

Putting a Price Tag on Personal Information – A Literature Review

Amina Wagner
Technische
Universität Darmstadt
wagner@is.tu-darmstadt.de

Nora Wessels
Technische
Universität Darmstadt
wessels@is.tu-darmstadt.de

Peter Buxmann
Technische
Universität Darmstadt
buxmann@is.tu-darmstadt.de

Hanna Krasnova
Universität
Potsdam
krasnova@uni-potsdam.de

Abstract

In the digital age, personal information is claimed to be the new commodity with a rising market demand and profitability for businesses. Simultaneously, people are becoming aware of the value of their personal information while being concerned about their privacy. This increases the demand of direct compensation or protection. In response to the commodification of privacy and the increased demand for compensation, a number of scholars have shed light on the value people assign to their personal information. However, these findings remain controversial as their results differ tremendously due to different research methods and contexts. To address this gap, we conducted a systematic literature review to gain insights into the current research state and to identify further research avenues. By synthesizing and analyzing 37 publications, we provide an integrative framework along with seven contextual factors affecting individuals' valuation of privacy.

1. Introduction

The valuation of personal information is more relevant today than ever before because personal information is claimed to be the new commodity of the 21st century with a rising market demand and profitability for businesses [1]. Particularly, online businesses like Facebook, Google & Co. monetize their users' personal information. Simultaneously, people are becoming aware of the value of their personal information [2] which increases the demand of direct compensation and participation [3, 4]. In response to the trend of monetizing personal information, startups (e.g., datacoup, datafairplay) have emerged developing an infrastructure for users to actively sell their personal information to third parties. Indeed, increasing scholarly attention has been brought to the economics of information reflected by the growing number of

studies in this field. More specifically, research has been conducted on how much people are willing to pay in order to protect their personal information and how much they demand for selling their data. However, sometimes it appeared as if people were incredibly privacy concerned and hence highly valued their data [5, 6] while other studies indicated that people do not value it at all [7, 8]. Even when researchers asked for the same type of data to be revealed, they obtained two completely different results. For instance, Huberman et al. (2005) showed that participants would sell their weight information for \$74.06 on average, whereas the study of Grossklags and Acquisti (2007) resulted in a price of \$31.80 for the same kind of information. Furthermore, Schreiner and Hess (2015) showed that Facebook users would pay on average 0.63 euro for a premium version while the study of Krasnova et al. (2009) resulted in a monthly fee of 1.2 and 1.4 euro for a privacy-enhanced social networking site (SNS).

As these results are confounding and scattered, it is important to understand the differences between scholars to get insights into the valuation of privacy and how it is affected. Moreover, a systematic approach to comprehensively describe the current research state is missing despite its importance to provide an integrative and common understanding of individuals' valuation of privacy. Furthermore, businesses can only partially rely on knowledge when offering services which affect privacy concerns of their customers. To address this practical and theoretical issue, we conducted a structured literature review to provide a narrative theoretical survey, comparison, and integration of current literature. Thereby, the following research question will be answered: *What influences the economic value people assign to their personal information and how can the existing approaches and results be conceptualized in a unified way?*

Building upon established structured literature review methods [11, 12], we analyzed empirical studies within 37 publications published in various journals, conferences, and workshops. We coded the determinants of privacy valuation along with its

research methods. These were then summarized in a twofold pattern including an in-depth look at underlying differences seeking to synthesize the resulting knowledge into an integrative theoretical framework [13]. Along with the determinants, willingness-to-pay and willingness-to-accept are then introduced as the two facets of how valuation of information is measured. Afterwards, we summarize and synthesize our main findings in an integrative theoretical framework. Findings are discussed and future Information Systems (IS) research suggestions are given before the paper closes with a conclusion.

2. Valuation of privacy

As privacy is monetized by businesses [14], it can be exchanged by individuals in order to gain certain benefits. Referred to as the privacy calculus, people are performing a trade-off between privacy risks and benefits when assessing the behavioral intention to disclose information [15]. Based on Smith et al. (1996) risks can be categorized into four dimensions: collection, improper access, error restrictions and secondary data usage. With regard to benefits, they should be perceived as higher than risks when revealing personal information [16, 17]. Scholars found proof that people exchange their personal information to gain advanced services [18] or monetary rewards [19]. Thus, understanding the value people put on their personal information is necessary for businesses to provide services accordingly. But personal information is different from other traded goods as the value people assign to their privacy is difficult to assess and generally subjective [7]. Further, people do not have valid and complete information of how their personal information will be used by businesses [20].

In an attempt to operationalize the valuation of privacy, previous scholars relied on surveys [e.g., 26] and experiments [e.g., 14] measuring the amount of data which is revealed and shared with third parties as a form of privacy valuation [10, 22, 23]. More specifically, they investigated what determines individual's privacy valuation and how privacy is traded by either measuring their willingness-to-pay (WTP) or their willingness-to-accept (WTA).

WTP for privacy deals with the fact that individuals prefer to pay a fee for privacy-enhancing features. It is referred to privacy premium which is typically offered by companies as a freemium product. Following the freemium idea, businesses provide their basic products free of charge while offering fee-based additional services [9]. In contrast, WTA describes individuals' willingness-to-sell data in return for monetary benefits

[20]. Thus, WTA describes the proposition that individuals respond to economic incentives in deciding whether to reveal personal data to a third party [7] by taking an active role as a seller.

3. Review method

In the following section, we provide an overview of our review method to identify the relevant literature by following the guidelines by von Brocke et al. (2009) and Webster and Watson (2002). By doing so, we describe the search term as well as the inclusion and exclusion criteria and present an overview of the conducted search process with its data sources. We describe the steps in detail in order to make the underlying process as transparent as possible following a call for more rigor [12].

With regard to our search terms, we conducted a pilot search based on the keywords used in prominent articles on privacy valuation [6, 22–24] as a starting point and refined this commencing search string iteratively. As the search query is crucial, the terms were selected precisely so that they sufficiently match the topic under investigation [12]. Given the variety of keywords describing the “valuation of personal information” we divided this rudimentary term in its main components and searched for synonyms and related expressions. Finally, the final search string consisted of four parts. The first part comprises synonyms for “value” as this is the main approach of our study. We used a number of search terms ranging from “economics”, “value/valuation”, and “worth” to terms describing pricing approaches. Of course, we also included “willingness” as it is the main component for WTA and WTP. The second part consists of different expressions for “personal” while the third part included the synonyms “information” and “data”. The last part of the final search query delimits the topic under investigation as the pilot search revealed that the topic received scholarly attention with the rise of ecommerce and SNS. This resulted in the following search query: ((“economics” OR “worth” OR valu* OR willingness-to* OR “freemium” OR “pricing”) AND (“privacy” OR “personal” OR “private”) AND (“data” OR “information”) AND (“online”)).

In order to ensure that only appropriate and relevant publications are included and that every paper incorporated in this review process is treated in the same way, we determined inclusion and exclusion criteria [11]. Inclusion criteria were defined as: (1) valuation of privacy and personal information was the main focus under investigation, (2) studies applied should be empirical and on an individual-level, and (3) studies investigated user's monetary WTP and/or WTA

in order to protect or divulge their personal data. In contrast, exclusion criteria included: (1) studies focused on privacy and personal data in general without examining the monetary value of the former, (2) the studies concentrated solely on testing measurement methods to evaluate privacy values or (3) were published before 2000 due to its validity in the online context.

In the next stage, we selected appropriate scientific databases which contained relevant publications [11]. The above presented search query was used for the EBSCOhost database whereas queries for other databases differed slightly due to its technical requirements. Finally, we conducted a systematic search in the following digital databases: ACM Digital Library, AIS Electronic Library, EBSCOhost Business Source Premier, ScienceDirect, SpringerLink, and WebOfScience. In order to be exhaustive, we decided to search by title and abstract without further restrictions with regard to specific journals, conferences, and topics. Second, we conducted a manual search in eight leading IS journals in the senior scholars' basket of journals (i.e., Management Information Systems Quarterly, Information Systems Research, Journal of Management Information Systems) and in the IEEE publication list to ensure that no major IS or technology research articles were neglected. All found publications were uploaded into a Citavi database. Our search resulted in 1169 publications (excluding duplicates) for all selected databases in total. Next we scanned the titles and abstracts based on the selection criteria, which reduced the sample size to 114. By applying full text analysis, the sample was again minimized to 17. As suggested by Webster and Watson (2002) we also conducted a forward and backward search on this set of relevant

publications. The process of backward search refers to the analyses of citations in the selected set of publications. In contrast, forward search aims at identifying publications that cite the selected key papers [11], which was conducted by utilizing respective functions of Google Scholar. During forward and backward searches, we applied the same procedure as described before by identifying potentially relevant publications through their titles and abstracts and further investigating them with a full text analysis. Finally, we obtained a concluding set of 37 publications published between 2002 and 2017 which was the basis for further analyses and discussion.

4. Integrative framework

After collecting the relevant literature, we coded the publications with regard to their research approaches and aggregated the results in a table (see Appendix). Subsequently, we followed suggestions by Baumeister and Leary (1997) and consolidated the results of our literature review in an integrative theoretical framework (see Figure 1) going beyond solely describing previous studies [11, 13].

In accordance with previous privacy literature [25], we identified the context as highly relevant for users' privacy valuations. While synthesizing the literature, seven contextual factors emerged: type of information, person, biases, individual, privacy, value related, and social factors. These determinants affect the valuation of privacy. As all of the publications in our final sample implicitly divide context factors and behavioral outcome, a twofold pattern was chosen. A detailed summary of these patterns follows.

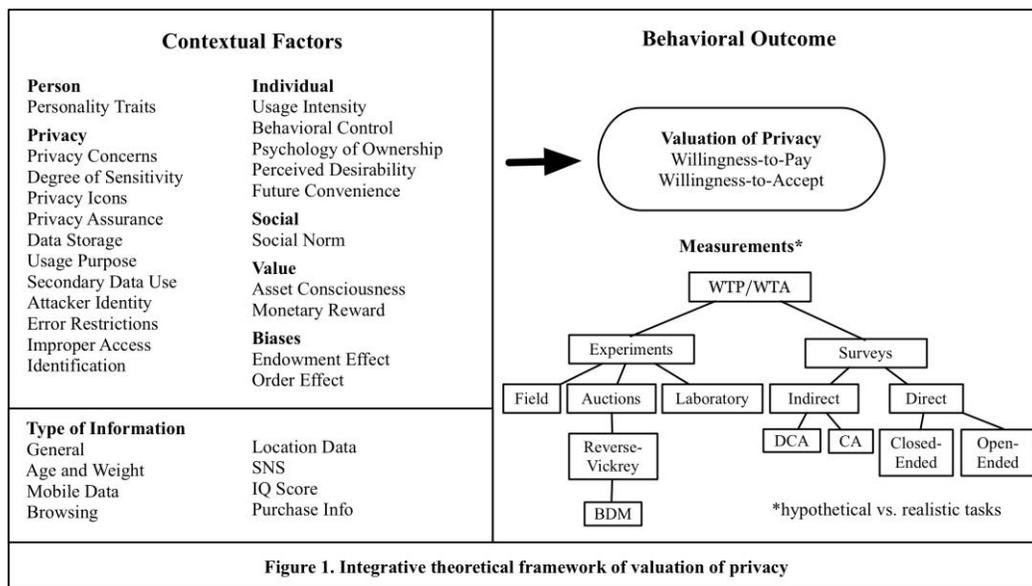


Figure 1. Integrative theoretical framework of valuation of privacy

4.1. Contextual factors

First, we identified the factor *type of information* which is determined by the research case of being highly relevant. All publications apart from Rose (2005) tested the impact of requests for certain types of information on individuals' privacy valuations. The type of information being evaluated by individuals ranges from SNS profile (10 papers), browsing information including websites (7 papers), purchase information (7 papers), location data (8 papers), mobile data (5 papers), IQ scores (2 papers), age and weight (2 paper) as well as general information/socio-demographics (4 papers). When authors investigated the value of SNS information, Facebook was used as the case distinguishing between all information stored on Facebook [8, 27], the Facebook wall, or profile information [28]. Among others, studies also tested peoples' privacy valuations in the context of web browsing by for example investigating the WTP for a privacy friendly search engine [29]. In addition, the valuation mode has been identified as a determinant of privacy valuation. A few studies built on behavioral economics and tested certain *biases* which affect the value individuals assign to their data [7, 20, 30]. Providing evidence for the endowment effect with regard to privacy valuations, Acquisti et al. (2009) demonstrated that participants valued their personal information even more when being asked to give it up compared to receiving it. This bias has also been confirmed by Kamleitner et al. (2016) in the context of privacy as a possession.

Moving beyond the type of information which is often determined by the research case and behavioral biases, other contextual factors have been identified as having a direct impact on individuals' WTP/WTA. The dispositional factor *person* comprises personality traits. Staiano et al. (2014) investigated the influence of personality traits on peoples' WTA. They found no significant correlations between bid values and personality traits apart from agreeableness. Further, some scholars controlled for demographics. For instance, Cvrcek et al. (2006) showed that median bids of women are higher compared to men but interestingly the vast amount of studies found no significant differences for age, gender, and income [14, 24, 33].

Furthermore, as the awareness of risks while sharing information online increases, we identified the factor *privacy* as another contextual determinant. According to Grossklags and Acquisti (2007), privacy preferences are the major antecedent for WTP and WTA. Looking at general privacy concerns, a great body of literature showed that valuation of privacy is negatively affected by the dispositional determinant

'general privacy concern' [23, 31, 34–36]. This is also exemplified in the study undertaken by Steinfeld (2015) demonstrating that abstainers are predominantly rejecting the offer due to higher privacy concerns compared to the group of traders. Egelman (2012) classified the participants according to Westin's metric into Privacy Fundamentalists, Privacy Unconcerned, and Privacy Pragmatists [37], but found no significant differences. In contrast, Nguyen et al. (2016) used the same metric and observed major differences between those groups.

Apart from general privacy concerns, scholars investigated different *privacy* antecedents by manipulating or framing perceived privacy issues. Hann and Lee (2002) explored the effect of three subcategories of privacy concerns (errors, secondary use, and improper access) building on the privacy definition of Smith et al. (1996). Secondary data use was found to be the major driver of valuation of privacy which is also acknowledged by Potoglou et al. (2013) and Preibusch (2013). Beyond that identification [5, 24, 34, 42] caused an increased demand for compensation whereas obfuscation decreased it [35]. In addition, Egelman et al. (2009) provide evidence that when buying a privacy-sensitive good, people are more reluctant to pay for privacy. Similarly, Danezis et al. (2005) stated considerable differences between the WTA for academic and commercial use. When the participants were told that their data will be used for commercial purposes their bids roughly doubled. In sum, many privacy related antecedents were tested in literature.

Although privacy related antecedents received a lot of attention in research, other factors like *value* have been identified as a major influence factor on privacy valuation. Spiekermann et al. (2012) demonstrated that asset consciousness drives the value assigned to SNS information whereas Steinfeld (2015) mentioned that the monetary reward offered in exchange for data is a major antecedent to explain peoples' disposition to trade their data.

Moreover, we identified *individual* factors such as the usage intensity or perceived desirability as antecedents determining one's perceptions and beliefs about a certain dataset. In the case of age and weight information, Huberman et al. (2005) found proof that information that is perceived as 'abnormal' is assessed as being more valuable than e.g. normal weight. Other scholars found proof that people are willing to trade their data to get future convenience in return [19, 22]. Lastly, we classified *social* factors as Racherla et al. (2011) showed that social norms influence the willingness-to-pay for privacy.

4.2. Behavioral outcome

Following the classification suggested by Grossklags and Acquisti (2007), we categorized the publications on valuation of privacy in WTP for privacy and WTA privacy invasion. With a share of 57% (21 papers), the majority of authors investigated WTP. According to the results of the literature review, one can assume that people do not value their personal information at all. On the social network front, people displayed a generally low WTP when being asked to simply save their Facebook profiles from deletion [27]. While psychology of ownership, meaning to see the profile as one's own property, was shown to be a driving factor for WTP; up to 62% were not willing to pay even a trivial amount to save their profiles from deletion. The result changes though when people are made aware that a third party is interested in their data and hence, were under the effect of asset consciousness. The share of people with a WTP of 0 euro drops to 40% and the average WTP increases by a factor of 3.4.

Additionally, Schreiner and Hess (2015) demonstrated that Facebook users would pay on average 0.63 euro while Krasnova et al. (2009) found a WTP between 1.2 and 1.4 euro a month for a privacy-enhanced SNS. These slightly different amounts might be explained due to opposing privacy definitions. Schreiner and Hess (2015) described the Facebook alternative as being less intrusive with regard to advertisement. Krasnova et al. (2009) goes beyond that and crafted a Facebook alternative which provides a higher level of customizability and privacy control.

When looking at privacy protection in the context of smartphones it also became apparent that people are rather averse using a smartphone application that has access to their SNS data [45]. In order to avoid a feature such as the FB login people report to be willing to pay between 1.79 and 6.24 euro depending on the number of permissions the FB login option asked for. Further, people are willing to sell their data when a certain price range is reached [5, 24]. But the WTA differentiates when information is being used for academic purposes compared to commercial purposes [21]. When it comes to very sensitive information like age and weight, people seem to value the information the most, especially when the weight deviates from the standard [6]. An additional result was that people seem to be quite unwilling to sell their location data recorded by their smartphones with WTA values ranging from about 3 euro for a single time location share and between 22.5 and 43 euro for a whole month of observation [5]. Those WTA amounts were among the highest observed throughout the review. It became clear that people are quite worried about such data that

allows others to draw conclusions on their daily routines and places they visit. Further, high amounts were raised for weight information. Huberman et al. (2005) showed that participants would sell their weight information for \$74.06 while Grossklags and Acquisti (2007) resulted in a requested price of \$31.80 for the same kind of information. These conflicting amounts can be explained by the research design. Grossklags and Acquisti (2007) investigated the WTA by applying open-questions whereas Huberman et al. (2005) relied on a reverse-second-price-auction.

Contrary, search engine users seem to be rather reluctant when it comes to protecting their own browsing behavior data. The amount they were willing to pay monthly for a premium version of a search engine such as Google with enhanced privacy features seemed to be around 1.5 dollar. Furthermore, it was shown that information on web behavior in general, be it the shops or the websites visited, is valued less than information that is not only linked to the web behavior of the user but also to his offline identity (such as name, address, or income). The median WTA for data out of the former category was found to be around 7 euro whereas the latter one was valued at 25 euro [24]. This is also exemplified by the study of Preibusch (2013) where people appreciate privacy-enhancing features in search engines when it is offered for free but only 15% would pay a minor premium for it. However when privacy icons are shown, the share of people choosing the shop with better privacy conditions is significantly higher than without [23]. They would even pay a premium fee for it [43].

Regarding the valuation of privacy, we found that all studies are related to one's own privacy except of one study focusing on the difference between own profile information and others' profile information. This study demonstrated that friends' privacy is less valued implying that people are 'privacy egoists' [46].

While certain rules of thumb may be derived from the studies e.g., location data is valued higher than SNS or browsing information, the methods used to elicit peoples' privacy valuations have to be considered.

4.3. Measurement methods

In the following section, we will provide an overview of different methods used in current studies for measuring the monetary valuation of privacy, in the form of WTA and WTP. The categorization is based on the classification framework for WTP measurement methods by Breidert et al. (2006). As demonstrated by Benndorf and Normann (2014) the measurement method has a non-trivial impact on peoples' valuation of privacy. They used two techniques to elicit valuation

of SNS information which resulted in two different results. The description of the methods follows.

We identified both, direct as well as indirect surveys as a frequently used method for measuring the monetary valuation of privacy. Especially direct surveys with online-questionnaires were often used either with simple open-ended questions, asking for a particular value as a threshold, or closed-ended questions, where a given value has to be assessed by the participants stating simple yes/no-answers [7]. A special form of these direct surveys is the contingent valuation method (CVM) that can be appropriately used for the valuation of goods or services which do not have an established market-price yet [27]. At the base of a fictitious scenario, the participants can either be asked to state a particular value [27] or they are making a discrete choice (yes/no) for a given price [26]. As most direct surveys are hypothetical in nature, indirect surveys like conjoint analysis (CA) and discrete choice method (DCM) are applied to reduce this problem. Conjoint analysis builds on a service with several different features. Consumers can then build a preference ranking out of the different product versions [46]. Therefore, it is possible to measure the relative importance of these features [10]. For instance, Hann and Lee (2002) varied the perceived privacy concerns with regard to error, improper access, and secondary data use that people encounter when visiting a website. Similarly to CA, the DCM considers a product or service as a combination of different attributes [47]. Participants are asked to choose one out of two or more hypothetical alternatives in order to measure the independent influence of product's attributes as well as the valuation of the different attributes [40, 45]. One type of the DCM is the binary choice method, which was used by Nguyen et al. (2016).

In contrast to surveys, other reviewed studies conducted field or laboratory experiments with real life consequences by measuring the WTA or WTP as actual behavior either locally in a laboratory setting or unbounded of a special location [20, 48, 49]. One of the laboratory experiments was conducted as a take-it-or-leave-it (TIOLI) experiment [28]. All aforementioned methods have in common, that they can be conducted independently of time and number of participants, contrary to auctions where several participants need to bid in parallel. In all eight papers conducting an auction, Vickrey auctions (VA) were applied in a reversed way [e.g., 43]. It is conducted with sealed bids whereas the winner with the highest bid wins, only having to pay the price of the second highest bid [47]. This forces the participants to release their true valuations, because too high or too low bids are not going to be successful. A special type of VA, the Becker-DeGroot-Marshak Mechanism (BDM) [51]

can also be applied to the WTA/WTP context by giving participants the opportunity to state the price they are willing to pay to purchase a particular good, for example a premium version of a SNS. If the stated price is lower than or equal to a randomly set price, the good can be bought at the random price [9].

Besides these differences of the measurement methods, the conducted studies varied also in the design settings of the task the participants had to fulfill. We identified hypothetical settings (20 studies in our sample), where people realize that they can accomplish the task without real implications for them as they are e.g. asked to imagine a specific situation [52] or had to choose between hypothetical alternatives [38]. Hypothetical studies may mitigate peoples' affect as the participants have no 'costs' stating an inappropriate value [10, 53]. Contrary, some studies provide real consequences for the participants, as they realistically sell their data [28, 35] or have to do a real purchase [23, 43]. But also in these cases, the participants were aware of the fact that they took part in an experiment.

5. Discussion

In the following, we will discuss our major findings obtained from the analysis of the reviewed studies and present our deriving future research suggestions. As the literature review reveals, numerous studies were seeking to quantify the monetary value people assign to their data over the last 15 years. The literature is centered on experimental designs ranging from online settings to laboratory and field experiments. However, the monetary value of privacy remains controversial. Especially as the terms personal information and privacy encompass so many different kinds of data that can be sold or protected. Judging from the results of our review, it appears that the value proposition to individuals' privacy is generally low. Further, the results of studies facing the participants with real consequences indicate that sometimes even a trivial discount is enough to sell personal information and that even tiny sums of money are seen as simply too much to protect it. Based on our analyses, one can see that scholars either focused on a specific subset of information or a situation-specific context like secondary data use or privacy assurances.

First of all, the majority of studies investigating peoples' privacy valuation focused on WTP. But more and more startups emerge, that allow users to actively sell their personal information. Despite this trend, the knowledge about generalizable WTA is limited due to the very specialized scopes of the preliminary studies. Therefore, a comprehensive perspective on all variable attributes affecting WTA might be a big a progress.

Beyond that, future research can look at the impact of re-sharing data that has been sold to an organization and is further shared by the latter with other parties.

For all 37 identified publications, we summarized determinants and assigned them to seven contextual factors with regard to WTA/WTP. The amount of identified contextual factors reveal the diversity of the previous studies. Overall, two predominant contextual factors emerged: privacy related factors and the type of information. While we found 11 subcategories of privacy factors, general privacy concerns and the degree of sensitivity of the data to be revealed were most widely used for both types of behavioral outcomes. All of these studies share one common result: the more sensitive the data and the more identifiable people are, the higher has been the price people attach to their data as they perceive higher risks.

In addition, it was shown that in some cases the reported values for WTA and WTP may appear to be high but that this may only be due to the way the research was conducted. According to the review, studies with real consequences should be conducted to elicit users' privacy valuation. Being incentivized, people raise more realistic amounts in order to protect or sell their data [e.g., 7]. Thereby, a 'hypothetical bias' should be omitted in future studies. Additionally, as described earlier, the results of studies using direct surveys differed tremendously from those using experiments like auctions. One of the reasons of these results might be social desirability or the talk-is-cheap problem. Hence, we conclude that hypothetical studies may lead to inflated WTA and WTP values and their hypothetical nature is probably one of the causes for the privacy paradox [e.g., 6]. Therefore, validity of these studies is questioned.

A weakness of the analyzed studies are the opposing definitions of privacy as well as how and why information is collected which caused confounding privacy valuations. Still, the more transparent data practices were presented, the higher has been the awareness of risks and thus the impact on peoples' economic valuation of privacy. Thus, when privacy information is easy accessible and plausible, people seem to react very sensitive to it. These studies are important to understand users' assessment in a specific context, but it is difficult to transfer them to a broader context with respect to complicated data policies, complex exchange partners, and indirect outcomes. As a result, research is not sufficient and satisfying in explaining peoples' inability to be consistent in their privacy valuation.

Looking at the theoretical contribution of prior studies, they are merely based on privacy literature while some use the privacy calculus and its underlying trade-off between risks and benefits as the conceptual

model [10, 38]. Just a few studies build on theories such as information-processing theory [19, 22], multi-attribute utility theory [38], theory of property rights [26], and theory of planned behavior [9]. Future research can adapt and extend theories from other disciplines focusing on the decision process and peoples' knowledge and awareness as well as their confidence in their own judgements. Some suggestions would be evaluability theory [54] and elastic justification [55] as well as general biases lend from behavioral economics. As IS research is interdisciplinary in nature, it should highlight how IT drives the valuation of privacy which is oftentimes due to the way privacy information is presented. Taken together, it would be important to clarify the mixed effects of some critical antecedents to derive to a broader conceptualization of privacy valuations. Finally, more research should be devoted to understand moderating effects of WTP and WTA.

Lastly, the sample size and sample characteristics differ tremendously among the selected studies. Thus, some kind of 'selection bias' can be recognized. Studies are mainly conducted with students as participants [e.g., 2, 15, 25]. Students are generally characterized by a lower reluctance to participate in scholars because they tend to be more sensitive to rewards and are easily reachable for researchers. This results in a very young sample compared to e.g. the field study of Acquisti et al. (2009). In addition, across all studies concerning the valuation of information, people have different cultural backgrounds ranging from a purely German sample [8–10] to a European sample [32] and a US sample [23, 43]. Furthermore, many studies used SNS as the case. One can argue that SNS users are privacy unconcerned as they reveal their data for free to use social networking services in return. Taken together, this implies that current research is not sufficiently representative for all internet users.

To sum up, our structured literature review has shown that people are very context-sensitive when evaluating their privacy. Especially, the measurement method and thus the study design can have a tremendous impact on the elicited monetary value of peoples' data. Privacy concerns as a dispositional factor and sensitivity of data seem to be a major driver of valuation of data. The more sensitive the data and the more transparent privacy issues are presented, the higher is the monetary value people attach to their data.

6. Conclusion

The goal of this structured literature review was to determine the value people assign to their personal

information and to conceptualize the preliminary approaches and findings in a unified way. We showed that the monetary valuation of personal information can be measured as how much people are willing to pay in order to protect (WTP) as well as how much they are willing to accept in order to sell (WTA) their personal information. Hence, we reviewed 37 publications examining at least one of these two forms of privacy valuation and synthesized them in an overview table (see Appendix) which served as the basis for further analysis. This paper makes several contributions to IS research and practice. Our paper is the first to provide a comprehensive review of the empirical studies on individuals' valuation of privacy. Thus, we introduce a comprehensive, integrative theoretical framework of privacy valuation along with their contextual factors like person, type of information, biases, privacy, individual, social, and value driven antecedents. This theoretical framework can serve as a basis to conceptualize the context-dependent valuation of information and its underlying phenomena, as well as guide future empirical research in this field. For online companies relying on customers' information, the framework shows that individuals disclose their information when benefits are offered in accordance. Additionally, online companies are made aware which key factors can drive the valuation of privacy critically like linkage to offline identity and perceived desirability. For individuals, this paper highlights multiple factors that drive the awareness and consciousness such as transparent secondary data use and identification to increase their valuation of privacy.

7. Acknowledgment

This work has been co-funded by the DFG as part of project A3 within the RTG 2050 "Privacy and Trust for Mobile Users" and supported by CRISP, funded by BMBF and HMWK.

8. References

- [1] S. Spiekermann, A. Acquisti, R. Böhme, K. Hui, "The challenges of personal data markets and privacy," *Electronic Markets*, 25(1), 2015, pp. 161–167.
- [2] C. Li, D. Y. Li, G. Miklau, D. Suci, "A Theory of Pricing Private Data," *ACM Transactions on Database Systems*, 39(4), 2014, pp. 1–28.
- [3] *New York Times*, "Start-Ups Seek to Help Users Put a Price on Their Personal Data," 2012.
- [4] S. Spiekermann, J. Korunovska, "Towards A Value Theory for Personal Data," *Journal of Information Technology*, 32(1), 2017, pp. 62–84.
- [5] O. Barak, G. Cohen, A. Gazit, E. Toch, "The Price Is Right? Economic Value of Location Sharing," *Proceedings of the 2nd ACM conference on Pervasive and ubiquitous computing adjunct publication*, 2013, pp. 891–899.
- [6] B. A. Huberman, E. Adar, L. R. Fine, H. P. Labs, P. M. Road, P. A. Ca, "Valuating Privacy," *IEEE Security & Privacy*, 3(5), 2005, pp. 22–25.
- [7] J. Grossklags, A. Acquisti, "When 25 Cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information," *Proceedings of Workshop on the Economics of Information Security*, 2007.
- [8] C. Bauer, J. Korunovska, S. Spiekermann, "On the Value of Information - What Facebook Users Are Willing To Pay," *Proceedings of 20th European Conference on Information Systems*, 2012.
- [9] M. Schreiner, T. Hess, "Why Are Consumers Willing to Pay for Privacy? An Application of the Privacy-freemium Model to Media Companies," *Proceedings of the 23rd European Conference on Information Systems*, 2015.
- [10] H. Krasnova, T. Hildebrand, O. Guenther, "Investigating the value of privacy in online social networks: conjoint analysis," *Proceedings of the 30th International Conference on Information Systems*, 2009.
- [11] J. Webster, R. T. Watson, "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *MIS Quarterly*, 26(2), 2002, pp. xiii–xxiii.
- [12] J. von Brocke, A. Simons, B. Niehaves, K. Riemer, R. Plattfaut, A. Cleven, ... K. Reimer, "Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process," *Proceedings of the 17th European Conference on Information Systems*, 2009.
- [13] R. Baumeister, M. Leary, "Writing Narrative Literature Reviews," *Review of General Psychology*, 1(3), 1997, pp. 311–320.
- [14] N. Steinfeld, "Trading with privacy: the price of personal information," *Online Information Review*, 39(7), 2015, pp. 923–938.
- [15] T. Dinev, P. Hart, "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research*, 17(1), 2006, pp. 61–80.
- [16] H. Xu, T. Dinev, J. Smith, P. Hart, "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances," *Journal of the Association for Information Systems*, 12(12), 2011, pp. 789–824.
- [17] R. T. Rust, P. K. Kannan, N. Peng, "The Customer Economics of Internet Privacy," *Journal of the Academy of Marketing Science*, 30(4), 2002, pp. 455–464.
- [18] R. K. Chelappa, R. G. Sin, "Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma," *Information Technology and Management*, (6), 2005, pp. 181–202.
- [19] I. Hann, T. S. Lee, "Online Information Privacy: Measuring The Cost-Benefit," *Proceedings of the 23rd International Conference on Information Systems*, 2002.
- [20] A. Acquisti, L. John, G. Loewenstein, "What is privacy worth?," *Proceedings of the Workshop on Information Systems and Economics*, 2009.
- [21] G. Danezis, S. Lewis, R. Anderson, "How much is location privacy worth?," *Proceedings of the 4th Workshop on the Economics of Information Security*, 2005.
- [22] I.-H. Hann, K.-L. Hui, S.-Y. Tom L., I. P. L. Png, "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach," *Journal of*

- Management Information Systems, 24(2), 2007, pp. 13–42.
- [23] J. Y. Tsai, S. Egelman, L. Cranor, A. Acquisti, “The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study,” *Information Systems Research*, 22(2), 2011, pp. 254–268.
- [24] J. P. Carrascal, C. Riederer, R. De Oliveira, “Your Browsing Behavior for a Big Mac: Economics of Personal Information Online Categories and Subject Descriptors,” *Proceedings of the 22nd International Conference on World Wide Web*, 2013.
- [25] L. Brandimarte and A. Acquisti, *The Economics of Privacy*, New York, Oxford University Press, 2012.
- [26] E. Rose, “Data Users versus Data Subjects: Are Consumers Willing to Pay for Property Rights to Personal Information?,” *Proceedings of the 38th Hawaii International Conference on System Sciences*, IEEE, 2005.
- [27] S. Spiekermann, J. Korunovska, C. Bauer, “Psychology Of Ownership And Asset Defense: Why People Value Their Personal Information Beyond Privacy,” *Proceedings of the 33rd International Conference on Information Systems*, 2012.
- [28] V. Benndorf and H.-T. Normann, *The Willingness to Sell Personal Data*, 2014.
- [29] J. Bughin, “Digital user segmentation and privacy concerns,” *Journal of Direct, Data and Digital Marketing Practice*, 13(2), 2011, pp. 156–165.
- [30] B. Kamleitner, H. Haddadi, “Can Users Price Real-Time Contextual Information?,” *ACM Transactions on Internet Technology. Special issue on economics of security and privacy*, 2017, 2016.
- [31] J. Staiano, N. Oliver, B. Lepri, R. De Oliveira, M. Caraviello, N. Sebe, “Money Walks: A Human-Centric Study on the Economics of Personal Mobile Data,” *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, 2014.
- [32] D. Cvrcek, V. Matyas, M. Kumpost, G. Danezis, “The value of location information,” *Proceedings of the ACM Workshop on Privacy in the Electronic Society*, 2006, pp. 109–118.
- [33] S. Egelman, A.P. Felt, and D. Wagner, *Choice Architecture and Smartphone Privacy: There’s A Price for That*, Berlin Heidelberg, Springer, 2012.
- [34] S. Preibusch, “The Value of Web Search Privacy,” *IEEE Security & Privacy*, 13(5), 2015, pp. 24–32.
- [35] A. J. B. Brush, J. Krumm, J. Scott, “Exploring End User Preferences for Location Obfuscation, Location-Based Services, and the Value of Location,” *Proceedings of the 12th ACM international conference on Ubiquitous computing*, 2010, pp. 95–104.
- [36] D. Christin, B. Christian, N. Leibecke, “What’s the Value of Your Privacy? Exploring Factors That Influence Privacy-sensitive Contributions to Participatory Sensing Applications,” *Proceedings of the 38th Conference on Local Computer Networks Workshops*, 2013, IEEE, pp. 918–923.
- [37] A.F. Westin, *Equifax-Harris Consumer Privacy Survey*, New York: Louis Harris & Associates, Equifax, Inc., 1991.
- [38] K. D. Nguyen, H. Rosoff, R. S. John, “The effects of attacker identity and individual user characteristics on the value of information privacy,” *Computers in Human Behavior*, 55(1), 2016, pp. 372–374.
- [39] H. J. Smith, S. J. Milberg, S. J. Burke, “Information privacy: measuring individuals’ concerns about organizational practices,” *MIS Quarterly*, 20(2), 1996, pp. 167–196.
- [40] D. Potoglou, S. Patil, C. Gijón, J. Palacios, C. Feijóo, “The Value of Personal Information Online: Results from Three Stated Preference Discrete Choice Experiments in the UK,” *Proceedings of the 21st European Conference for Information Systems*, 2013.
- [41] S. Preibusch, “The value of privacy in Web search,” *The Twelfth Workshop on the Economics of Information Security (WEIS)*, 2013.
- [42] T. Regner, G. Riegner, “Privacy Is Precious : On the Attempt to Lift Anonymity on the Internet to Increase Revenue,” *Journal of Economics & Management Strategy*, 26(2), 2017, pp. 318–336.
- [43] S. Egelman, J. Tsai, L. F. Cranor, A. Acquisti, “Timing Is Everything? The Effects of Timing and Placement of Online Privacy Indicators,” *Proceedings of the 27th international conference on Human factors in computing systems*, 2009.
- [44] P. Racherla, J. S. Babb, M. J. Keith, “Pay-What-You-Want Pricing for Mobile Applications: The Effect of Privacy Assurances and Social Information,” *Proceedings of the Conference for Information Systems Applied Research*, 4(1833), 2011.
- [45] H. Krasnova, O. Abramova, N. Eling, P. Buxmann, “Dangers of Facebook Login for Mobile Apps: Is There a Price Tag for Social Information?,” *Proceedings of 35th International Conference on Information Systems*, 2014.
- [46] Y. Pu, J. Grossklags, “Towards a Model on the Factors Influencing Social App Users’ Valuation of Interdependent Privacy,” *Proceedings of the 6th Workshop on Economic of Information Security*, 2016.
- [47] C. Breidert, M. Hahsler, T. Reutterer, “Willingness-To-Pay,” *Innovative Marketing*, 2(4), 2006, pp. 8–32.
- [48] A. R. Beresford, D. Kübler, S. Preibusch, “Unwillingness to pay for privacy: A field experiment,” *Economics Letters*, 117(1), 2012, pp. 25–27.
- [49] S. Preibusch, D. Kübler, B. Alastair R., “Price versus privacy: an experiment into the competitive advantage of collecting less personal information,” *Electronic Commerce Research*, 13(4), 2013, pp. 423–455.
- [50] N. Jentzsch, “Auctioning Privacy-Sensitive Goods: A Note on Incentive-Compatibility,” in *Privacy Technologies and Policy*, Cham, Springer, 2014, pp. 133–142.
- [51] G. M. Becker, M. H. DeGroot, J. Marschak, “Measuring Utility By a Single-Response Sequential Method,” *Systems Research & Behavioral Science*, 9(3), 1964, pp. 226–232.
- [52] B. Roeber, O. Rehse, R. Knorrek, B. Thomsen, “Personal data: how context shapes consumers’ data sharing with organizations from various sectors,” *Electronic Markets*, 25(95), 2015, pp. 95–108.
- [53] S. Singleton, J. Harper, “With a Grain of Salt - What Consumer Privacy Surveys Don’t Tell Us,” *Competitive Enterprise Institute*, 2001.
- [54] C. K. Hsee, J. Zhang, “General Evaluability Theory,” *Perspectives on Psychological Science*, 5(4), 2010, pp. 343–355.
- [55] M. E. Schweitzer, C. K. Hsee, “Stretching the Truth: Elastic Justification and Motivated Communication of Uncertain Information,” *The Journal of Risk and Uncertainty*, 25(2), 2002, pp. 185–201.

