to the topic, the participants first brainstormed what data they provide when they go online or use smart devices. Secondly, all information types studied by Markos et al. (2017) were provided on paper cards and the participants should discuss their sensitivity, rank them, and add further sensitive or controversial data types.

The following data types were added by the participants: browsing history, medication, online dating activities, shopping behavior, alcohol consumption, data about sporting activities, hair color, and name of pet.

Additionally, some of the original items by Markos et al. (2017) were shown to be not comprehensible to German internet users. All information types that were not understood directly by all participants were dropped for the subsequent study. Additional items were dropped because of translation problems as well as distinct differences in the significance of some information types between the cultures (e.g., the DRIVER'S LICENSE NUMBER, as the driver's license is not used as ID equivalent in Germany).

The final list consists of 32 information types identical to Markos et al.'s study to allow for comparability. 10 information types were dropped and 8 were newly included. The list of data types is displayed in Fig. 2 in Section 5.1.

3.2. The questionnaire

The survey was implemented on the platform SurveyMonkey and consisted of three parts. First, demographic characteristics (age, gender, and educational level) were assessed. In the second part, the participants evaluated the sensitivity of 40 information types. The participants were asked "How sensitive are the following data types to you?" and rated the

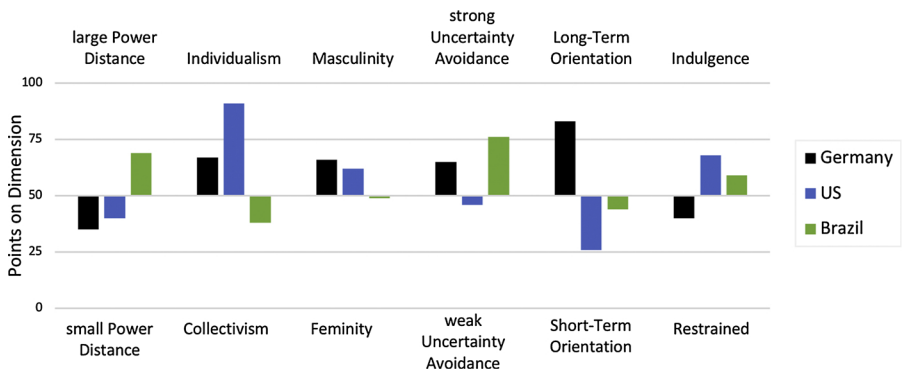

Fig. 1. Cultural characteristics in comparison between Germany, US, and Brazil with the 6-D model by Hofstede (data taken from Hofstede, Hofstede, & Minkov, 2010).

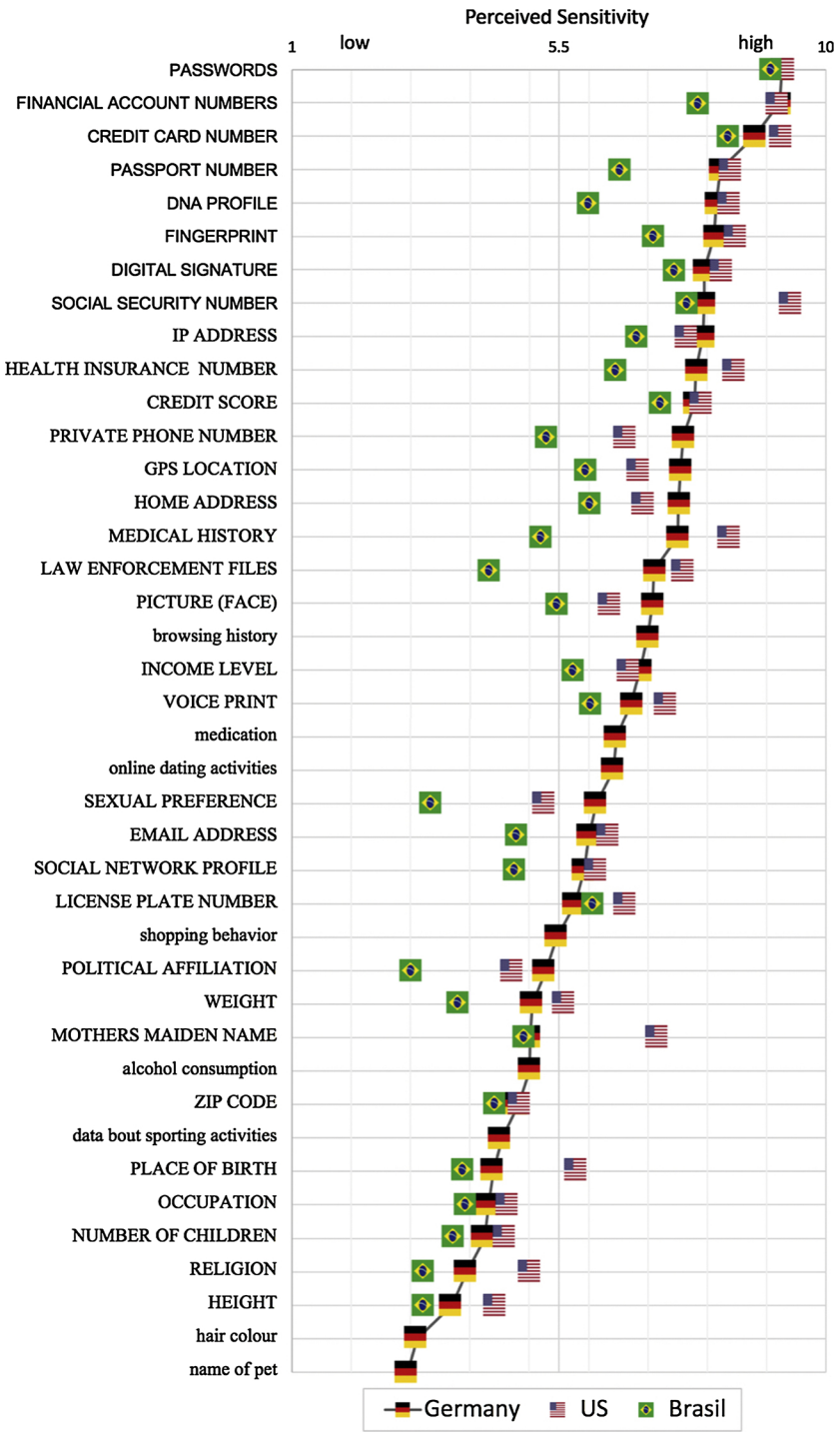

Fig. 2. Perceived sensitivity of all 40 data types of information in comparison between the nations (capitalized information types were also used in the study by Markos et al. (2017).

sensitivity on a 6-point symmetric scale from "not sensitive at all" (1) to "very sensitive" (6). We used a 6-point scale to avoid overtaxing the participants and their discrimination abilities (cf., Lozano, García-Cueto, ö Muñiz, 2008). For comparison purposes we transformed our scale to fit the 10-point scale used by Markos et al. (2017). The order of the data types presented was randomized to prevent sequence effects.

The third part of the questionnaire determined the participants' privacy disposition (based on Xu et al., 2008), experiences with privacy violations (based on Zeissig, Lidynia, Vervier, Gadeib, ö Ziefle, 2017), and risk propensity (based on Rohrmann, 1997). The items are listed in Table 1. All items were assessed on a 6-point Likert scale ranging from 1 "I do not agree at all" to 6 "I fully agree". Additionally, trust in institutions (e.g., government agencies, insurance companies, etc.) was evaluated on an 6-point answering scale from 1 "I don't trust them at all" to 6 "I fully trust them".

For reliability analysis, Cronbach's Alpha was calculated. The scale *experiences with privacy violations* missed adequate reliability ($\alpha < .7$) and was excluded from further analysis.

Table 1
Items and reliability of the constructs using Cronbach's α (N = 592).

Disposition to Value Privacy (Xu et al., 2008), α = .80
Compared to others, I am more sensitive about the way online companies handle my personal information. To me, it is the most important thing to keep my online privacy. Compared to others, I tend to be more concerned about threats to my personal privacy.
Risk Propensity (Rohrmann, 1997), α = .71
I'm quite cautious when I make plans and when I act on them.* I follow the motto, „nothing ventured, nothing gained". I've not much sympathy for adventurous decisions.* I like to put something at stake.
Privacy Violation Experience (Zeissig et al., 2017), α = .68
I have had bad experiences with regard to my online privacy before. I experienced misuse of data from friends or family. I have not yet made bad experiences with the misuse of my data.*
Trust in Institutions, α = .82
To what degree do you trust the following institutions to reliably handle data? government agencies, research, TÜV (Technical Inspection Association), insurance companies, medium-sized companies, start-ups, online companies

* Reverse-phrased items.

3.3. Statistical analysis

Comparison between our German results and those of Markos et al. (2017) are descriptive. The ranking of the data types is compared using rank-order correlation. Instead of using the ranks for the calculation, the mean sensitivity was input as rank to contribute for the different lists. To group data types based on their perceived sensitivity, a hierarchical cluster analysis is conducted. In order to examine the influence of user factors on the perception of sensitivity, regression analyses are calculated (method: enter). The level of significance was set at 5% for all analyses.

4. The sample

The questionnaire was distributed online via an independent market research company in order to reach a census representative sample of German internet users. 601 participants in an age range of 18–69 years of age completed the questionnaire in February 2018. Nine response sets were excluded due to contradictory answering patterns, leaving 592 individual data sets for the here reported analyses. The sample shows heterogeneous distributions regarding age (M = 38.7, SD = 20.15), gender (59.1% women), and education level (21.1% university degree) (cf. Table 2).

The participants report on average to value their privacy (privacy disposition: M = 4.25, SD = 0.98) and to be rather risk averse (risk propensity: M = 3.13, SD = .87). Experiences with online privacy violations vary but on average the sample is rather neutral (M = 3.26, SD = 1.13). Trust in institutions varies also depending on the institutions: most participants trust government agencies (M = 4.28, SD = 1.26), research (M = 4.1, SD = 1.1), TÜV (Technical Inspection Association, a widespread, private auditing and certification body) (M = 4.08, SD = 1.06), insurance companies (M = 3.94, SD = 1.2), and medium-sized companies (M = 3.64, SD = 0.97). In contrast, most participants do not trust start-ups (M = 3.13, SD = 1.0) and online companies (M = 2.83, SD = 1.23). On average, the trust index for the whole sample is neutral with a slight positive trusting tendency (M = 3.72, SD = 0.87).

Table 2
Demographic characteristics of the sample (N = 592).

Age [years]	mean (SD)	38.7 (20.15)
	15-19	25.2%
	20-29	25.3%
	30-59	24.8%
	< 60	24.7%
Gender	women	59.1%
	men	40.9%
Education level	no certificate	7.1%
	certificate of secondary education	7.6%
	general certificate of secondary education	18.4%
	apprenticeship	19.3%
	general qualification for university entrance	26.5%
	university degree	21.1%

5. Results

In this section, we will first present the descriptive results of perceived information sensitivity in Germany and the comparison to Brazil and the US (referring to the outcomes reported by Markos et al. (2017)). Second, factors of data types are extracted that are related in their perceived sensitivity. Furthermore, demographic characteristics as well as privacy perceptions are analyzed for their influence on perceived sensitivity.

5.1. Descriptive results on information sensitivity in Germany and comparison to brazilian and US samples

The average sensitivity ratings for each data type are displayed in Fig. 2, sorted descending from the most sensitive data. From a German perspective, PASSWORDS represented the most sensitive data type with a very high perceived sensitivity (M = 9.26) followed closely by FINANCIAL ACCOUNT DATA (M = 9.22). Least sensitive were HAIR COLOR (M = 3.11) and NAME OF PET (M = 2.96). 14 data types were perceived as (rather) not sensitive, whereas the remaining 26 were perceived as (rather) sensitive.

In comparison between the nations, the data types were perceived more sensitive by the US sample (M = 6.95) than the German sample (M = 6.68) and much less sensitive by the Brazilian sample (M = 5.55). The rank orders for sensitivity were similar between Germany and USA (r = .91) and Germany and Brazil (r = .87). This fits with the results of Markos et al. (2017) in which the rank order of Brazil and USA is quite similar (r = .89). Germans perceived especially private phone number, gps location, home address, picture, sexual preferences, and political affiliation as much more sensitive than both Brazilians and US Americans. On the other hand, the LICENSE PLATE NUMBER was seen as less sensitive by Germans than by the two American samples. Regarding the high sensitivity of PASSWORDS, the three samples agreed.

Some differences to the American sample stand out. In the US, the SOCIAL SECURITY NUMBER was perceived as the most sensitive type of information (M = 9.40), whereas Germans ranked it as eighth most important (M = 7.94). Also, Germans perceived the MOTHER'S MAIDEN NAME as rather non-sensitive (M = 5.02), which has a higher sensitivity in the US (M = 7.17). PRIVATE PHONE NUMBER (M_{Ger} = 7.6; M_{US} = 6.6), SEXUAL PREFERENCE (M_{Ger} = 6.14; M_{US} = 5.29), as well as a PICTURE showing ones face (M_{Ger} = 7.08; M_{US} = 6.35) were more sensitive for Germans than for Americans.

Compared to the Brazilian sample, Germans evaluated many data types to be much more sensitive, especially the DNA profile, law enforcement files, picture, sexual preference, political affiliation.

5.2. Clusteranalysis: data categories

Similar to Markos et al. (2017), we conducted a cluster analysis on the sensitivity of the data types resulting in a three cluster solution of *highly, medium*, and *less sensitive data* categories (cf. Table 3). Comparing our solution to the three cluster solution of high, medium, and low privacy segments by Markos et al. (2017), we see only one difference regarding the *high sensitivity data* category: CREDIT SCORE was

Table 3
Identified clusters of *highly, medium,* and *less sensitive data* categories in the German sample.

Highly sensitive data	Medium sensitive data	Less sensitive data
PASSWORDS	CREDIT SCORE*	EMAIL ADDRESS
FINANCIAL ACCOUNT NO.	PRIVATE PHONE NO.	SOCIAL NETWORK PROFILE*
CREDIT CARD	GPS LOCATION	LICENSE PLATE NO.*
PASSPORT NO.	HOME ADDRESS	shopping behavior
DNA PROFILE	MEDICAL HISTORY	POLITICAL AFFILIATION
FINGERPRINT	LAW ENFORCEMENT FILES	WEIGHT
DIGITALSIGNATURE	PICTURE (FACE)	MOTHER'S MAIDEN NAME*
SOCIAL SECURITY NO.	browsing history	alcohol consumption
IP ADDRESS	INCOME LEVEL	ZIP CODE
HEALTH INSURANCE	VOICE PRINT	data about sporting activities
IDENTITIY NO.	medication	PLACE OF BIRTH
	online dating activities	OCCUPATION
	SEXUAL PREFERENCE*	NUMBER OF CHILDREN
		RELIGION
		HEIGHT
		hair color
		name of pet

*Differences in classification to that of Markos et al. (2017).

Table 4
Mean perceived sensitivity across countries (1 = low, 10 = high information sensitivity).

	Germany	U.S.	Brazil
All Information Types	6.68	6.95	5.55
Highly Sensitive Information	8.24	8.66	7.32
Medium Sensitive Information	7.06	7	5.45
Less Sensitive Information	4.68	5.5	4.16

clustered as *medium sensitive* in our German data set whereas it belonged to the high privacy segment in the mixed Brazilian and US sample. Other differences regarding the cluster solutions are in line with the above described differences in perceived sensitivity: SEXUAL PREFERENCES were a *medium sensitive data* type for Germans, but LICENSE PLATE NUMBER, MOTHER'S MAIDEN NAME, and SOCIAL NETWORK PROFILES were ranked into the *low sensitive data* category. In Markos et al. (2017), it was the other way around.

In Table 4, the mean perceived sensitivity of all data types and the three clusters are contrasted across nations to cast light on the differences in intercultural evaluations. Where Germans showed a slightly lower mean sensitivity regarding all data types than the US, they perceived medium sensitive information as slightly more sensitive, but less sensitive information almost 1 point less sensitive. The Brazilians reported to perceive all information as less sensitive and even the medium sensitive information was evaluated as neutral in sensitivity (M = 5.45 being very close to the midpoint of the scale).

5.3. Influences on perceived sensitivity

Beyond the cross-national comparisons, we assessed different user factors to examine their influence on the individual perception of sensitivity. The results of regression regarding all data types as well as the data categories are reported in Table 5.

Privacy disposition showed a strong positive influence regarding all data types showing that individuals who value their privacy more also perceived most information to be more sensitive. Risk propensity showed an influence regarding all data types, which is, in more detail, only prevalent for the medium sensitive cluster. As could be expected, a higher risk propensity led to a lower perceived sensitivity. Interestingly, people who report a higher trust in institutions perceive highly sensitive data to be more sensitive, but trust index shows no effect on the other information clusters. Age showed a marginal impact on the perception of highly sensitive data, but also not for the other data types. A higher level of education leads to the sensitivity being perceived as higher for all but the less sensitive data. Gender cannot predict perceived sensitivity significantly. The individual variables under study explain only a small amount of variance ($.17 < R^2_{adj} < .26$).

6. Discussion

We empirically analyzed the sensitivity perceptions of German internet users and compared these to US American and Brazilian results from a recent study conducted by Markos et al. (2017). Our study thus represents a European picture in terms of information sensitivity perceptions, taking German internet users as an example. The findings showed both similarities and differences to US American and Brazilian perceptions in this regard. A cluster analysis was used to find categories of data that are similar in perceived sensitivity. Regression calculations were conducted to examine which user factors influence the perception of sensitivity on an individual level.

6.1. Perception of sensitivity: a German and a cross-national view

German internet users perceive passwords as most sensitive, followed by identifying data types such as financial account numbers, passport number, or fingerprint, confirming previous research that personally identifying information is most sensitive. Name of pet was on average the least sensitive despite it being used frequently as security question to access online accounts. Also, the mother's maiden name is perceived as neutral (close to the arithmetic neutral point), even though it is one information needed to open bank account and the like. This indicates that, either, these risks were not taken into consideration, or not only risks evaluation plays a role for the perception of sensitivity.

Table 5
Regression on perceived sensitivity using forced entry method in comparison between all data types and the data categories (N = 592).

	All Data		Highly Sensitive Data		Medium Sensitive Data		Less Sensitive Data	
	B	*Sig.*	B	*Sig.*	B	*Sig.*	B	*Sig.*
Intercept	2.01	*< .001*	3.06	*< .001*	2.27	*< .001*	1.31	*< .001*
Privacy Disposition	**0.41**	*< .001*	**0.35**	*< .001*	**0.46**	*< .001*	**.39**	*< .001*
Risk Propensity	**−0.07**	*.040.*	−0.07	*n.s.*	**−0.11**	*.012*	−0.05	*n.s.*
Trust Index	0.06	*n.s.*	**0.10**	*.028*	0.08	*n.s.*	0.02	*n.s.*
Age	−0.00	*n.s.*	**0.004**	*.045*	−0.00	*n.s.*	−0.00	*n.s.*
Gender	0.02	*n.s.*	−0.10	*n.s.*	−0.01	*n.s.*	0.09	*n.s.*
Education	**0.06**	*.003*	**0.08**	*< .001*	**0.07**	*.004*	0.04	*n.s.*
R^2_{adj}	.26		.18		.24		.17	

* Bold numbers depict significant results, n.s. = not significant ($p > .05$).

In the comparison to the US Americans and Brazilians, the average perceived sensitivity of Germans lies in between. The comparison of the mean sensitivity of the data segments that we identified in the cluster analysis illustrates that especially medium sensitive data is perceived as more sensitive by Germans than by US Americans, whereas Americans perceive highly sensitive and less sensitive data as more sensitive. In Brazil, all data segments are less sensitive.

The rank order of the perceived sensitivity of the data types was similar between all three countries despite the differences in absolute sensitivity rating. Markos et al. (2017) hypothesized that there is a global consensus on what constitutes sensitivity because of this similarity. Our study supports their hypothesis with cross-Atlantic data.

Germany, the US, and Brazil differ in many cultural values, but Markos et al. (2017) could show that not the cultural values but the nationality itself has the greatest impact on sensitivity perception and hypothesize that the data protection policy of the country plays an important role.

Germany has a rather strict and historically grown data protection legislation. Habituation to this circumstance and how people, companies, and institutions typically handle data in Germany could explain some of the national differences. To distinguish the effects of cultural values from the effects of legislation and policies, a comparison between the legislative, technical, and users' perspective on information sensitivity would be insightful. This could also uncover whether there are discrepancies in the nation-wide education of responsible internet behaviors and media usage.

Some distinct differences between the countries exits, that can be explained by national specificities. For example, in the US, the social security number is rated as most sensitive, as it is used often and can reveal much data about the person. Thus, it can be misused with severe consequences. In Germany, the social security number has a much lower importance and is correspondingly rated as less sensitive. These differences indicate that the risk evaluation is indeed essential to the perception of sensitivity.

But risk perceptions are prone to highly individual evaluations. In contrast to objectively calculated risks – a combination of the risk magnitude and risk probability – users base their risk perceptions, e.g., on past experience with adverse risk events, the perception of control and controllability, and the evaluation of the risk probability as well as coping resources (Renn, 1989). Moreover, optimism bias leads individuals to believe that they themselves are less vulnerable and less at risk than other people (Cho, Lee, ö Chung, 2010). Thus, humans' risk evaluations and decision making is characterized by affective heuristics (Slovic ö Peters, 2006) and bounded rationality (Acquisti ö Grossklags, 2005) and are subjective by nature.

At the same time, risk evaluation and perception of sensitivity are impacted by personality and individual characteristics. In a regression analysis, we could illustrate that privacy disposition strongly influences the perception of sensitivity. Thus, there are individuals who attach more value to their privacy and also perceive data as more sensitive compared to others. Higher risk propensity leads to a lower sensitivity perception of medium sensitive data. Furthermore, the education level could explain some individual differences. These results show that individual sensitivity perception is considerably influenced by personality, attitudes, and also demographic characteristics. Distinguishing different user types regarding their privacy attitudes as well as having a more detailed look at fringe groups in future research could help to understand users and their online behavior (see also Schomakers, Lidynia, Vervier, ö Ziefle, 2018; Smit, Van Noort, ö Voorveld, 2014).

6.2. Evaluation of the approach and the outcomes

From a social science perspective, the underlying question of studying privacy and information sensitivity perceptions is whether internet users might be able to gauge what happens with their data, which of the personal information is sensitive, and what harms could follow if data are not handled with care and responsibility. There exists a considerable body of research showing that users are quite mindless with their personal data when using the internet, even though they report to be very concerned about possible privacy intrusions by third parties (Gerber, Gerber, ö Volkamer, 2018). This heuristic and not necessarily conscious behavior – subsumed under the term privacy paradox (Norberg, Horne, ö Horne, 2007) – is not easy to resolve. Users' daily behaviors to share their data might be based on ignorance about the factual sensitivity of information and data types. Or, users might have a different understanding of dangers and a different perception of whether they are in control. In addition, users might opt to share data because the temporary reward is higher for them than the potential risks. In that sense, privacy decisions can be described as an individual weighing of risks and benefits – referred to as privacy calculus (Dinev ö Hart, 2006; Wang, Duong, ö Chen, 2016). In order to disentangle privacy behaviors on the internet, the different sources (e.g., context, sensitivity perception, privacy calculus) need to be addressed separately: In this research, we concentrated on the identification of the perceived sensitivity of information and data types in a first step. In order to receive a" pure" picture, no usage context was provided, resulting in a sensitivity cartography of data. Critically, one could ask whether context-free sensitivity perceptions exists and what it might signify. We know from previous empirical research – and also saw indications in our results – that risk evaluations are central to the perception of sensitivity (Milne et al., 2016).

But risk is hard to judge without knowing the context and the potential recipient of the information in question. On the other hand, this is also often the case when information is provided online or tracked by smart devices. The information that has once been stored can be misused in contexts that it was not meant for in the first place. Also, the information users voluntarily publish online for one context can be accessed and used in other contexts. Thus, our context-free approach to sensitivity can be the right approach in order to examine online privacy perceptions.

6.3. Limitations and future research lines

So far, the sensitivity perceptions reported in this paper are restricted to context-free evaluation of different data types. To validate the findings, the next steps will aim to explore information sensitivity in different (critical) usage contexts (e.g., health services, work environments, or mobility) to estimate the contextual impact. Also, the participants' prior emotional state or the recent framing of a situation could contribute to systematic variance within the data. To control emotional states, an emotional stimulus could be used before the empirical assessment of perceived sensitivity and privacy perceptions as it was used by Kehr, Kowatsch, Wentzel, and Fleisch, (2015).

Another issue this study faced is the language transition. For example, the original study surveyed license plate number and vehicle registration number, both of which translate into the same in German. Even though we cannot exclude some inaccuracies due to language transitions, the overall findings seem to be stable due to the large sample size and the international cross-validation.

The comparison to the Brazilian and US American sensitivity perceptions gathered by Markos et al. (2017) could only be done descriptively. Thus, we cannot determine whether the reported differences are statistically significant and how strong the effects are. The relatively large samples sizes of both studies support the hypothesis that differences in means are statistically significant, but this has not been verified yet.

To date, the picture about information sensitivity includes three Western countries on different continents. However, information about sensitivity perceptions in Asia, Africa, and Oceania is needed to further test the idea of a global consensus as hypothesized by Markos et al. (2017). One might speculate that countries with a different markedness in the cultural values "Individualism", "Uncertainty Avoidance", or

"Indulgence" show also a different perception of sensitivity (Li, Kobsa, Knijnenburg, ö Nguyen, 2017; Trepte et al., 2017). Also, countries with altogether different political systems, or even just varying degrees of democratic co-determination, could also show different perceptions of information sensitivity (Milberg, Burke, Smith, ö Kallman, 1995).

Due to the future demographic challenges, it is decisive to understand how age and generation impose special challenges to responsible internet behaviors. When looking at related work, the influence of the users' age on privacy attitudes and behaviors yielded a mixed picture. In this study, we did not find age effects in sensitivity perceptions, confirming the findings of Markos et al. (2017). One could speculate that adult internet users – due to longer experience and higher level of awareness due to the topic's frequent media exposure – have appropriate and sufficient knowledge about data sensitivity. Further study should include also children and younger teenagers as vulnerable internet and social media users with respect to their perceptions of information sensitivity. This might help to develop individually tailored educational formats that could be used in school and professional trainings to establish a responsible and informed mindset of technology appropriate behaviors that adheres to the claims within the concept of digital citizenship (Ribble, Bailey, ö Ross, 2004).

7. Conclusion

The perception of information sensitivity is central to privacy attitudes and behaviors in different usage contexts, e.g., information disclosure behavior in social media or online shops. In this study, a representative sample of German internet users evaluated the sensitivity of 40 different data types which results in an empirical cartography of perceived information sensitivity. Germans perceive information on average as less sensitive than do US Americans but more sensitive than Brazilians (cf., Markos et al., 2017). Nevertheless, the ranking of data based on sensitivity is similar across nations, indicating that there is a consensus on what constitutes sensitivity across nations. Still, there are some distinct differences between the evaluations of the nationalities that may be explained by cultural differences and habits and the corresponding variance in the risks of disclosing the information types in the respective country. Also, the privacy disposition, education level, and risk propensity influences the perception of sensitivity on an individual level, illustrating the user diversity in privacy perceptions. The findings contribute to an understanding of how to design information and communication strategies to inform internet users how to manage their data carefully.

Declaration of interest

This research has been funded by the German Ministry of Education and Research (Project MyneData, no. KIS1DSD045).

Acknowledgements

The authors thank all participants for sharing their personal opinions. Thanks also to Stefan Ahlers for research support. This research has been funded by the German Ministry of Education and Research (BMBF) under project MyneData (KIS1DSD045).

References

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy, 3*(1), 26–33.

AlAlwan, A., Rana, N. P., Dwivedi, Y. K., & Algharabat, R. (2017). Social media in marketing: A review and analysis of the existing literature. *Telematics and Informatics, 34*(7), 1177–1190.

Asplund, M., & Nadjm-Tehrani, S. (2016). Attitudes and perceptions of IOT security in critical societal services. *IEEE Access, 4*, 2130–2138.

Bansal, G., Zahedi, F. M., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems, 49*, 138–150.

Bergström, A. (2015). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior, 53*, 419–426.

Blank, G., Bolsover, G., & Dubois, E. (2014). *A new privacy paradox: Young people and privacy on social network sites.* Global Cyber Security Capacity Centre: Draft Working Paper.

Burgoon, J. K. (1982). Privacy and communication. *Annals of the International Communication Association, 6*(1), 206–249.

Cho, H., Lee, J.-S. S., & Chung, S. (2010). Optimistic Bias About Online Privacy Risks: Testing the Moderating Effects of Perceived Controllability and Prior Experience. *Computers in Human Behavior, 26*(5), 987–995.

Dinev, T., & Hart, P. (2006). An extended privacy Calculus model for E-Commerce transactions. *Information Systems Research, 17*(1), 61–80.

European Commission (2015). *Data protection eurobarometer (Tech. Rep.)*. European Commission.

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security, 77*(August), 226–261.

Hofstede, G. (2011). Dimensionalizing Cultures: The Hofstede Model in Context. *Online Readings in Psychology and Culture, 2*(1), 1–26.

Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). *Cultures and organizations - software of the mind. Intercultural cooperation and its importance for survival* (third edition ed.). New York: McGraw-Hill.

Hoofnagle, C., King, J., Li, S., & Turow, J. (2010). *How different are young adults from older adults when it comes to information privacy attitudes and policies?* .

Hossain, M. A., & Dwivedi, Y. K. (2014). What improves citizens' privacy perceptions toward RFID technology? A cross-country investigation using mixed method approach. *International Journal of Information Management, 34*(6), 711–719.

Jones, S., Johnson-Yale, C., Millermaier, S., & Perez, F. S. (2009). Everyday life online: U.S. College students' use of the internet. *First Monday, 14*(10).

Kapoor, K. K., Tamilmani, K., Rana, N. P., Patil, P., Dwivedi, Y. K., & Nerur, S. (2018). Advances in social media research: Past, present and future. *Information Systems Frontiers, 20*(3), 531–558.

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal, 25*(6).

Kirs, P., & Bagchi, K. (2012). The impact of trust and changes in trust: A national comparison of individual adoptions of information and communication technologies and related phenomenon. *International Journal of Information Management, 32*(5), 431–441.

Koops, B.-j., Newell, B. C., Timan, T., Skorvanek, I., Chokrevski, T., & Galic, M. (2017). A typology of privacy. *University of Pennsylvania Journal of International Law, 38*(2), 1–93.

Krasnova, H., & Veltri, N. F. (2010). *Privacy calculus on social networking sites: Explorative evidence from Germany and USA. Proceedings of the Annual Hawaii International Conference on System Sciences*1–10.

Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and privacy calculus on social networking sites: The role of culture. *Business & Information Systems Engineering, 4*(3), 127–135.

Li, Y. (2011a). *Developing a dichotomy of information privacy concerns. 17th Americas Conference on Information Systems (AMCIS 2011)*1–8.

Li, Y. (2011b). Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communications of the Association for Information Systems, 28*(28), 453–496.

Li, Y., Kobsa, A., Knijnenburg, B. P., & Nguyen, C. (2017). Cross-cultural privacy prediction. *Proceedings on Privacy Enhancing Technologies, 2*, 1–20.

Lozano, L. M., García-Cueto, E., & Muñiz, J. (2008). Effect of the number of response categories on the reliability and validity of rating scales. *Methodology, 4*(2), 73–79.

Malheiros, M., Preibusch, S., & Sasse, M. A. (2013). "Fairly truthful": the impact of perceived effort, fairness, relevance, and sensitivity on personal data disclosure. *LNCS, 7904*, 250–266.

Markos, E., Milne, G. R., & Peltier, J. W. (2017). Information sensitivity and willingness to provide continua: A comparative privacy study of the United States and Brazil. *Journal of Public Policy & Marketing, 36*(1), 79–96.

McKnight, D. H., & Chervany, N. L. (2000). *What is trust? A conceptual analysis and an interdisciplinary model. Proceedings on Americas Conference on Information Systems AMIS*827–833.

Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. (1995). Values, personal information privacy, and regulatory approaches. *Communications of the ACM, 38*(December (12)), 65–74.

Milne, G. R., Pettinico, G., Hajjat, F. M., & Markos, E. (2016). Information sensitivity typology: Mapping the degree and type of risk consumers perceive in personal data sharing. *The Journal of Consumer Affairs,* 1–29.

Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: A qualitative study in seven european countries. *European Journal of Information Systems, 2317*(2), 103–125.

Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., & Wang, S. (2012). Disclosure antecedents in an online service context: The role of sensitivity of information. *Journal of Service Research, 15*(1), 76–98.

Nambiar, R., Bhardwaj, R., Sethi, A., & Vargheese, R. (2013). *A look at challenges and opportunities of big data analytics in healthcare. IEEE International Conference on Big Data*17–22.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox : Personal Information Disclosure Intentions versus Behaviors. *The Journal of Consumer Affairs, 41*(1), 100–126.

Potoglou, D., Dunkerley, F., Patil, S., & Robinson, N. (2017). Public preferences for

internet surveillance, data retention and privacy enhancing services: Evidence from a pan-european study. *Computers in Human Behavior, 75*(June), 811–825.
Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013). *Anonymity, privacy, and security online (Tech. Rep.)*. Pew Research Center.
Renn, O. (1989). *risk perception and risk management. 14th Congress of the World Energy Conference*.
Ribble, M. S., Bailey, G. D., & Ross, T. W. (2004). Digital citizenship: Addressing appropriate technology behavior. *Learning & Leading with Technology, 32*(1), 6.
Rohm, A. J., & Milne, G. R. (2004). Just what the doctor ordered the role of information sensitivity and trust in reducing medical information privacy concern. *Journal of Business Research, 57*, 1000–1011.
Rohrmann, B. (1997). *Risk orientation questionnaire: Attitudes towards risk decisions.* Melbourne, Australia: University of Melbourne.
Sagiroglu, S., & Sinanc, D. (2013). *Big data: A review. International Conference on Collaboration Technologies and Systems (CTS)*42–47.
Schomakers, E.-M., Lidynia, C., Vervier, L., & Ziefle, M. (2018). Of guardians, cynics, and pragmatists a typology of privacy concerns and behavior. *3rd International Conference on Internet of Things, Big Data and Security*.
Shiau, W.-L., Dwivedi, Y. K., & Yang, H.-S. (2017). Co-citation and cluster analyses of extant literature on social networks. *International Journal of Information Management, 37*(5), 390–399.
Slovic, P., & Peters, E. (2006). Risk perception and affect. *Current Directions in Psychological Science, 15*(6), 322–325.
Smit, E. G., Van Noort, G., & Voorveld, H. A. M. (2014). Understanding online behavioral advertising: User knowledge, privacy concerns and online coping behavior in Europe. *Computers in Human Behavior, 32*, 15–22.
Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989–1015.
Trepte, S., Reinecke, L., Ellison, N. B., Quiring, O., Yao, M. Z., & Ziegele, M. (2017). A cross-cultural perspective on the privacy Calculus. *Social Media + Society, 3*(1), 1–13.
UM London, & eMarketer (2018). Smartphone user penetration as percentage of total population in Western Europe from 2011 to 2018. *Statista - The Statistics Portal*.
Valdez, A. C., & Ziefle, M. (2018). The users perspective on the privacy-utility trade-offs in health recommender systems. *International Journal of Human-computer Studies*.
Van den Broeck, E., Poels, K., & Walrave, M. (2015). Older and Wiser? Facebook use, privacy concern, and privacy protection in the life stages of emerging, Young, and middle adulthood. *Social Media + Society, 1*(2).
Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management, 36*(4), 531–542.
Westin, A. F. (1967). Privacy and freedom. *American Sociological Review, 33*(1), 173.
Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). *Examining the formation of individual's privacy concerns: Toward an integrative view. International Conference on Information Systems*.
Zeissig, E.-M., Lidynia, C., Vervier, L., Gadeib, A., & Ziefle, M. (2017). Online privacy perceptions of older adults. In J. Zhou, & G. Salvendy (Eds.). *International Conference on human aspects of IT for the aged population, LNCS 10298* (pp. 181–200). .
Ziefle, M., & Calero Valdez, A. (2018). Decisions about medical data disclosure in the internet: An age perspective. In J. Zhou, & G. Salvendy (Eds.). *International Conference on human aspects of IT for the aged population, LNCS 10927* (pp. 186–201). .