IRDG Institut für das Recht der digitalen Gesellschaft

UNIVERSITY OF PASSAU Faculty of Law

UNIVERSITY OF PASSAU IRDG RESEARCH PAPER SERIES NO. 22-02

THE CULTURAL CONTEXT OF PERSONAL DATA DISCLOSURE DECISIONS

Daniela Wawra

February 2022

Place of Publication

University of Passau IRDG
c/o Chair of German and European Private Law, Civil Procedure, and Legal Theory
Innstraße 39
94032 Passau

https://www.jura.uni-passau.de/irdg/

Abstract

This paper introduces the research design of the interdisciplinary project *Vectors of data disclosure – A comparative study of the use of personal data from a legal, cultural studies, and information systems perspective*[1], funded by the Bavarian Research Institute for Digital Transformation[2], from a cultural studies point of view. Based on a literature review, factors that can influence people's willingness to share (WTS) personal data are identified and discussed. Subsequently, a research framework is developed that approaches the narrower cultural context of data disclosure decisions. It aims to provide insights into people's mentalities regarding data sharing on a macro level and thus into the cultural preconditions of information governance.

Cite as

Wawra, D. (2022). The Cultural Context of Personal Data Disclosure Decisions. *University of Passau Institute for Law of the Digital Society Research Paper Series No. 22-02.* https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/.

Keywords

Culture, Data Disclosure, Digitalization, Privacy, Willingness to Share (WTS) Data.

---

[1] Lead principal investigator: Moritz Hennemann; further principal investigators: Kai von Lewinski, Daniela Wawra, and Thomas Widjaja; external advisor: Urs Gasser. The author wants to thank her colleagues for their useful comments when preparing this article.

[2] https://www.bidt.digital/ (last access: 11/24/2021).

Contents

I. Introduction: The Research Project

"Data is one of the main drivers of innovation in the 21st century. But at the same time, the constantly evolving possibilities for data processing keep bringing about novel threat scenarios. This has prompted us to investigate – in a concerted approach – the underlying personal decision-making processes, cultural influences and legal protection mechanisms."[3] Against this background, the overarching goals of our interdisciplinary project on data disclosure are

(1) to uncover cultural and regulatory influences on people's decisions about whether and how to disclose personal data and

(2) to integrate these findings into a model of the personal data disclosure process.

We have selected the following eight countries for our study: Brazil, China, Germany, Ghana, Japan, Russia, Switzerland, and the United States. These countries represent a variety of legal systems and cultural contexts that make it possible to identify culture-specific and cross-cultural trends that can affect people's willingness to share (WTS) data. These aspects are considered to be particularly relevant in transnational contexts of data disclosure, in which we are interested in our project as well.

In what follows, first of all a literature review will give an overview of the research field, before we extract parameters for the investigation of the cultural preconditions of information governance for our project.

II. Influences on Data Disclosure Decisions: The Research Context

Buchwald et al. (2017) define the self-disclosure of data as "the action of uncovering personal information, such as locations or activities." Communication privacy management theory (CPM) states that, prior to disclosing, "people face a conflict between privacy and disclosure while determining whether to reveal private data and information or not" (Buchwald et al. 2017). In the context of our project, informational privacy can be defined "as the claim of an individual to determine what information about himself or herself should be known to others" (Westin 2003, p. 431) and as the demand to be protected from unwanted access to personal data (Rössler 2001, p. 25). This includes "when such information will be obtained and what uses will be made of it by others. […] When a privacy claim is recognized in law or social convention, we can speak of 'privacy rights'" (Westin 2003).

Various (meta) studies in the context of privacy, data protection and data disclosure in different settings – often in online environments pertaining to the use of online services and social network sites (SNSs) – so far have identified and investigated a number of variables that (potentially) can have an influence on an individual's data disclosure decision. Bauer, Schiffinger (2015) for example describe the "scope of the investigated variables" as "tremendous" and list as examples, by no means exhaustively, what can be categorized as personality traits (e.g. anxiety) (cf. also e.g. Robinson 2018, Zhang et al. 2021), socio-demographic factors like age (cf. e.g. Anaraky et al. 2021), gender and education (cf. e.g. Trepte, Masur 2017, Herbert et al. 2020), as well as benefits (e.g. rewards), trust, anonymity and system design. What has sometimes been summarized as contextual factors has become more and more the focus of research (cf. e.g. Anderson, Agarwal 2011, Yun et al. 2019, p. 571, Ackermann et al. 2021), and these are what we are mostly interested in in the cultural part of our project.

[3] Moritz Hennemann in an interview with Katrina Jordan (2021) for the Digital Research Magazine of the University of Passau.

1. Privacy Concerns, Risks and Benefits of Data Disclosure

Variables that have featured prominently in this line of research on data disclosure are, first of all, privacy concerns as well as benefits and risks associated with data disclosure. This focus can be traced back to social exchange theory that "postulates that users' willingness to disclose personal information is based on their assessments of the costs, risks, and benefits" (Bauer, Schiffinger 2015). Privacy concerns can be described as comprising "individuals' beliefs about the risks and potential negative consequences associated with sharing information" (Baruh et al. 2017, p. 27). They have frequently been shown to correlate negatively with the willingness to share data (cf. e.g. Son, Kim 2008, Krasnova et al. 2010, Baruh et al. 2017, Gerber et al. 2018, Okazaki et al. 2020, Tang, Wang 2021). However, this effect "is unstable across contexts" (Grosso et al. 2020). This can be attributed to the fact that privacy concerns have often been constructed as a rather generic, stable and enduring concept (cf. Smith et al. 1996, Malhotra et al. 2004, Ackermann et al. 2021). Westin's Privacy Segmentation Index (cf. Westin 1991, Kumaraguru, Cranor 2005), for example, clusters consumers in "Fundamentalists," "Pragmatics," and "Unconcerned." Fundamentalists are described as not trusting organizations with regard to their personal data, being concerned about the use of their data and appreciating new data regulation legislation. To be able to control their privacy is more important to them than possible benefits of data disclosure. Pragmatics calculate the benefits versus the risks of sharing their personal data, take companies' efforts to protect their data into account, by which they can gain consumers' trust, and they like to be able to choose if they disclose data or not. The Unconcerned trust organizations with their personal data, they do not mind to disclose their data for benefits and do not have a positive attitude towards new data regulation legislation. This segmentation is based on a survey that was conducted in the United States. According to this approach, people are expected to fit into one of these categories, and their (intended) data disclosure behavior is supposed to be predictable based on their categorization. However, "[p]revious research has failed to establish a robust correlation" in this respect (Woodruff et al. 2014, p. 1, cf. also Consolvo et al. 2005, King, Hoofnagle 2008, Malheiros et al. 2013), and the index has been criticized, among other things, for assuming that people (always) make data disclosure decisions based on highly informed and rational deliberations and that the described general attitudes lead to corresponding disclosure behavior independent of the specific context (cf. Woodruff et al. 2014, p. 1). However, privacy concerns and a general interest in privacy issues do not always translate into privacy protection measures and/or the retention of data in concrete disclosure situations: This is known as the privacy paradox (cf. Norberg et al. 2007). Particularly on the internet, "many users show theoretical interest in their privacy and maintain a positive attitude towards privacy-protection behavior, […] [however,] this rarely translates into actual protective behavior" (Barth, de Jong 2017; cf. also Pötzsch 2009, Joinson et al. 2010). In addition, individuals may indicate that they intend to limit their sharing of personal data, but "actual disclosure often significantly exceeds intention" (Barth, de Jong 2017; cf. also Norberg et al. 2007). It has thus to be taken into account that individuals' assessment in concrete data disclosure scenarios can vary, and that their WTS personal data is not solely guided by general, stable privacy concerns. While privacy concerns have been conceived as "an individual variable remaining generally stable across contexts, decisions to disclose information are highly contextual – they are shaped by the informational norms deemed appropriate within the given context" (Grosso et al. 2020, cf. also Martin 2020). Grosso et al. (2020) deduce "that the relationship between PCs [privacy concerns] and WSPI [the willingness to share personal information] is more complex than a simple negative one, and that it can only be better understood by investigating the information flow's context in detail."

Furthermore, "[…] the context delimits the contours of the analysis within which the information flow's appropriateness is assessed. This appropriateness assessment depends on the discloser's perception of the informational norms […]. These norms can be explicitly expressed in rules or laws, or they can be implicitly embodied in 'conventional' behaviors" (Grosso et al. 2020). Theoretically, this follows Nissenbaum's (2004, 2010, 2011, see also Martin, Nissenbaum 2016, Nissenbaum 2018) concept of privacy as contextual integrity, which has been suggested as a 'solution' to the privacy paradox. From this conceptualization of privacy follows an important distinction: There is a difference between "'giving up' privacy and giving up information" (Grosso et al. 2020, cf. Martin, Nissenbaum 2016). This means that individuals sometimes do not have the feeling that they concede parts of their privacy when they disclose data about themselves, as this sharing of information seems appropriate to them in a certain context. Consequently, privacy can generally be attributed a high value and privacy concerns can be high, while, at the same time, individuals do not hesitate to share personal data in a specific disclosure context nevertheless (cf. Palmatier, Martin 2019, Grosso 2020). If we apply the concept of privacy as contextual integrity to our research topic, privacy concerns as an individual variable can be attributed a negative impact on people's WTS data. However, it can be assumed that they vary in their manifestation and, depending on the concrete context, may not play a role at all. The concept of privacy concerns has been further developed into the privacy calculus (cf. Dinev, Hart 2006), which takes into account a second factor that can influence data disclosure decisions: It does not solely focus on the risks that individuals associate with data disclosure but considers the benefits as well. It is therefore seen as a more adequate concept to explain why people disclose or withhold data (cf. Ackermann et al. 2021). Privacy benefits have sometimes been categorized into "financial rewards (e.g. Hann et al., 2007; Hui et al., 2006; Xu et al., 2009), personalization benefits (Chellappa, Sin, 2005; White, 2004) and social adjustment benefits (Lu et al., 2004)" (Buchwald et al. 2017). Social adjustment benefits can be defined as "the establishment of social identity by integrating into desired social groups" (Lu et al. 2004, p. 572). They allow individuals to "fulfil their need for affiliation" (Buchwald et al. 2017). Benefits of data sharing can outweigh the risks and lead to disclosure despite an individual's privacy concerns (cf. e.g. Barth, de Jong 2017). Other authors, however, attribute greater influence to the perceived risks than to the perceived benefits as an explanatory factor of data disclosure decisions (cf. Keith et al. 2013, Buchwald et al. 2017). Again, these different results could be due to the different situational contexts in which the data disclosure decisions took place.

2. Online Privacy Literacy

A further explanation for the privacy paradox that has been postulated and frequently researched in relation to data disclosure is online privacy literacy. In this line of reasoning, the privacy paradox has been explained by users' not yet having experienced privacy violations, which may make them underestimate privacy risks and cause a lax handling of their data (cf. Baruh et al. 2017, p. 29, cf. also Dienlin, Trepte 2015). Online privacy literacy usually comprises declarative as well as procedural knowledge: Declarative knowledge consists of what an individual knows about the risks they expose themselves to and about the rights they have when they consider the disclosure of personal data. Procedural knowledge relates to individuals' skills to protect their data (cf. Baruh et al. 2017, p. 29, see also Trepte et al. 2015). Baruh et al. (2017) establish a significant association between privacy concern and privacy literacy: "Users with higher privacy literacy reported higher concern for privacy" (Baruh et al. 2017, p. 39). In line with this, other studies have shown that low awareness of privacy issues is connected to lower risk perception and an increased willingness to share personal data (cf. e.g. Cheng et al. 2021, Zhang et al. 2021). Users with privacy concerns were also "more likely to utilize privacy protective measures"

(Baruh et al. 2017, p. 26). Other research, however, has established a negative correlation between privacy literacy and privacy concerns, arguing that more literate users are better in protecting their privacy by taking appropriate measures and will therefore have less concerns about their privacy (cf. Turow, Hennessy 2007, Baruh et al. 2017). Opposite research outcomes might not least be due to the fact that the parameter 'online privacy literacy' comprises quite different aspects, which its subcategorization into declarative and procedural knowledge already indicates. There are not many studies so far which differentiate between the two and allow for well-founded conclusions with regard to their respective impact on data disclosure. Thus, Baruh et al. (2017, p. 47) "recommend the inclusion of measures that can differentiate between these two types of literacies" in future studies. The concept of online privacy literacy can even be segmented into more than these two components. Masur (2020, p. 260) has suggested

"an extended model of online privacy literacy which includes three basic dimensions: 1) factual privacy knowledge, 2) privacy-related reflection ability, and 3) privacy and data protection skills, and theorizes an overarching dimension called critical privacy literacy."

Masur (2020) thus adds a reflective competence to the declarative and procedural knowledge about privacy protection.

3. Type of Data

Apart from privacy literacy, privacy concerns, risks and benefits associated with data sharing, the type of data has also proven to be of major relevance for people's disclosure decisions: As a general tendency, it can be stated that the more sensitive specific data (e.g. financial and health data) are perceived by individuals, the greater people's privacy concerns and the more they hesitate to share them (cf. e.g. Roeber et al. 2015, Buchwald et al. 2017, Milne et al. 2017, Lim et al. 2018, Marwick, Hargittai 2019, Mazurek, Małagocka 2019, Okazaki et al. 2020, Ackermann et al. 2021, Anaraky et al. 2021). In their study that combines the potential influence of the variables industry sector, type of requested data, intended use of data, type of compensation for shared data, and granting of anonymity on data disclosure decisions, Ackermann et al. (2021) discovered that

"[t]he more sensitive a particular type of data is perceived, the less impact do other factors have on corresponding WTS-decisions. In other words, consumers will be very unlikely to share private data that they perceive as very sensitive, irrespective of what type of compensation they are offered in return or the degree of anonymity that is granted to them."

At the same time, when data are

"not perceived as very sensitive, other factors, such as what compensation is offered and whether the data allow for personal identification, for instance, will likely have a considerable impact on individual decisions to share these data" (Ackermann et al. 2021)

Ackermann et al. (2021) furthermore conclude that data disclosure is more likely when there is a "match between the core business a company is engaged in and the type of data that is requested."

4. Data Control

Perceived control over the use of personal data has been identified as yet another influence on privacy concerns: The more control people assume to have over the use of their data, the less accentuated their privacy concerns are and the more likely data disclosure becomes, even if the personal data are perceived as sensitive (cf. e.g. Brandimarte et al. 2013, Phelps et al. 2000, Ackermann et al. 2021). Control over data can be enhanced by giving people the option to delete their data should they no longer feel comfortable with their disclosure (cf. e.g. Roeber et al. 2015) and by using anonymized data, i.e. data that cannot be linked to an individual (cf. e.g. Hoffmann et al. 1999, Ackermann et al. 2021). Ackermann et al. (2021) even identified the granting

of anonymity as "the most effective single factor for evoking WTS."

5. Attitudes Towards Data Receiver

Research findings are relatively consistent that attitudes towards potential data receivers also influence people's willingness to disclose data considerably: Trust in a data receiver has a positive influence on the willingness to share data (cf. e.g. Mazurek, Małagocka 2019, Grosso et al. 2020, Okazaki et al. 2020, Anaraky et al. 2021, Urbonavicius et al. 2021). Grosso et al. (2020) differentiate between trust in a company and its personnel on a "micro-level, and trust in a country at the macro-level." The latter is shown to have an indirect positive impact on trust on the micro-level, which has a positive effect on the WTS personal data.

6. Communication

Moreover, transparency in data receivers' communication on the use of collected personal data has been identified as an influential factor that can enhance people's willingness to disclose personal data (cf. e.g. Mazurek, Małagocka 2019). Certain communication strategies, like e.g. message framing, i.e. accentuating the positive (gain frame) or negative consequences (loss frame) of data disclosure, have also been identified as positive or negative influences on people's WTS data (cf. e.g. White et al. 2011, Zhang et al. 2021).

7. Internet Penetration

Furthermore, internet penetration has been investigated as a potential significant factor in relation to data disclosure (cf. e.g. Liang et al. 2017). It depended on the type of data, however, whether there was a positive or negative correlation: "Users in societies with higher penetration rate were more likely to keep their accounts public and less likely to disclose geolocation in tweets" (Liang et al. 2017, p. 1489). Further studies are needed to investigate a possible link between the degree of digitalization in a society and people's WTS data.

8. Cultural Dimensions

Studies have also explored possible links between general value orientations prevalent in national cultures and people's WTS personal data. They have mostly used Hofstede's (2001, 2019, 2022) cultural dimensions and investigated different disclosure scenarios (cf. e.g. Milberg et al. 2000, Bellman et al. 2004, Yun et al. 2014, Liang et al. 2017, Trepte et al. 2017, Baruh et al. 2017, Li et al. 2017, Okazaki et al. 2020). Most of the research has been done on Hofstede's traditional four dimensions: individualism/collectivism, uncertainty avoidance, power distance and masculinity, but the later added dimensions indulgence/restraint as well as long term versus short term normative orientation (also known as (short-term) normative versus (long-term) pragmatic or Monumentalism versus Flexhumility) have also been researched. We exclude such general cultural dimensions for now. They can characterize the general, broader cultural context, but we are first and foremost interested in the narrower cultural context of data disclosure in particular. After we have captured the latter, relations with the former can also be explored.

9. Data Disclosure as a Multifactorial and Context-Dependent Process

The literature review shows that it has become more and more evident that data disclosure decisions can be influenced by multiple factors, which interact and can work with different force in different directions, like vectors (cf. von Lewinski 2014), promoting or impeding the WTS data. Privacy concerns are often constructed as a central parameter of data disclosure decisions. Other variables (expected risks and benefits, online privacy literacy, data control, data sensitivity, trust in data receiver) are then conceptualized as influential factors that intensify or decrease privacy concerns, which, finally, enhance or reduce the WTS: Thus, as a general tendency, the greater the perceived risks, the more pronounced the privacy concerns, and the greater the perceived benefits, the less pronounced the privacy concerns. In addition, online privacy literacy has

been described as increasing or decreasing privacy concerns. A context-independent direction of its effect on the WTS data can therefore not be determined. Increased data sensitivity, in contrast, has been shown to usually lead to more privacy concerns. Perceived data control (including anonymity) has been associated with less privacy concerns as has trust in the data receiver. It has also to be considered, however, that privacy concerns do not occur in every data disclosure situation. In addition, it has to be kept in mind that personality traits and socio-demographic factors can also have an influence on individuals' inclinations to share data (see above, cf. e.g. Ghose et al. 2022, Zimaitis et al. 2020, Zhang et al. 2021).

The studies cited clearly lead to the conclusion that the concrete situational context affects the interplay and intensity of the individual variables that can influence data disclosure decisions. This is in line with Nissenbaum's (2004, 2010, 2011, see also Martin, Nissenbaum 2016) concept of privacy as contextual integrity as well as CPM theory (see above). However, at the same time, it is possible to extract for most of the individual variables the general direction of their impact on the WTS data (and independently of privacy concerns), i.e. positive (enhancing the WTS) or negative (reducing the WTS) (see above).

Finally, it has to be taken into consideration that the traditional model of the process of data disclosure decisions, the privacy calculus, "assumes that consumers weigh potential risks against benefits when deciding to share their personal data" (Ackermann et al. 2021), i.e. it is usually implied

"that consumers make a conscious, deliberate decision. However, it seems plausible that consumers, facing high complexity, often do not have sufficient time and mental resources to collect all relevant information and make trade-offs between their need for privacy and other goals" (Ackermann et al. 2021, cf. also Kim et al. 2015).

Ackermann et al. (2021) therefore advocate a focus "on the role of contextual factors," as this

"can reveal heuristic strategies that consumers apply when deciding whether to share personal information. For instance, it has been shown that perceptions and decisions are strongly affected by the context or the situation when people are in a heuristic mode of decision-making" (Ackermann et al. 2021, cf. also John et al. 2009).

Consequently, we understand the process of data disclosure decisions to be a conscious or unconscious, more or less extensive negotiation of usually more than one of the aforementioned (and potentially more) variables that is context-dependent.

III. A Comparative Macro Perspective on Data Disclosure: The Research Approach

The context of data disclosure can be approached from a macro (societal, national), meso (institutional) and micro (individual) perspective: "Micro is individual choice, and macro is its aggregate consequences" (Dopfer et al. 2004, p. 264).

"In the macro domain we abstract from […] detail in order to focus upon the aggregate consequences – this is a quasi-statistical exercise that is not connected to the micro domain in an analytical sense even though it is possible to, for example, sum micro value added to obtain macro value added in an *ex post* statistical sense" (Dopfer et al., p. 267).

We will start with a macro perspective in the cultural part of our research project by looking at the narrower cultural context of data disclosure at country level. We will structure our overview of the cultural preconditions that can shape data disclosure decisions along central parameters (see IV. 2.) that are based on the previous discussion of the research context (see II.), particularly on the factors that can influence the WTS data elaborated above. Most studies that investigate the willingness to

disclose data are limited to one country. Significantly fewer studies engage in country comparisons and, when they do, they typically compare only two or, more rarely, several more countries. Therefore, as Okazaki et al. (2020) state: "More research is needed to measure the effects of customer privacy concerns in different regions." Our next research step will therefore be a cultural comparison of the results of our macro study, that, as far as possible, includes all our eight study countries, provided comparable data can be obtained. Therefore, the approach to our topic on the macro level can further be described as a "[c]omparison across structural units (e.g., nations […])", which "will result in the aggregation of individual and contextual data" (Masur et al. 2021, p. 12). Masur et al. (2021, p. 12) attribute such an approach a value in its "own right, given the inherent tension between global information infrastructures and localized user experiences." We agree with Masur et al. (2021, p. 5)

"that any attempt at classifying societal settings is inherently limited and oversimplifying. Nonetheless, […] differentiating cultural, social, political, economic, and technological structures provides a fruitful framework for explaining similarities, differences, or inconsistencies in privacy-related outcomes" (Masur et al. 2021, p. 5).

At this stage of our project, the interplay of the parameters is not yet the focus of our research. This will have to be analyzed in concrete data disclosure scenarios in studies on the micro level.

IV. The Cultural Context of Data Disclosure

1. Introduction

In our project, we aim to provide insights into the data protection norms that apply in different countries, people's attitudes towards and views on issues related to data disclosure decisions as well as their behavior in specific data disclosure situations. Culture-specific and cross-cultural aspects will be identified and detailed. Our research program is grounded in a "*derived etics*" approach (Berry 1989, Barmeyer 2018, p. 132). Applied to our research topic, we assume that we can identify certain parameters that have an influence on data disclosure processes cross-culturally. These etic parameters (see also Barmeyer 2018, p. 127), however, are expected to show culture-specific – i.e. emic – variation. In order to proceed on this assumption, we follow a cultural comparative empirical approach (cf. e.g. Barmeyer 2012, p. 113-114): By comparing respective data that have been collected in eight different countries, we work towards better understanding common and different assessments of data disclosure issues in different cultures.

Culture, however, is an "elusive construct" that is "complex, variable, and difficult to define" (Jackson 2020, p. 28). Of the many and diverse definitions of culture[4], we want to highlight the following: According to the Globe (2020) project, which has in common with our project that it works with survey data from different countries, "culture typically refers to a set of parameters of collectives that differentiate each collective in a meaningful way, with a focus on the 'sharedness' of cultural indicators among members of the collective." They go on to define culture as "[s]hared motives, values, beliefs, identities, and interpretations or meanings of significant events that result from common experiences of members of collectives that are transmitted across generations" (Globe 2020). This reflects the view that culture tends to be rather stable and permanent and that it is based on generational transmission. Other definitions of culture do not include such a diachronic aspect. Berrell (2021)[5] for example

[4] For a systematic overview of different approaches to culture see e.g. Straub (2007) and Jackson (2020, p. 26-50).

[5] Berrell (2021) claims that these "norms (…) and values" are "shared by the population of a sovereign nation." We do not agree with this, as it is never the whole population of a country that shares the same "norms

conceptualizes culture as consisting of "the norms, behaviors, beliefs, customs, […] values" that are expressed by a collective. Others add or focus on further components of culture, among others, "assumptions", "attitudes" and "expectations" "that people have in common with others in a community" (Guzman 2009). These componential approaches to culture can be applied to all sorts of collectives, be they small or large. The 'components' that shape a culture are basically not static but dynamic and can be more or less stable. Norms in the form of laws, for example, are often more enduring than attitudes or behaviors in specific situations. Besides, cultures regularly develop in exchange with other cultures (which can range from sub- to transnational cultures) (cf. e.g. Jackson 2020, p. 45-46). In line with Markos et al. (2017), we argue that "[a] comprehensive understanding of privacy issues [– and data disclosure is such an issue –] must be viewed not only in terms of information sensitivity but also as a function of entrenched beliefs grounded in social and cultural contexts." Consequently, "a person's privacy perceptions and willingness to disclose should be viewed as the convergence of personal preferences, social interactions, and cultural orientation" (Markos et al. 2017).

2. Cultural Preconditions of Information Governance: The Research Parameters

Based on the previous discussions, especially the literature review (see II.), and based on larger global but also national surveys on issues related to data disclosure (e.g. CIGI-Ipsos 2019a, b, c, Cisco 2021, EVS/WVS 2021a, b, c, IMD 2021, Ipsos 2019, Markos et al. 2017, Trepte, Masur 2016) we have established our research parameters. They provide insights into a particular cultural segment, i.e. in the "assumptions", "attitudes", "expectations" (Guzman 2009), "norms, behaviors, beliefs, customs, […] [and] values" (Berrell 2021) that can influence people's WTS personal data. The following figure gives an overview of the parameters that we focus on in the first part of our project:

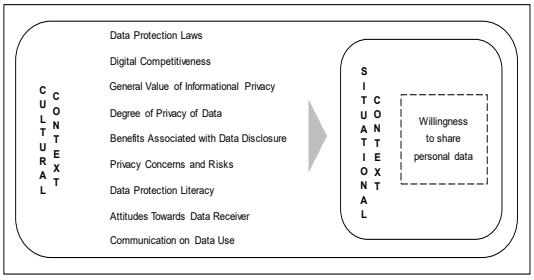

Fig. 1. Central parameters of data disclosure

On the left, the parameters are displayed that can influence people's WTS data. They constitute the narrower cultural context of data disclosure decisions. This list of research parameters proceeds from more fundamental to more specific parameters of data disclosure. It is to be expected that (at least some of) these parameters are valued differently in different cultures. The norms that apply to data disclosure processes, i.e. mainly data protection laws, constitute our first research parameter. It will be elaborated in the legal part of the project. Further central components of the cultural context are captured by the other research parameters (see figure 1). The goal in the first phase of the cultural part of our project is to identify the cultural preconditions for information governance. Consequently, we start out by looking at the individual parameters of data disclosure to identify general cultural tendencies for each. In what follows, the parameters are briefly defined and, as far as possible, characterized in terms of the general direction of their individual influence – positive (enhancing) or negative (reducing) – on the WTS data. The characterizations are based on the literature review above (see II.). It has to be emphasized that what follows constitutes an aggregated, macro level perspective on each parameter (see III.), i.e. we abstract from concrete data disclosure scenarios, and the following evaluations are always based on

(…) and values." It is rather all the "norms (…) and values" that exist in a country that shape its national culture, which is always diverse. We can, however, identify majority trends.

the theoretical assumption that people expect a violation of their privacy when they consider data disclosure. We also neglect the interplay of the parameters in concrete data disclosure scenarios. In these, i.e. depending on the situational context, the force of each individual parameter can vary, and thus its impact on the data disclosure decision, but the general direction of the influence of the individual parameter on the WTS personal data remains the same, unless indicated otherwise in what follows (see also II. and III.).

The parameter following *Data Protection Laws* is ***Digital Competitiveness***. It is understood in the sense of the "IMD World Digital Competitiveness Ranking" (WDCR), a well-established and widely accepted regularly published ranking, as the "capacity of economies to use digital technologies to transform themselves" (IMD 2021, p. 3). The WDCR "analyzes and ranks the extent to which countries adopt and explore digital technologies leading to transformation in government practices, business models and society in general" (IMD 2021, p. 32). We start with this parameter as we assume that this is a very fundamental factor that can influence data disclosure decisions. The reasoning here is that the degree of digitalization of a culture might well have an impact on whether people are more or less inclined to share personal data: For example, if they are more accustomed to disclosing data, and if there are more privacy protection measures in place, this could influence their WTS data positively. On an aggregate, macro level, the direction of the impact of this parameter (and its individual components) has not yet been determined and needs to be explored further. If we consider the results of the study on internet penetration cited above (see II. 7.), it is possible that the impact of this parameter depends in particular on the specific type of data requested.

The parameter ***General Value of Informational Privacy*** indicates how important or unimportant informational privacy is considered to be in a culture. Informational privacy is understood "as the claim of an individual to determine what information about himself or herself should be known to others" (Westin 2003, p. 431) and as the demand to be protected from unwanted access to personal data (Rössler 2001, p. 25) (see II.). It is assumed that the more value people generally place on their informational privacy, the more cautious they will tend to be when asked to disclose personal data.

The parameter ***Degree of Privacy of Data*** or data sensitivity surveys how private or sensitive individuals consider certain kinds of personal data to be, like, e.g., financial and health data. The more sensitive certain data are perceived to be, the more reluctant people will be to share them.

The parameter ***Benefits Associated with Data Disclosure*** renders the positive effects people expect from the disclosure of their personal data. Based on the literature review (see II. 1.), the benefits have mainly been divided into three categories so far: (1) social adjustment benefits, (2) financial rewards, and (3) personalization benefits. One would generally expect that a perceived benefit of data disclosure will increase the WTS data. It might, however, vary, what an individual perceives as a benefit.

The parameter ***Privacy Concerns and Risks*** comprises the negative effects people associate with data disclosure. These include their general concerns about the security of their personal data, and their control over them. Here, the basic assumption is that the impact of privacy concerns and perceived risks on the WTS data is negative, i.e. people are less willing to disclose personal data.

The parameter ***Data Protection Literacy*** captures people's awareness and knowledge of data protection, privacy rules and policies as well as the skills they report to have, and the measures they take to protect their personal data. Based on the literature review (see II. 2.), it is unclear whether this parameter, which is closely related to but somewhat more narrowly defined than the variable online privacy

literacy, can be attributed a general effect on the WTS data. More research that differentiates between at least declarative and procedural knowledge is needed.

The parameter ***Attitudes Towards Data Receiver*** refers to people's attitudes towards institutions to which they disclose their data. These comprise above all their trust in national and foreign governments and (different kinds of) companies pertaining to the protection and correct use of their data. It is generally to be expected that the more people trust a data receiver, the more willing they are to share personal data.

The parameter ***Communication on Data Use*** or transparency relates to the importance people attribute to communication on how their personal data are used. If transparent communication of data use is important to somebody, their WTS data is expected to increase if the communication fulfills their expectations.

Based on the literature review (see II. 3. and 4.), the degree of privacy or sensitivity that is assigned to data and also the granting of anonymity (as a means to improve people's perceived control over their data and thereby reducing their privacy concerns) stand out as the factors that have been attributed the most impact on people's WTS personal data so far.

The sketches of the parameters sum up each one's individual potential effect on people's WTS data from a macro perspective. Their multi-dimension combinations (cf. von Lewinski, p. 6) and highly complex interaction mechanisms need to be analyzed in concrete situational contexts (see II. 9.) on a micro level. Consequently, more of the contextual parameters should be integrated in empirical studies on data disclosure, because, so far, "research has often focused on one or two of conceivable contextual factors only, neglecting potential interactions between them" (Ackermann et al. 2021).

3. The Research Questions and Country Reports

In order to better understand the cultural context of data disclosure, basic research questions that we address on the macro level for each of our selected countries are the following:

- Which data protection legislation applies?
- How do data disclosure regimes (and data protection laws in general) of different countries interact? How can these legal systems be compared?[6]
- What is the degree of digitalization (how digitally competitive is the country)?
- Which fundamental value does informational privacy have?
- Are certain kinds of data considered to be more sensitive than others?
- Which benefits are associated with data disclosure?
- Which privacy concerns do people have when they are asked to disclose personal data? Which risks do they see?
- How literate are people in data protection, i.e. what do they know about data protection legislation and possibilities to protect their personal data (declarative knowledge)? How do they assess their practical skills to protect their data (procedural knowledge)?
- Are individuals more willing to share personal data with specific data receivers such as national or foreign

[6] These questions will be addressed in the legal part of our project, which is supervised by Kai von Lewinski and Moritz Hennemann, who also formulated these legal research questions.

governments and different kinds of companies (mainly based on trust)?

- Which influence does communication have on people's willingness to share personal data? Are people more willing to disclose data if data recipients are transparent about what they will do with the data?

In the initial phase of our project, these and other related questions are first fundamentally examined for the individual countries we have selected. In order to obtain as broad an empirical data base as possible, we first compile country reports that focus on the results of large-scale surveys. As we are planning a cultural comparative study as a next research step, we have given preference to global surveys to facilitate this endeavor. The country reports are structured along the parameters introduced above (see figure 1). The parameter *data protection laws* is detailed in separate legal country reports. The information relating to people's WTS personal data in the respective country of investigation is extracted from the surveys and summarized. The individual country reports thus capture the views, assessments, assumptions, attitudes, evaluations and reported behaviors that prevail among citizens with regard to data disclosure. This gives us an important insight into the cultural mentality on our topic and thus into the narrower cultural context of data disclosure and thereby into the cultural preconditions for information governance. It allows us to identify culture-specific and cross-cultural trends with regard to influences on people's WTS data. The knowledge we gain from the survey-based country reports is statistical in nature and reflects the aggregate views of respondents (see III.). On the basis of this macro approach (see III.) and the conception of culture elaborated above (see IV. 1.), it has to be emphasized for all our research parameters – with the exception of data protection laws – that, while the results of our analysis are based on a broad data set, they show nothing more and nothing less than trends that can be more or less stable and representative for different societal groups. All data should therefore be collected and compared diachronically regularly to see how stable they are and to identify possible significant changes. We integrate differentiations according to socio-demographic factors (such as age, education, ethnicity, gender, income, political orientation, rural or urban neighborhood) in the German and the US report. In these countries, the data basis is broader and more differentiated than in the other countries we studied and is therefore most suitable for this endeavor. This is not least to show the extent to which there is also intracultural variation that can influence data disclosure decisions (cf. e.g. DeSilver 2013, Madden 2015, 2017, Trepte, Masur 2017, Auxier et al. 2019, Auxier 2020, Herbert et al. 2020). More studies are needed to examine within-country variations in more detail, particularly in other cultures than Germany and the US (see also II. and IV.).

V. Outlook

The legal and cultural country reports can serve as a source of information for researchers and practitioners alike for whom data disclosure issues are relevant. They should be considered in particular by legislature and stakeholders who receive personal data, such as governments, companies, and (non-profit) organizations. They are also particularly relevant in transnational contexts of data disclosure.

Within the framework of our interdisciplinary project, the legal and cultural country reports are furthermore pre-studies for subsequent comparative studies of our countries of investigation. The cultural reports provide a window into people's mentalities in relation to data disclosure issues in the selected countries and thus capture the narrower cultural context in which data disclosure decisions are embedded. They also reveal survey gaps in the countries that we study: Ghana and Switzerland, for example, have not been part of the large, global CIGI-Ipsos (2019a, b, c) and Ipsos (2019) studies at all, and some relevant topics

(e.g. the impact of anonymity) have not yet been included in these surveys either. These remain research desiderata for the future.

VI. References

Ackermann, K. A., Burkhalter, L., Mildenberger, T., Frey, M., and Bearth, A. (2021). Willingness to Share Data: Contextual Determinants of Consumers' Decisions to Share Private Data with Companies. Journal of Consumer Behaviour 2021. 1-12. DOI: 10.1002/cb.2012 (last access: 02/07/2022).

Anaraky, R. G., Byrne, K. A., Wisniewski, P. J., Page, X., and Knijnenburg, B. (2021). To Disclose or Not to Disclose: Examining the Privacy Decision-Making Processes of Older vs. Younger Adults. CHI '21: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. 1-14. DOI: 10.1145/3411764.3445204 (last access: 02/07/2022).

Anderson, C., Agarwal, R. (2011). The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information. Information Systems Research 22(3). 469-490. DOI: 10.1287/isre.1100.0335 (last access: 02/09/2022).

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., and Turner, E. (2019). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. Pew Research Center. November 15. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (last access: 12/21/2021).

Auxier, B. (2020). How Americans See Digital Privacy Issues Amid the COVID-19 Outbreak. Pew Research Center. May 4. https://www.pewresearch.org/fact-tank/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/ (last access: 12/21/2021).

Barmeyer, C. (2012). Taschenlexikon Interkulturalität. Göttingen: Vandenhoeck & Ruprecht.

Barmeyer, C. (2018). Konstruktives Interkulturelles Management. Göttingen: Vandenhoeck & Ruprecht.

Barth, S., de Jong, M. D. T. (2017). The Privacy Paradox – Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review. Telematics and Informatics 34(7). 1038-1058. DOI: 10.1016/j.tele.2017.04.013 (last access: 02/07/2022).

Baruh, L., Secinti, E., and Cemalcilar, Z. (2017). Online Privacy Concerns and Privacy Management: A Meta-Analytical Review: Privacy Concerns Meta-Analysis. Journal of Communication 67(1). 26-53. DOI: 10.1111/jcom.12276 (last access: 02/07/2022).

Bauer, C., Schiffinger, M. (2015). Self-Disclosure in Online Interaction: A Meta-analysis. 2015 48th Hawaii International Conference on System Sciences. 3621-3630. DOI: 10.1109/HICSS.2015.435 (last access: 02/07/2022).

Beke, F., Eggers, F., and Verhoef, P. (2018). Consumer Informational Privacy: Current Knowledge and Research Directions. Foundations and Trends in Marketing 11(1). 1-71. DOI: 10.1561/1700000057 (last access: 02/09/2022).

Bellman, S., Johnson, E., Kobrin, S., and Lohse, G. (2004). International Differences in Information Privacy Concerns: A Global Survey of Consumers. https://www8.gsb.columbia.edu/sites/decision-sciences/files/files/1172.pdf (last access: 02/09/2022).

Berrell, M. (2021). National Culture and the Social Relations of Anywhere Working. https://www.igi-global.com/chapter/national-culture-and-the-social-relations-of-

anywhere-working/263827 (last access: 10/14/2021).

Berry, J. (1989). Imposed Etics-Emics-Derived Emics: The Operationalization of a Compelling Idea. International Journal of Psychology 24(6). 721-735.

Brandimarte, L., Acquisti, A., and Loewenstein, G. (2013). Misplaced Confidences: Privacy and the Control Paradox. Social Psychological and Personality Science 4(3). 340-347. DOI: 10.1177/1948550612455931 (last access: 01/28/2022).

Buchwald, A., Letner, A., Urbach, N., and von Entreß-Fürsteneck, M. (2017). Towards Explaining the Willingness to Disclose Personal Self-Tracking Data to Service Providers. 2017 Twenty-Fifth European Conference on Information Systems (ECIS). 1-11. https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/682/wi-682.pdf (last access: 02/07/2022).

Chellappa, R., Sin, R.G. (2005). Personalization Versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. Information Technology and Management 6. 181-202. DOI: 10.1007/s10799-005-5879-y (last access: 01/27/2022).

Cheng, X., Hou, T., and Mou, J. (2021). Investigating Perceived Risks and Benefits of Information Privacy Disclosure in IT-Enabled Ride-Sharing. Information & Management 58(6). 104350. DOI: 10.1016/j.im.2021.103450 (last access: 01/27/2022).

CIGI-Ipsos (2019a). CIGI-Ipsos Global Survey on Internet Security and Trust. Parts I & II: Internet Security, Online Privacy & Trust. Centre for International Governance Innovation. www.cigionline.org/internet-survey-2019 (last access: 12/15/2021).

CIGI-Ipsos (2019b). CIGI-Ipsos Global Survey Internet Security & Trust. Part 6: Cross-Border Data Flows. Centre for International Governance Innovation. www.cigionline.org/internet-survey-2019 (last access: 12/15/2021).

CIGI-Ipsos (2019c). CIGI-Ipsos Global Survey on Internet Security & Trust. Detailed Results Tables. www.cigionline.org/internet-survey-2019 (last access: 12/15/2021).

Cisco (2021). Consumer Privacy Survey. Building Consumer Confidence Through Transparency and Control. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf (last access: 12/03/2021).

Consolvo, S., Smith, I., Matthews, T., LaMarca, A., Tabert, J., and Powledge, P. (2005). Location Disclosure to Social Relations: Why, When, & What People Want to Share. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. 81-90. https://dl.acm.org/doi/10.1145/1054972.1054985 (last access: 02/17/2022).

DeSilver, D. (2013). Young Americans and Privacy. It's Complicated. Pew Research Center. June 20. http://www.pewresearch.org/fact-tank/2013/06/20/young-americans-and-privacy-its-complicated (last access: 12/21/2021).

Dienlin, T., Trepte, S. (2015). Is the Privacy Paradox a Relic of the Past? An In-Depth Analysis of Privacy Attitudes and Privacy Behaviors. European Journal of Social Psychology 45(3). 285-297. DOI: 10.1002/ejsp.2049 (last access: 01/28/2022).

Dinev, T., Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. Information Systems Research 17(1). 61-80. DOI: 10.1287/isre.1060.0080 (last access: 01/28/2022).

Dopfer, K., Foster, J., and Potts, J. (2004). Micro-Meso-Macro. Journal of Evolutionary Economics 14(3). 263-279. https://www.researchgate.net/publication/24058011_Micro-Meso-Macro (last access: 02/08/2022).

EVS/WVS (2021a). World Values Survey Wave 7 (2017-2020). Questionnaire: WVS-7 Master Questionnaire 2017-2020. https://www.worldvaluessurvey.org/WVSDocumentationWV7.jsp (last access: 12/15/2021).

EVS/WVS (2021b). European Values Study and World Values Survey: Joint EVS/WVS 2017-2021 Dataset (Joint EVS/WVS). JD Systems Institute & WVSA. Dataset Version 1.1.0. https://www.worldvaluessurvey.org/WVSEVSjoint2017.jsp (last access: 12/15/2021).

EVS/WVS (2021c). European Values Study and World Values Survey: Joint EVS/WVS 2017-2020 Data-Set (version 2.0.0). Documentation: Frequency Tables. WVS/EVS Joint v2.0 Results by Country. https://www.worldvaluessurvey.org/WVSDocumentationWV7.jsp (last access: 12/15/2021).

Gerber, N., Gerber, P., and Volkamer, M. (2018). Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior. Computers & Security 77. 226-261. DOI: 10.1016/j.cose.2018.04.002 (last access: 02/07/2022).

Ghose, A., Li, B., Macha, M., Sun, C., and Foutz, N. (2022). Trading Privacy for Public Good: How Did America React During COVID-19? NYU Stern School of Business. DOI: 10.2139/ssrn.3624069 (last access: 02/09/2022).

Globe (2020). An Overview of the 2004 Study: Understanding the Relationship Between National Culture, Societal Effectiveness and Desirable Leadership Attributes. https://globeproject.com/study_2004_2007#theory (last access: 12/15/2021).

Grosso, M., Castaldo, S., Li, H. A., and Larivière, B. (2020). What Information Do Shoppers Share? The Effect of Personnel-, Retailer-, and Country-Trust on Willingness to Share Information. Journal of Retailing 96(4). 524-547. DOI: 10.1016/j.jretai.2020.08.002 (last access: 02/07/2022).

Guzman, I. (2009). Occupational Culture and Socialization in IS. In: Encyclopedia of Human Resources Information Systems: Challenges in e-HRM. https://www.igi-global.com/chapter/occupational-culture-socialization/13296 (last access: 11/06/2021).

Hann, I.-H., Hui, K.-L., Lee, S.-Y., and Png, I. (2007). Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach. Journal of Management Information Systems 24(2). 13-42. DOI: 10.2753/MIS0742-1222240202 (last access: 01/28/2022).

Herbert, F., Schmidbauer-Wolf, G., and Reuter, C. (2020). Differences in IT Security Behavior and Knowledge of Private Users in Germany. https://library.gito.de/wp-content/uploads/2021/08/V3_Herbert-Differences_in_IT_Security_Behavior_and_Knowledge-541_c.pdf (last access: 02/07/2022).

Hoffmann, D., Novak, T., and Peralta, M. (1999). Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web. The Information Society 15(2). 129-139. DOI: 10.1080/019722499128583 (last access: 01/28/2022).

Hofstede, G. (2001). Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations Across Nations. 2nd Edition, Thousand Oaks CA: Sage Publications.

Hofstede, G. (2019). The 6-D Model of National Culture. http://geerthofstede.com/culture-geert-hofstede-gert-jan-hofstede/6d-model-of-national-culture/ (last access: 11/05/2021).

Hofstede, G. (2022). The Dimensions of National Culture. https://hi.hofstede-insights.com/national-culture (last access: 02/11/2022).

Hui, K.-L., Tan, B. C., and Goh, C.-Y. (2006). Online Information Disclosure: Motivators and Measurements. ACM Transactions on Internet Technology 6(4). 415-441. DOI: 10.1145/1183463.1183467 (last access: 01/28/2022).

IMD (2021). IMD World Digital Competitiveness Ranking 2021. https://www.imd.org/centers/world-competitiveness-center/rankings/world-digital-competitiveness/ (last access: 12/15/2021).

Ipsos (2019). Global Citizens & Data Privacy: An Ipsos-World Economic Forum Project. https://www.ipsos.com/sites/default/files/ct/news/documents/2019-01/ipsos-wef_-_global_consumer_views_on_data_privacy_-_2019-01-25-final.pptx_lecture_seule_0.pdf?mod=article_inline (last access: 12/15/2021).

Jackson, J. (2020) (2nd edition). Introducing Language and Intercultural Communication. London: Routledge.

Joinson, A., Reips, U.-D., Buchanan, T., and Schofield, C. B. P. (2010). Privacy, Trust, and Self-Disclosure Online. Human-Computer Interaction 25(1). 1-24. DOI: 10.1080/07370020903586662 (last access: 02/07/2022).

John, L. K., Acquisti, A., and Loewenstein, G. (2009). The Best of Strangers: Context Dependent Willingness to Divulge Personal Information (SSRN Scholarly Paper ID 1430482). Social Science Research Network. https://papers.ssrn.com/abstract=1430482 (last access: 02/04/2022).

Jordan, K. (2021). For What Reasons – and in What Ways – Do We Divulge Our Data? Bidt Funds Pioneering Interdisciplinary Project at the University of Passau. Digital Research Magazine. University of Passau. https://www.digital.uni-passau.de/en/stories/project-details/forschungsprojekt/warum-und-wie-wir-daten-preisgeben-bidt-fordert-zukunftsweisendes-interdisziplinares-projekt-an-der/?tx_converis_pi1%5Boverrideuid%5D=7085&cHash=ed69999c31ae46a6433d558532a2ac23 (last access: 11/19/2021).

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., and Greer, C. (2013). Information Disclosure on Mobile Devices: Re-Examining Privacy Calculus with Actual User Behavior. International Journal of Human-Computer Studies 71(12). 1163-1173. DOI: 10.1016/j.ijhcs.2013.08.016 (last access: 01/28/2022).

Kim, M., Ly, K., and Soman, D. (2015). A Behavioural Lens on Consumer Privacy. Behavioural Economics in Action Research Report Series. Toronto: Rotman School of Management, University of Toronto. https://inside.rotman.utoronto.ca/behaviouraleconomicsinaction/files/2013/09/ConsumerPrivacy-BEAR-2015-Final.pdf (last access: 02/07/2022).

King, J., Hoofnagle, C. (2008). A Supermajority of Californians Support Limits on Law Enforcement Access to Cell Phone Location Information. Social Science Research Network. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1137988 (last access: 02/16/2022).

Krasnova, H., Spiekermann, S., Koroleva, K., and Hildebrand, T. (2010). Online Social Networks: Why We Disclose. Journal of Information Technology 25(2). 109-125. DOI: 10.1057/jit.2010.6 (last access: 02/07/2022).

Kumaraguru, P., Cranor, L. F. (2005). Privacy Indexes: A Survey of Westin's Studies. https://www.cs.cmu.edu/~ponguru/CMU-ISRI-05-138.pdf (last access: 02/07/2022).

Li, Y., Kobsa, A., Knijnenburg, B. P., and Carolyn Nguyen, M.-H. (2017). Cross-Cultural Privacy Prediction. Proceedings on Privacy Enhancing Technologies 2017(2). 113-132. https://doi.org/10.1515/popets-2017-0019 (last access: 02/14/2022).

Liang, H., Shen, F., and Fu, K. (2017). Privacy Protection and Self-Disclosure Across Societies: A Study of Global Twitter Users. New Media and Society 19 (9). 1476-1497. DOI: 10.1177/1461444816642210 (last access: 01/28/2022).

Lim, S., Woo, J., Lee, J., and Huh, S.-Y. (2018). Consumer Valuation of Personal Information in the Age of Big Data. Journal of the Association for Information Science and Technology. 69(1). 60-71. https://doi.org/10.1002/asi.23915 (last access: 02/07/2022).

Lu, Y., Tan, B., and Hui, K.-L. (2004). Inducing Consumers to Disclose Personal Information to Internet Businesses with Social Adjustment Benefits. Proceedings of the Twenty-Fifth International Conference on Information Systems. Washington DC, USA. http://repository.ust.hk/ir/Record/1783.1-57524 (last access: 02/16/2022).

Madden, M. (2015). Privacy and Security Experiences of Low-Socioeconomic Status Populations. Data & Society Research Institute. https://datasociety.net/library/privacy-security-and-digital-inequality/ (last access: 12/21/2021).

Madden, M. (2017). Privacy, Security, and Digital Inequality. Data & Society. https://datasociety.net/library/privacy-security-and-digital-inequality/ (last access: 12/21/2021).

Malheiros, M., Preibusch, S., and Sasse, M. (2013). 'fairly truthful': The Impact of Perceived Effort, Fairness, Relevance, and Sensitivity on Personal Data Disclosure. In: Proceedings of the 6th International Conference on Trust & Trustworthy Computing (TRUST). 250-266. DOI: 10.1007/978-3-642-38908-5_19 (last access: 02/17/2022).

Malhotra, N. K., Kim, S. S., and Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. Information Systems Research 15(4). 336-355. http://www.jstor.org/stable/23015787 (last access: 02/07/2022).

Markos, E., Milne, G., and Peltier, J. (2017). Information Sensitivity and Willingness to Provide Continua: A Comparative Privacy Study of the United States and Brazil. https://doi.org/10.1509/jppm.15.159 (last access: 11/24/2021).

Martin, K., Nissenbaum, H. (2016). Measuring Privacy: An Empirical Test Using Context to Expose Confounding Variables. Columbia Science & Technology Law Review 18(1). 176-218. DOI: 10.2139/ssrn.2709584 (last access: 01/27/2022).

Martin, K. (2020). Breaking the Privacy Paradox: The Value of Privacy and Associated Duty of Firms. Business Ethics Quarterly 30(1). 65-96. DOI: 10.1017/beq.2019.24 (last access: 02/07/2022).

Marwick, A., Hargittai, E. (2019). Nothing to Hide, Nothing to Lose? Incentives and Disincentives to Sharing Information with Institutions Online. Information, Communication & Society 22(12). 1697-1713. DOI: 10.1080/1369118X.2018.1450432 (last access: 01/28/2022).

Masur, P. (2020). How Online Privacy Literacy Supports Self-Data Protection and Self-Determination in the Age of Information. Media and Communication 8(2). 258-269. https://doi.org/10.17645/mac.v8i2.2855 (last access: 02/14/2022).

Masur, P., Epstein, D., Quinn, K., Wilhelm, C., Baruh, L., and Lutz, C. (2021). A Comparative Privacy Research Framework. SocArXiv, 9 December. https://doi.org/10.31235/osf.io/fjqhs (last access: 01/31/2022).

Mazurek, G., Małagocka, K. (2019). What If You Ask and They Say Yes? Consumers' Willingness to Disclose Personal Data is Stronger Than You Think. Business Horizons 62(6). 751-759. DOI: 10.1016/j.bushor.2019.07.008 (last access: 02/05/2022).

Milberg, S., Smith, H., and Burke, S. (2000). Information Privacy: Corporate Management and National Regulation. Organization Science 11(1). 35-57. DOI: 10.1287/orsc.11.1.35.12567 (last access: 02/09/2022).

Milne, G., Pettinico, G., Hajjat, F., and Markos, E. (2017). Information Sensitivity Typology: Mapping the Degree and Type of Risk Consumers Perceive in Personal Data Sharing. Journal of Consumer Affairs 51(1). 113-161. DOI: 10.1111/joca.12111 (last access: 01/28/2022).

Nissenbaum, H. (2004). Privacy as Contextual Integrity. Washington Law Review 79(1). 119-157. https://heinonline.org/HOL/P?h=hein.journals/washlr79&i=129 (last access: 02/14/2022).

Nissenbaum, H. (2010). Privacy in Context: Technology, Policy, and the Integrity of Social Life. The Journal of Value Inquiry 45. 97-102. DOI: 10.1007/s10790-010-9251-z (last access: 01/27/2022).

Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. Daedalus 140(4). 32-48. DOI: 10.1162/DAED_a_00113 (last access: 01/27/2022).

Nissenbaum, H. (2018). Respecting Context to Protect Privacy: Why Meaning Matters. Science and Engineering Ethics 24(3). 831-852. DOI: 10.1007/s11948-015-9674-9 (last access: 02/07/2022).

Norberg, P. A., Horne, D. R., and Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. Journal of Consumer Affairs 41(1). 100-126. DOI: 10.1111/j.1745-6606.2006.00070.x (last access: 02/07/2022).

Okazaki, S., Eisend, M., Plangger, K., de Ruyter, K., and Grewal, D. (2020). Understanding the Strategic Consequences of Customer Privacy Concerns: A Meta-Analytic Review. Journal of Retailing 96(4). 458-473. DOI: 10.1016/j.jretai.2020.05.007 (last access: 02/07/2022).

Palmatier, R. W., Martin, K. D. (2019). The Intelligent Marketer's Guide to Data Privacy. The Impact of Big Data on Customer Trust. Palgrave Macmillan. DOI: 10.1007/978-3-030-03724-6 (last access: 02/07/2022).

Phelps, J., Nowak, G., and Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. Journal of Public Policy & Marketing 19(1). 27-41. DOI: 10.1509/jppm.19.1.27.16941 (last access: 01/28/2022).

Pötzsch, S. (2009). Privacy Awareness: A Means to Solve the Privacy Paradox? In: V. Matyáš, S. Fischer-Hübner, D. Cvrček, and P. Švenda (eds.). The Future of Identity in the Information Society 298. Berlin: Springer. 226-236. DOI: 10.1007/978-3-642-03315-5_17 (last access: 02/07/2022).

Robinson, S. (2018). Factors Predicting Attitude Toward Disclosing Personal Data Online. Journal of Organizational Computing and Electronic Commerce 28(3). 214-233. https://www.tandfonline.com/doi/pdf/10.1080/10919392.2018.1482601 (last access: 02/04/2022).

Roeber, B., Rehse, O., Knorrek, R., and Thomsen, B. (2015). Personal Data: How Context Shapes Consumers' Data Sharing with Organizations from Various Sectors. Electronic Markets 25(2). 95-108. DOI: 10.1007/s12525-015-0183-0 (last access: 01/28/2022).

Rössler, B. (2001). Der Wert des Privaten. Frankfurt am Main: Suhrkamp.

Smith, H. J., Milberg, S. J., and Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. MIS Quarterly 20(2). 167-196. DOI: 10.2307/249477 (last access: 02/07/2022).

Son, J.-Y., Kim, S. (2008). Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model. MIS

Quarterly 32(3). 503-529. DOI: 10.2307/25148854 (last access: 02/07/2022).

Straub, J. (2007). Kultur. In: Straub, Jürgen et. al. Handbuch Interkulturelle Kommunikation und Kompetenz. Stuttgart. 7-24.

Tang, Y., Wang, L. (2021). How Chinese Web Users Value Their Personal Information: An Empirical Study on WeChat Users. Psychology Research and Behavior Management 14. 987-999. DOI: 10.2147/PRBM.S318139 (last access: 02/07/2022).

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., and Lind, F. (2015). Do People Know about Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In S. Gutwirth, R. Leenes, and P. d. de Hert. Reforming European data protection law. Heidelberg: Springer. 333-365. DOI: 10.1007/978-94-017-9385-8 (last access: 02/07/2022).

Trepte, S., Masur, P. (2016). Cultural Differences in Social Media Use, Privacy, and Self-Disclosure. http://opus.uni-hohenheim.de/volltexte/2016/1218/pdf/Trepte_Masur_ResearchReport.pdf (last access: 12/07/2021).

Trepte, S., Masur, P. (2017). Privacy Attitudes, Perceptions, and Behaviors of the German Population. https://www.philipp-masur.de/documents/pubs/Trepte_Masur_2017_Research_Report_Hohenheim.pdf (last access: 02/07/2022).

Trepte, S., Reinecke, L., Ellison, B., Quiring, O., Yao, M., and Ziegele, M. (2017). A Cross-Cultural Perspective on the Privacy Calculus. Social Media and Society 3(1). DOI: 10.1177/2056305116688035 (last access: 02/09/2022).

Turow, J., Hennessy, M. (2007). Internet Privacy and Institutional Trust: Insights from a National Survey. New Media & Society 9(2). 300-318. DOI: 10.1177/1461444807072219 (last access: 01/27/2022).

Urbonavicius, S., Degutis, M., Zimaitis, I., Kaduskeviciute, V., and Skare, V. (2021). From Social Networking to Willingness to Disclose Personal Data when Shopping Online: Modelling in the Context of Social Exchange Theory. Journal of Business Research 136. 76-85. DOI: 10.1016/j.jbusres.2021.07.031 (last access: 01/27/2022).

von Lewinski, K. (2014). Die Matrix des Datenschutzes. Tübingen: Mohr Siebeck.

Westin, A., Harris Louis & Associates (1991). Harris-Equifax Consumer Privacy Survey. Tech. rep. Conducted for Equifax Inc. 1255 adults of the U.S. public.

Westin, A. (2003). Social and Political Dimensions of Privacy: Social and Political. Journal of Social Issues 59(2). 431-453. https://doi.org/10.1111/1540-4560.00072 (last access: 02/14/2022).

White K., Macdonnell R., and Dahl D. (2011). It's the Mind-Set that Matters: The Role of Construal Level and Message Framing in Influencing Consumer Efficacy and Conservation Behaviors. Journal of Marketing Research 48(3). 472-485. DOI: 10.1509/jmkr.48.3.472 (last access: 01/26/2022).

White, T. B. (2004). Consumer Disclosure and Disclosure Avoidance: A Motivational Framework. Journal of Consumer Psychology. 14(1/2). 41-51.

Woodruff, A., Pihur, V., Consolvo, S., Schmidt, L., Brandimarte, L., and Acquisti, 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. Tenth Symposium On Usable Privacy and Security. 1-18. https://www.usenix.org/system/files/conference/soups2014/soups14-paper-woodruff.pdf (last access: 02/14/2022).

Xu, H., Teo, H.-H., Tan, B. C. Y., and Agarwal, R. (2009). The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services. Journal of Management Information Systems 26(3). 135-174. DOI:

10.2753/MIS0742-1222260305 (last access: 01/28/2022).

Yun, H., Gwanhoo, L., Dan, K. (2014). A Meta-Analytic Review of Empirical Research on Online Information Privacy Concerns: Antecedents, Outcomes, and Moderators. *ICIS 2014 Proceedings 20.* https://aisel.aisnet.org/icis2014/proceedings/ISSecurity/20 (last access: 02/09/2022).

Yun, H., Lee, G., and Kim, D. J. (2019). A Chronological Review of Empirical Research on Personal Information Privacy Concerns: An Analysis of Contexts and Research Constructs. Information & Management 56(4). 570-601. DOI: 10.1016/j.im.2018.10.001 (last access: 02/07/2022).

Zhang, C., Cui, C., and Yao, Q. (2021). "I" Am Willing to Disclose, but "We" are Unwilling: The Impact of Self-Construal on Individuals' Willingness to Disclose. Psychology Research and Behavior Management 14. 1929-1945. DOI: 10.2147/PRBM.S336223 (last access: 02/07/2022).

Zimaitis, I., Urbonavicius, S., Degutis, M., and Kaduskeviciute, V. (2020). Impact of Age on the Willingness to Disclose Personal Data in E-Shopping. Proceedings of the European Marketing Academy 11(84569). http://proceedings.emac-online.org/pdfs/R2020-84569.pdf (last access: 02/09/2022).