The Trouble with Trust:
When Certification is Not Enough to Turn Trust into Willingness to Share Data

Cynthia Sokoll[(1)]

[(1)] Cynthia Sokoll is Doctoral Candidate at the Institute for Customer Insight, University of St. Gallen, Switzerland (cynthiasabrina.sokoll@unisg.ch).

Abstract

Consumer data has recently become immensely important for a company's success. However, firms often collect data from smart devices unbeknownst to consumers. Having no control over their data leaves many consumers concerned about data privacy and decreases their willingness to give companies personal information. One approach to solving this trust issue is to insert an intermediary in the data transfer process, i.e., between the consumer's smart product and the respective manufacturer, thereby guaranteeing proper data handling and data transfer practices. Based on four empirical studies, this paper explores whether installing such a certification authority as an intermediary increases consumer willingness to share information and how consumers' trust in data privacy influences this process. It also analyzes which entity is best suited to performing data certification. The results show that even though consumers' trust in data privacy is significantly increased by the existence of an independent third-party as a certification authority, this is not true for their willingness to share data. In addition, the existence of a third-party certification intermediary can even decrease the willingness to share information if consumers' trust in their smart product is high. Thus, certification is only to a limited extent a viable option for increasing a consumer's willingness to share smart product data. Consequently, managers should look for other approaches to earn consumers' trust and to foster their willingness to provide information, either instead of or at least in combination with data certification. The paper also presents new theoretical insights into certification in the digital age as well as trust and its sub-dimensions.

Keywords: data privacy, data disclosure, certification, smart products, trust

Introduction

Data are an important and valuable asset for companies (Tao et al., 2019). They give firms worldwide the opportunity to target and influence consumers directly, e.g., with customized product offers (Prince, 2018). Moreover, consumer data can give companies a decisive competitive advantage (Babula et al., 2017; Mazurek & Małagocka, 2019). While companies have long been collecting consumer data, this has significantly increased in recent years due to digitalization, with an increasing volume and quality of data now stored, shared, and analyzed (Cukier & Mayer-Schoenberger, 2013). If a product generates data, these data are often transferred to various entities. Brandtzaeg et al. (2019), for example, found that out of 21 mobile phone apps analyzed, 19 apps transferred personal data to about 600 primary and third-party domains. In addition, less than 15% of these data flows are disclosed (Libert, 2018), and a significant percentage of consumers do not know how their data are used (Truong et al., 2016). Moreover, consumers cannot be sure how many and which parties receive their data (Schudy & Utikal, 2017). Hence, individuals no longer have (full) control over their data privacy (Pinchot et al., 2018), potentially leaving consumers worried (Prince, 2018). Privacy concerns, however, may harm companies, for instance, by having a strong negative effect on consumers' purchase intentions (Eastlick et al., 2006). Even if companies inform consumers about their data privacy and data handling practices, this does not necessarily happen in a consumer-friendly manner, as, for example, privacy policy statements take over 84 minutes to read on average (Libert, 2018).

Amid this area of conflict—between protecting consumers' privacy while collecting as much data as possible for economic benefit (Moiso & Minerva, 2012)—, research suggested manifold mechanisms and ideas to strike the best possible balance for all stakeholders involved. One approach that has been proposed in the literature in various forms (e.g., Moiso & Minerva, 2012) is to install a trusted entity between the consumer and the smart product data recipient (i.e., the respective manufacturer), who guarantees consumers data privacy protection. This paper explores in detail the idea of installing such a certification authority. This entity will, for example, guarantee the safety of the smart product data, rule out security threats, and serve as a gatekeeper, forwarding only consumer-authorized data to the respective manufacturer. How feasible is this? Market forecasts for the worldwide testing, inspection, and certification industry certainly provide cogent arguments for adopting this approach, as a potential market growth from $209.4 billion in 2019 to $266.2 billion by 2024 is expected (MarketsandMarkets, 2019). Moreover, certification benefits companies in various ways, including

competitive advantages, market access, and the external confirmation of one's regulatory compliance (Tanner, 2000). However, certification also has critical aspects, for example, assessment independence or whether the audited company pays the certifying institution (Albersmeier et al., 2009). Moreover, Holland (2016) found that certification may have negative consequences under certain conditions, e.g., when the consumer does not trust the certification standard. Apart from several advantages and disadvantages, the existing empirical results on the impact of certification on consumers' feelings, intentions, and behaviors are not unanimous either, with previous research finding evidence for and against the effectiveness of certification (see below).

The fact that opinions vary and that empirical data on the acceptance of the above-described certification intermediaries are scarce raises a key question: If, and under which circumstances might data certification by a certification authority be a viable method for increasing consumers' trust in data privacy and for enhancing their willingness to share data? Moreover, it is not clear which entity is best suited to serving as a certification authority. These issues were explored with the help of four quantitative studies (of which one was correlative and three were experiments) focusing on different kinds of smart products. The results of this paper add to the literature on signaling, certification, trust, data privacy, and data disclosure. Moreover, they indicate that an independent third-party is considered a superior certification authority compared to various other entities, and also superior to no certification, yet not always significantly so. While third-party certification was found to increase trust in data privacy in all three experimental studies, it did not significantly increase the willingness to disclose information. Moreover, if consumers highly trust their smart product, the existence of a certification authority may significantly decrease the willingness to share data. One practical implication of the results is that companies, so as not to harm their economic aspirations, must carefully evaluate their measures for dealing with the lack of consumer trust in data privacy and the low willingness of consumers to provide data. In this regard, companies might consider employing other measures than data certification in order to achieve their goals, either stand-alone or possibly in combination with certification.

Theoretical background

Certification as a quality signal

Frequently, when consumers have no information about a product or cannot evaluate its quality before purchase or usage, they use signals as a source of information about this

good (Ali & Kapoor, 2009). A signal is a "marketer-controlled, easy-to-acquire informational cue, extrinsic to the product itself, that consumers use to form inferences about the quality or value of that product" (Bloom & Reve, 1990, p. 59). Thus, signals reduce uncertainty, simplify purchases and transactions (Wells et al., 2011), and lessen the information asymmetry between the parties involved in an economic exchange (Lohr & Krissoff, 2002). Certification is one example of various signals employed by companies (Minard, 2016), for example in marketing (Aiken & Boush, 2006). It is defined as "the (voluntary) assessment and approval by a (accredited) party on a (accredited) standard" (Meuwissen et al. 2003, p. 172).

Certification has been studied in various industries for years, for example, in e-commerce (e.g., Houston & Taylor, 1999), cloud computing (e.g., Lins et al., 2016), food and nutrition (e.g., Wu et al., 2014), software (e.g., Heck et al., 2010), and autonomous systems (e.g., Van Dijke et al., 2012). The position as certifying party can be taken over by various entities, such as a government, commercial enterprises (Sporleder & Goldsmith, 2001), or third-parties (Anders et al., 2010). This paper defines a third-party as an "Independent Organisation with expertise to provide an assessment and verification of the company's compliance with standards and/or legal requirements" (Tanner, 2000, p. 415). However, research has found diverging results of which certification authority is the most suitable entity for influencing consumer behavior. For example, while Lytton (2014) argued that third-party certification is superior to government certification, Ortega et al. (2011) found that the willingness-to-pay among Chinese consumers is higher for government-certified food compared to third-party-certified nutrition. Moreover, Atkinson and Rosenthal (2014) showed that consumers have more trust in government than in corporate certification, but only for low-involvement products. Nöteberg et al. (2003), however, did not detect significant differences between various possible certifying institutions, such as accounting companies, banks, or firms in the computer industry. Yet, although the question about the most suitable certification authority remains open, several authors agree that certification is superior to no certification with regard to the influence on consumer behavior (Rifon et al., 2005; Yang et al., 2006). Based on these findings, this paper advances two propositions. First, certification is superior to no certification in influencing human behavior, independently of which entity serves as the certification authority. Second, it is hypothesized that in the case of smart product data, as analyzed here, certification by an independent third-party is superior to certification by any other entity regarding the effect on consumers' feelings and behaviors. This is based on the

assumption that consumers might fear that their personal information is more likely to be misused by smart product manufacturers, governments, or other commercial entities compared to an independent third-party, which endeavors to safeguard consumer data privacy.

To date, numerous studies on how certification influences consumers' psychological processes and behaviors have been conducted, mainly with favorable results. Examples include the positive effect of certification on purchase intention (Kamins & Marks, 1991; Nöteberg et al., 2003; Özpolat et al., 2013; Zhang, 2005), satisfaction (Park et al., 2010), brand image (Martínez Caro & Martínez García, 2009), and perceived product quality (Houston & Taylor, 1999; Wu et al., 2014). On the negative side, certification has been found to have no effect on purchase intention (Bahmanziari et al., 2009). Results also diverge regarding the influence of certification on trust. While numerous studies have found evidence for the positive impact of certification on trust (Chang et al., 2013; Kaplan & Nieschwietz, 2003; Kim & Kim, 2011; West, 2015; Yang et al., 2006), trusting intentions (Sha, 2009), and perceived trustworthiness (Lee et al., 2004; Portz et al., 2001), some have not confirmed this effect with regard to trust (Bahmanziari et al., 2009; Kim et al., 2008; Kimery & McCord, 2002; McKnight et al., 2004) and trusting beliefs (Yousafzai et al., 2005). In sum, even though the results regarding the influence of certification on trust are not unanimous, the literature has mostly reported a positive relationship between the two variables. This positive influence of certification on trust is also postulated in this paper.

However, certification as it has been performed in the past, will not be suitable in a digitalized future. While some researchers have suggested that certification should best be continuously executed in a flexible and dynamic environment, such as cloud computing (Windhorst & Sunyaev, 2013), others have proposed installing a third-party auditor between a data owner and a cloud service provider to audit the data stored in the cloud (Vanitha & Raju, 2013). In a similar direction, Katopodis et al. (2014, p. 394) argued for a "hybrid approach for certifying security properties of cloud services that combines monitoring and testing data." One conclusion from these results is that in fast-changing environments, data should be audited continuously by a third-party. This might not only apply to cloud services, but also to other types of digital technologies, such as smart products. In this paper, smart devices are described as "products that are equipped with intelligence-generating technologies including (i) *sensors* and/or *actuation*, either to gather data from the environment or to use the data to change the environment, (ii)

computing power for data analysis, and (iii) optional *interfaces* to exchange information with their environment" (Dawid et al., 2017, p. 204). As this definition implies, smart products rely heavily on data for their functionality and act autonomously in their decision-making (Rijsdijk & Hultink, 2003). In this regard, Dinmohammadi et al. (2018) pointed out that especially autonomous systems need strong certification techniques. In sum, these studies indicate that the certification market for digital products is about to change. At the same time, this means that new certification approaches for smart (and autonomous) products are necessary, such as the approach introduced and evaluated here (see below).

Data disclosure

Along with the increasing success of smart products in recent years, the amount of consumer data collected by companies has continuously risen (Cukier & Mayer-Schoenberger, 2013). Consumers are highly concerned about this (Norman et al., 2016), as these data collections may invade their data privacy (Pinchot et al., 2018). For the purposes of this paper, data privacy is defined as "the concept that personally identifiable information (PII) and other data about an individual should only be accessible to authorized parties" (Pinchot et al., 2018, p. 92). To mitigate their fears, companies should endeavor to show consumers that they will address their privacy concerns and will use their data responsibly (Hui et al., 2007).

To date, numerous factors have been found to positively influence consumers in deciding to share their data with companies, for example, loyalty clubs (Mazurek & Małagocka, 2019; Sayre & Horne, 2000), financial rewards (Benndorf & Normann, 2018; Derikx et al., 2016; Hann et al., 2007), perceived value and satisfaction (Leppäniemi et al., 2017), reciprocity (Acquisti et al., 2012; Happ et al., 2016; Moon, 2000), the number of data recipients (Schudy & Utikal, 2017), reasons for data collection (Zimmer et al., 2010), and the data retention period (Leon et al., 2013). Apart from this, the willingness to share information is influenced by the data-receiving organization (Roeber et al., 2015; Seifert et al., 2018), the type of information (Leon et al., 2013; Milne et al., 2012; Phelps et al., 2000; Prince, 2018; Ward et al., 2005), the sensitivity of the information (Lwin et al., 2007), and the context (John et al., 2011). Moreover, trust was frequently found to increase consumers' willingness to disclose information (Chellappa & Sin, 2005; Lauer & Deng, 2007; Milne & Boza, 1999; Milne & Culnan, 2004; Schoenbachler & Gordon, 2002; Tessem & Nyre, 2013). Nam et al.

(2006, p. 216) also concluded that displaying "privacy-related certificates and logos conferred by credible third-party organizations" on a website to increase consumer trust improves data quality and quantity. In addition, certification influences people's beliefs about privacy as well as their willingness to share data (Aiken & Boush, 2006). The last result is also supported by Wang et al. (2004).

Furthermore, apart from wanting to protect their privacy, consumers are also demanding control over their information (Liu et al., 2005; Phelps et al., 2000). According to some research, consumers should be able to decide which data they wish to share with whom in which situations, at which locations, and from which activities (Hull et al., 2004). Hence, consumers should be able to block or limit access to their data (Hull et al., 2004). Various solutions to meet these demands from consumers have been proposed. Truong et al. (2016), for example, suggested a trust service platform for smart city data that offers features such as data access control and data monetization. The platform also enables controlling and adapting data sharing depending on the environment (Truong et al., 2016). Similarly Cao et al. (2020, 2016, 2015) recommended an Internet-of-Things platform, which makes it possible to track the usage of consumer data (Cao et al., 2016) and provides all stakeholders with control over how their data is used (Cao et al., 2020). The platform is intended to improve transparency (Cao et al., 2020) and to motivate consumers to share their data (Cao et al., 2016). Other authors have described a similar approach for websites (Xu et al., 2012) and mobile apps (Brandtzaeg et al., 2019).

This paper combines these approaches with the need for dynamic certification in the fast-changing environments described above. It introduces an extended certification authority, similar to the "Bank of Individuals' Data" proposed by Moiso and Minerva (2012, p. 202), and analyzes its influence on consumer behavior. According to these authors, such entities allow consumers to collect and store their data securely and enable them to decide with which parties they want to share their data and under what conditions (Moiso & Minerva, 2012). Moreover, this intermediary executes several functions such as "data certification, accountability on data usage, data usage policy enforcement" (Moiso & Minerva, 2012, p. 204). The data are collected automatically from various sources, such as smart products and mobile devices (Moiso & Minerva, 2012). However, only scarce empirical evidence exists for this kind of intermediaries between consumers and companies. This paper therefore proposes introducing a certification authority in-between the data transfer process from a smart product to the respective manufacturer. This entity would not only guarantee data privacy and proper

data handling, and execute security measures. It would also provide secure storage for the collected information. Moreover, prior to the smart product data being transferred onwards from the certification authority to the manufacturer, they would be anonymized and the consumer could decide (via personalized settings) who should receive which data, in which condition, and in which case.

Based on the findings in the literature described above, this paper suggests that the existence of such a certification authority influences consumers' willingness to share information with the manufacturer, with this process being mediated by trust in data privacy. As inferred from the above results, the role of the certification authority should best be assumed by an independent third-party. For not only should this lead to the highest trust in data privacy but also to the greatest willingness to share information compared to any other entity and compared to no certification.

Trust in smart products

Trust, an important aspect in many areas of life, has been found to influence the use and acceptance of technological products (Choi & Ji, 2015; Lee & See, 2004). In its most general form, trust has been defined as "a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another" (Rousseau et al. 1998, p. 395). In both the offline and the online context, trust has frequently been divided into several dimensions. Offline distinctions include, for example, affect- and cognition-based trust (McAllister, 1995), calculus-, knowledge-, and identification-based trust (Lewicki & Bunker, 1996), or calculative, relational and institutional trust (Rousseau et al., 1998). In the online context, for example, Beldad et al. (2011) distinguished two dimensions of trust. Those refer to the "organization's ability to protect users' personal information from unwarranted external intrusion and its motivation and intention to protect and to respect collected pieces of personal information considering the organization's ability to abuse them" (Beldad et al., 2011, p. 224). A further differentiation is the separation of trust into soft and hard trust (Head et al., 2001; Head & Hassanein, 2002). While hard trust concerns technological solutions for safe interaction, soft trust refers to trust in data privacy (Head et al., 2001; Head & Hassanein, 2002). Head and Hassanein (2002, p. 310) cautioned that "issues of "soft trust" cannot be as easily resolved through the application of technology solutions" such as those of hard trust. Based on this distinction, this paper differentiates between trust in the smart product itself, referring to the technical functionality and safety of the

product (following the definition of hard trust) and trust in data privacy, referring to the sensible handling of consumer data and the protection of their privacy (following the definition of soft trust).

However, while certification is supposed to increase consumers' trust in their data privacy in this paper, their trust in the smart product itself might interact in an adverse way with the effect of certification on the willingness to share information. Thus, the existence of a certification authority is only supposed to be beneficial with regard to the willingness to share data when consumers have low trust in their smart product. As, in this case, consumers might feel that their data are not safe with the smart product, certification will increase their feeling of data privacy, which in turn makes them more willing to share their information. In contrast, if consumers have high trust in the smart product, and if their data are certified at the same time, their willingness to provide information is hypothesized to decrease in this paper. This decreasing willingness to share data supposedly stems from consumers' feeling that their data are safe with their smart product. Thus, an additional entity (i.e., the certification authority) that has access to consumer data via the data transfer and certification process (and hence is potentially able to misuse the data) is considered unnecessary by consumers. Consequently, consumers' willingness to provide information decreases. This assumption is also supported by Schudy and Utikal (2017), who found that the larger the number of entities receiving personal data, the less consumers are willing to provide information. Moreover, certification is not always beneficial but may also be detrimental under certain conditions (Holland, 2016).

Summary and hypotheses

This paper proposes the existence of a data certification authority between a smart product and the respective manufacturer as a means of positively influencing consumer behavior. Based on findings in the literature, data certification is hypothesized to be superior to no certification (i.e., a direct data transfer from the smart product to the respective manufacturer) in terms of higher trust in data privacy and greater willingness to share data, independently of which entity conducts certification. Among various certification authorities, however, an independent third-party is considered to be best suited compared to commercial or governmental entities and compared to no certification. Moreover, certification has been found to positively influence trust, which, in turn, has been shown to increase a person's willingness to share information. Thus,

the effect of data certification by an independent third-party (supposedly the most suited certification authority) on the willingness to share data with the manufacturer is assumed to be mediated by the consumer's trust in data privacy. These relations are described formally in hypotheses H1a, H1b, and H2:

H1a: The certification of smart product data by any certification authority (irrespectively of whether an independent third-party, a government, or a commercial entity assumes this role) is superior to no certification in terms of higher trust in data privacy and greater willingness to share data.

H1b: An independent third-party is a superior data certification authority compared to a government and a commercial entity in terms of higher trust in data privacy and greater willingness to share data.

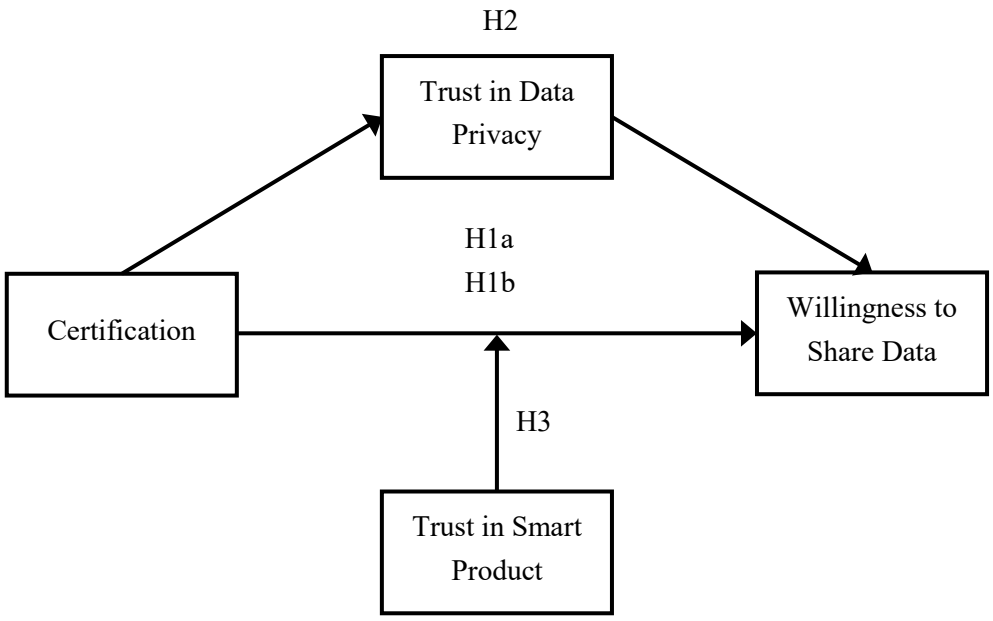
H2: The effect of certification of smart product data by an independent third-party on the willingness to share data is mediated by trust in data privacy.

However, certification of smart product data is supposedly only beneficial in certain cases. As explained above, data certification is only hypothesized to be necessary if consumer trust in the smart product is low. In this case, consumers feel that certification benefits them in terms of a higher data privacy protection. Thus, they should be more willing to share information compared to a direct data transfer (i.e., no certification). On the other hand, if consumers sufficiently trust their smart product, certification might be seen as unnecessary and consumers might be less willing to provide personal information, as they feel that their data are already safe with their respective smart product. Based on this argumentation, H3 is proposed:

H3: While third-party certification increases the willingness to share data for low levels of smart product trust, it decreases the willingness to share data for high levels of smart product trust.

The conceptual model in Figure 1 summarizes the theoretical hypotheses:

Figure 1: Conceptual model of the influence of certification on the willingness to share data



Overview of studies

A pilot study and three experiments were carried out to test the above-derived hypotheses. The pilot study explored consumers' opinions of data privacy and their views on the idea of employing a certification authority for smart product data certification. The first experiment was designed to compare the ability of different certification authorities (i.e., a government, a commercial entity, and an independent third-party) to increase consumers' trust in data privacy and to influence their willingness to share data. Moreover, the mediating role of trust in data privacy was explored. On this basis, the second experiment analyzed whether the results of the first experiment can be reproduced when using a different smart product category. The third and last experiment explored a boundary condition of when third-party certification is effective in enhancing people's willingness to disclose information and when it negatively influences their willingness to share data. All four studies were conducted with German participants. Respondents for the three online studies (pilot study and studies 1 and 2) were recruited via a market research agency. These participants represented the German population in terms of age and gender. Each respondent took

part in only one of the online studies; participating multiple times was not possible. For an overview of the four studies, see Table 1.

Table 1: Overview of the four studies

	Data collection	**Design**	**Product**	**Hypothesis testing**	**Results**
0	Online survey (N = 606, 50% female, M_{age} = 41.61)	Survey	Smart products	-	- Study shows the importance of data privacy for consumers - Evidence for the idea of a certification authority and for the willingness to share data is ambiguous - Independent third-party as the most suitable certification authority
1	Online experiment (N = 651, 50% female, M_{age} = 42.30)	Four-condition between-subjects design (no certification vs. third-party certification vs. government certification vs. commercial enterprise certification)	Smart speaker	H1a, H1b, H2	- **H1a rejected**: Certification is not superior to no certification with regard to increased trust in data privacy and greater willingness to share data. - **H1b rejected:** An independent third-party is not a superior certification authority compared to any other entity. - **H2 accepted**: Trust in data privacy mediates the effect of certification on the willingness to share data.
2	Online experiment (N = 558, 50% female, M_{age} = 42.32 years)	Two-condition between-subjects design (no certification vs. third-party certification)	Smart-phone	H2	- **H2 accepted.**
3	Laboratory experiment (N = 75, 31% female, M_{age} = 24.31 years)	Two-condition between-subjects design (no certification vs. third-party certification)	Smart-phone	H2, H3	- **H2 rejected.** - **H3 accepted**: While third-party certification increases the willingness to share data for low levels of smart product trust, it decreases the willingness to share data for high levels of smart product trust.

Pilot study

The pilot study was exploratory and served the purpose to analyze how and under which conditions consumers are willing to share their data. It also investigated consumers' opinions on data privacy and on the existence of a certification authority for smart product data certification.

Method

Participants and design

The online study was conducted with a total of 606 German participants (50.00% female, $M_{age} = 41.61$ years). To be admitted to the study, participants had to own at least a smartphone as a smart product.

Materials and procedure

The pilot study examined consumers' opinions of smart products in terms of attitude (7-point scale from 1 = "very negative" to 7 = "very positive": "How would you describe your attitude toward your smart product(s)?"), satisfaction (7-point scale from 1 = "not at all satisfied" to 7 = "very satisfied": "How satisfied are you with your smart product(s)?"), and trust (7-point scale from 1 = "trust not at all" to 7 = "fully trust": "How much do you trust your smart product(s)?"). Moreover, the importance of data privacy (7-point scale from 1 = "not important at all" to 7 = "very important": "How important is the protection of your personal data to you?") and respondents' awareness of privacy practices was evaluated (three items adapted from Malhotra, Kim and Agarwal, 2004; 7-point scale from 1 = "strongly disagree" to 7 = "strongly agree": "1. Companies using information from smart products should disclose the way the data are collected, processed, and used"; "2. A good consumer online privacy policy should have a clear and conspicuous disclosure"; "3. It is very important to me that I am aware and knowledgeable about how my personal information will be used"; Cronbach's $\alpha = .84$).

In addition, respondents were asked to indicate their willingness to share the data from their smart product(s) (7-point scale from 1 = "not willing at all" to 7 = "very much willing": "How willing are you to share the data from your smart product(s)?"). Moreover, they were requested to give their opinion on how suitable they deemed each of the seven entities suggested for the role of the certification authority (7-point scale from 1 = "not at all suitable" to 7 = "very suitable": "How suitable do you deem each of

the below-listed entities for the role of the certification authority?"). The certification authorities to be evaluated were a cloud service provider, a start-up company, a technology company, a software company, a government, an independent third-party, and a university. Furthermore, respondents' trust propensity was investigated (three items from Cheung and Lee, 2003, one item deleted from the original scale, 7-point scale from 1 = "strongly disagree" to 7 = "strongly agree": "1. It is easy for me to trust a person/thing"; "2. My tendency to trust a person/thing is high"; "3. I tend to trust a person/thing, even though I have little knowledge of it"; Cronbach's α = .91).

Results

In general, participants had a positive image of smart products ($M_{attitude}$ = 5.10, $M_{satisfaction}$ = 5.49, M_{trust} = 4.92). They stated that data privacy was very important to them ($M_{dataprivacy}$ = 6.08) and that their awareness of privacy practices was high ($M_{privacypractices}$ = 5.84). However, their willingness to share data was rather low ($M_{sharedata}$ = 2.95). The participants exhibited moderately varying preferences for the suggested certification authorities, with the independent third-party being the most preferred authority ($M_{startup}$ = 3.38, $M_{technology}$= 3.47, $M_{cloudserivce}$ = 3.52, $M_{software}$ = 3.68, $M_{government}$ = 3.81, $M_{university}$ = 4.31, $M_{thirdparty}$ = 4.43). A repeated measures analysis of variance (ANOVA) showed significant differences in the evaluation of the proposed certification authorities ($F(6, 3630) = 88.19$, $p < .001$, $\eta_p^2 = .13$). A post-hoc test using a Bonferroni correction with alpha-adjustment revealed that even though no significant difference existed between an independent third-party and a university in terms of suitability as a certification authority, respondents preferred both parties significantly more as certification authorities than any of the other five evaluated entities (i.e., a cloud service provider, a start-up company, a technology company, a software company, and a government; $p_{university\_thirdparty}$ = .60; $p_{university}$ < .001 and $p_{thirdparty}$ < .001 for the comparison between the university or the third-party and any other suggested entity respectively; for a full comparison of all evaluated entities, see Appendix A). However, preferences for the other five possible certification authorities were less clear-cut. Moreover, participants' trust propensity was neither high nor low ($M_{trustpropensity}$ = 3.80).

In the next step, a correlational analysis was conducted. The results were as follows (for a full correlation table, see Appendix B): A positive image in terms of attitude toward, satisfaction with, or trust in a smart product was significantly correlated with the willingness to share data ($r_{attitude*sharedata}(604)$ = .32, $r_{satisfaction*sharedata}(604)$ = .18,

$r_{trust*sharedata}(604) = .41$, $p < .001$ for all three correlations). While trust propensity was positively correlated with the willingness to share data ($r_{trustpropensity*sharedata}(604) = .47$, $p < .001$), the importance of data privacy and the awareness of privacy practices were both negatively correlated with the willingness to share data ($r_{dataprivacy*sharedata}(604) = -.26$, $p < .001$, $r_{privacypractices*sharedata}(604) = -.23$, $p < .001$). Apart from the independent third-party as a certification authority, the values for the suitability of all other evaluated certification entities were significantly negatively correlated with the importance of data privacy ($r_{thirdparty*dataprivacy}(604) = -.06$, $p = .12$). Additionally, the willingness to share data was positively correlated with the evaluation of an independent third-party as a certification authority ($r_{thirdparty*sharedata}(604) = .33$, $p < .001$). However, this was also true for the other six entities evaluated as possible certification authorities, and partially even more strongly so.

Discussion

The average value for the willingness to share data shows that respondents were not very inclined to do so. One reason for this reluctance might be that people highly value data privacy. Moreover, participants who highly value data privacy are less likely to share their data. A somewhat surprising finding is that apart from an independent third-party, all other entities evaluated as possible certification authorities were correlated negatively with the importance of data privacy. Thus, only persons who did not perceive data privacy as important evaluated these entities as suitable certification authorities. While this might indicate that consumers are not strongly interested in an additional entity becoming involved, it is positive news in that an independent third-party might be a viable option as a certification authority, as suggested by H1b. Furthermore, the independent third-party was evaluated as the most suitable certification authority, along with the university (which might also be seen as independent). The government and all evaluated commercial entities (i.e., a cloud service provider, a start-up company, a technology company, and a software company) followed significantly behind. Based on the results from the repeated measures ANOVA and the post-hoc test, the independent third-party (as the entity with the higher average value for suitability as a certification authority compared to the university), a government, and a commercial entity (as a generalization of the various companies analyzed) were selected for further evaluation as possible certification authorities in the subsequent study (Study 1).

Moreover, preliminary support for H2 is provided by the fact that the willingness to share data positively correlates with both an independent third-party as certification authority and trust propensity. However, the fact that the correlations are positive for the willingness to share data with all evaluated certification authorities casts doubt on the superiority of the independent third-party over all other entities taken into account in this study. In sum, the need for a certification authority in general, as well as the suitability of an independent third-party for this function, is inconclusive and needs to be evaluated further. Moreover, this study is limited by focusing on smart products in general rather than on a specific kind of device. The subsequent experiments address this limitation.

Study 1

Based on the ambiguous results of the pilot study, the first experiment had several purposes. One aim was to compare the three entities (an independent third-party, a government, and a commercial enterprise) established by the pilot study as a potential certification authority. Moreover, the experiment was used to find that entity best suited to increasing consumers' trust in data privacy and their willingness to share information with the smart product manufacturer. Another aim was to empirically analyze whether the effect of third-party certification on the willingness to share data is mediated by trust in data privacy. Formally, this study tested hypotheses H1a, H1b, and H2.

Method

Participants and design

Study 1 employed a four-condition between-subjects design. 651 participants took part in the online experiment (originally 653 participants, 49.77% female, M_{age} = 42.30 years). Participants were required to own a smart speaker, which was the focal product of the study. Two respondents were excluded from the analysis: One had not yet used his smart speaker and the other was no longer using it. Participants were randomly assigned to one of four study conditions: no certification authority (N = 163, control condition), an independent third-party as the certification authority (N = 156, a German testing, certification, and inspection company), the German government as the certification authority (N = 169), or a commercial enterprise based in Germany as the certification authority (N = 163, a technology company).

Materials and procedure

For the experimental manipulation, participants read a scenario description of how data were transferred from their smart speaker to the respective product manufacturer. In the control condition, a direct data transfer from the smart device to the manufacturer was described. The text explained that it was not entirely clear in which situation which types of data were transmitted, what the manufacturer used the data for, whether they were stored, passed on to partner companies, or anonymized, etc. Furthermore, it was not known whether the data were used for commercial purposes and whether any kind of security measures to protect the consumer information were in place. In the three experimental conditions, a certification authority acting as an intermediary in the data transfer process between the respondent's smart speaker and the respective product manufacturer was described. The certification authority was either an independent third-party, the government, or a commercial enterprise. After the data transfer from the smart speaker to the certification authority, data were anonymized, stored (e.g., for back-up), and checked for security (e.g., hacking or data manipulation). It was emphasized that data would not serve commercial purposes. Moreover, consumers could decide in personalized settings which of their data they agreed to being transferred onward, i.e., from the certification authority to the manufacturer (for full exemplary descriptions of the study scenarios, see Appendix C). After reading the respective scenario, respondents had to think about it for two minutes. Then, they had to submit their written opinion in an open text box. This procedure was followed to increase participants' engagement with the scenario and to elicit more in-depth consideration.

In the next step, participants were asked to indicate their willingness to share different kinds of data in each of the four study conditions. For each person, an average value was calculated based on whether they were willing to share 14 different kinds of data with the respective smart speaker manufacturer (on a 7-point scale from 1 = "not willing at all" to 7 = "very much willing": "How willing are you to share the types of data listed below from your smart speaker with the manufacturer?"; Cronbach's $\alpha = .96$). The types of data were media data (photos, videos, etc.), media usage (movies, music, books, etc.), personal data (biometrical data, relationship status, etc.), passwords and logins (for social media accounts, etc.), contact data (addresses, telephone numbers, etc.), messages (e-mails, text messages, etc.), location data (GPS data, mobility profiles, etc.), list of installed apps and app usage information (usage of apps in minutes, etc.), search history (search engines, etc.), connection data (call duration, etc.), health information (sport and sleep patterns, etc.), wireless connections used (Bluetooth, etc.), meetings (meeting

locations, travel information, etc.), and the usage of voice control and microphone (voice assistants, etc.). The types of data evaluated were based on various research (Leon et al., 2013; Sturgess et al., 2018; Zang et al., 2015) and extended and adjusted to fit smart product data categories. Participants were asked to add data types if they deemed some to be missing (in order to ensure completeness), but this was not the case. Participants' trust in data privacy was measured with three items (adjusted from Thomson, 2006; 7-point scale from 1 = "not at all" to 7 = "very much": "1. How much can you count on the fact that in the described scenario your data will only be used for the specified purpose, will not be passed on unauthorized, misused, or similar?"; "2. How much can you trust that in the described scenario your data will only be used for the specified purpose, will not be passed on unauthorized, misused, or similar?"; "3. How dependable do you consider it to be that in the described scenario your data will only be used for the specified purpose, will not be passed on unauthorized, misused, or similar?"; Cronbach's $\alpha = .94$).

Results

The average values for trust in data privacy and willingness to share information for each experimental group were computed for data analysis. A one-way ANOVA revealed that participants differed with marginal significance in their trust in data privacy ($F(3,647) = 2.23$, $p = .08$, $\eta_p^2 = .10$, $M_{control} = 3.62$, $M_{thirdparty} = 4.10$, $M_{government} = 3.88$, $M_{commercialenterprise} = 3.92$). A planned contrasts analysis showed that certification (by a third-party, a government, or a commercial enterprise) led to a significantly higher trust in data privacy compared to the control condition of no certification ($t(647) = 2.29$, $p = .02$). However, comparing the third-party certification authority with the other two entities (i.e., a government and a commercial enterprise) in terms of trust in data privacy with a planned contrasts analysis revealed no significant differences ($t(647) = 1.21$, $p = .23$). Regarding the willingness to share data, there was no significant difference across the four study conditions ($F(3,647) = .70$, $p = .55$, $\eta_p^2 = .003$, $M_{control} = 3.57$, $M_{thirdparty} = 3.79$, $M_{government} = 3.55$, $M_{commercialenterprise} = 3.64$).

In addition, a regression analysis was performed with the different certification conditions as the independent multi-categorical variables, trust in data privacy as the mediator, and willingness to share data as the dependent variable. PROCESS Model 4 was used for the analysis (Hayes, 2018; $N_{bootstrapping} = 5{,}000$; for the detailed regression results of studies 1-3, see Appendix D). While the relative total effects ($b_{totalthirdparty} =$

.22, SE = .18, 95% CI = [-.14, .57], $b_{totalgovernment}$ = -.02, SE = .18, 95% CI = [-.37, .33], $b_{totalenterprise}$ = .07, SE = .18, 95% CI = [-.28, .43]) and the relative direct effects ($b_{directthirdparty}$ = -.11, SE = .13, 95% CI = [-.37, .14], $b_{directgovernment}$ = -.20, SE = .13, 95% CI = [-.45, .04], $b_{directenterprise}$ = -.14, SE = .13, 95% CI = [-.39, .11]) were not significant for any party, trust in data privacy was found to mediate the effect of certification on the willingness to share data in the independent third-party certification condition ($b_{indirectthirdparty}$ = .33; SE = .13, 95% CI = [.09, .59]). However, this mediating relationship was found neither for the government ($b_{indirectgovernment}$ = .18, SE = .13, 95% CI [-.07, .44]) nor for the commercial enterprise ($b_{indirectenterprise}$ = .21, SE = .13, 95% CI [-.04, .47]).

Discussion

Based on the results of the pilot study, Study 1 aimed to analyze different entities for their suitability as a certification authority. The data analysis shows that certification is superior to no certification regarding a significantly higher trust in data privacy. However, no differences in the willingness to share data were found between the four experimental groups. Thus, H1a has to be rejected. This is also true for H1b: Even though the means for trust in data privacy as well as for the willingness to share data were both highest in the case of the independent third-party as a certification authority compared to the other study conditions, the differences were not significant. Moreover, the data analysis shows that the effect of data certification by an independent third-party on the willingness to share data is mediated by trust in data privacy. This leads to the acceptance of H2. This mediation is indirect-only, as the indirect effect was significant, contrary to the direct effect (Zhao et al., 2010). In this case, the existence of an omitted mediator is unlikely (Zhao et al., 2010). In sum, based on the results of the data analysis, the independent third-party was employed as the data certification authority in the following two experimental studies, even though the results are not completely unambiguous.

Study 2

Study 2 aimed to verify and re-examine the results of Study 1 with regard to H2 with a different product group—a smartphone instead of a smart speaker.

Method

Participants and design

Study 2 employed a two-condition between-subjects design. 558 participants took part in the experimental online study (originally 559 participants, 50.18% female, M_{age} = 42.32 years). One participant was excluded from the data analysis, as he had stated in the feedback section of the online study that he had not read the scenario description. Respondents were randomly assigned to one of the two study conditions: no certification authority (N = 276, control condition) or an independent third-party as a certification authority (N = 282, a German testing, certification, and inspection company).

Materials and procedure

The setup of Study 2 and the two study scenarios (no certification vs. third-party certification) were analogous to Study 1. The questions employed to measure respondents' trust in data privacy (Cronbach's α = .94) and their willingness to share data (Cronbach's α = .95) were adopted from Study 1.

Results

In line with the results of Study 1, participants in the third-party certification condition had higher trust in data privacy compared to those in the control condition ($t(556)$ = 2.74, p = .006, d = .23, $M_{control}$ = 3.29, $M_{thirdparty}$ = 3.64). However, there was no difference in the willingness to share data between the two study conditions ($t(556)$ = .22, p = .83, d = .02, $M_{control}$ = 3.03, $M_{thirdparty}$ = 3.00).

Additionally, a regression analysis with certification as the independent variable, trust in data privacy as the mediator, and willingness to share data as the dependent variable was conducted (PROCESS Model 4; Hayes, 2018; $N_{bootstrapping}$ = 5,000). The results show that the effect of third-party certification on the willingness to share data was mediated by trust in data privacy ($b_{indirect}$ = .21, SE = .08, 95% CI = [.06, .36]). While the total effect was not significant (b_{total} = -.03, SE = .12, 95% CI = [-.26, .21]), the direct effect was statistically significant (b_{direct} = -.23, SE = .09, 95% CI = [-.41, -.05]).

Discussion

The results of Study 2 confirm the preliminary results of Study 1. This experiment showed that data certification increases consumers' trust in data privacy, but not their willingness to share data. Moreover, the effect of third-party certification on the willingness to share information is mediated by trust in data privacy. Thus, H2 is accepted. However, according to the classification of Zhao et al. (2010), this mediation is a competitive mediation and points toward an omitted mediator. This contrasts with Study 1, which found evidence for an indirect-only mediation, where an omitted mediator is unlikely (Zhao et al., 2010). Thus, the mediating effect of trust in data privacy should be studied further. This was done, among others, in Study 3. Another point that needs clarification is the fact that the willingness to share data is not only not statistically different in studies 1 and 2 respectively, but even slightly lower in the experimental than in the control condition in Study 2. This fact was also taken into account in Study 3. The third experiment analyzed the possibly ambiguous effect of certification on the willingness to share information, thereby serving as an initial indication of the feasibility of implementing a data certification authority for smart products.

Study 3

Based on the equivocal results of the two previous experiments regarding the willingness to share data, Study 3 analyzed whether a boundary condition exists when the presence of an independent third-party certification authority increases the willingness to share data and when it does not. In this regard, Study 3 tested whether strong trust or distrust in a product may negatively influence the effect of third-party certification on consumers' willingness to share data. A laboratory experiment was used to test this relationship, formally described by H3. In addition, Study 3 continued the analysis of the mediating effect of trust in data privacy.

Method

Participants and design

Study 3 employed a two-condition between-subjects design (no certification authority vs. an independent third-party as certification authority). Seventy-six participants originally took part in the computer-based laboratory study conducted at a Swiss university. One participant was excluded from the analysis as he had mistakenly closed

the survey window on the computer and had to restart the study—producing different answers in each round. The final sample consisted of 75 participants (30.67% female, M_{age} = 24.31 years) with 37 participants in the control condition and 38 participants in the experimental condition. The same German testing, certification, and inspection company as in studies 1 and 2 was employed as the data certification authority in Study 3. Participants had to have grown up in Germany to be eligible for the laboratory experiment. This was done to keep nationality constant across the four studies. The focal product of the experiment was a smartphone, as in Study 2.

Materials and procedure

The study was conducted in the experimental laboratory of a Swiss university close to the German border, thereby ensuring a sufficient number of German nationals as participants. When arriving at the laboratory, participants were welcomed and received details about the course of the experiment. Respondents had to sign a form of consent in order to be allowed to participate in the study. Before the experiment began, open questions from the participants were answered. The study did not pose any physical or psychological risks to respondents at any time. Next, participants took part in the computer-based experiment on their own in a separate room. Apart from small differences, the setup and the study scenarios of the third study were analogous to studies 1 and 2. For example, the specific smartphone brand of the participants was named in the scenario descriptions compared to the prior studies, where only the generic formulation "manufacturer" was used. This was due to the fact that participants could be asked for their smartphone brand when entering the experimental laboratory and thus, the scenarios could be personalized. However, with the online experiments in studies 1 and 2, this had not been possible. Participants were also told before the study by the experimenter as well as on-screen during the experiment that their decision to share a certain type of data would be consequential and that they would have to provide this information at a later stage of the experiment. The aim was to give participants the impression that their decisions were consequential, thereby encouraging them to thoroughly consider their willingness to share a particular type of data. However, for ethical reasons as well as for reasons of data privacy, participants were not really asked to provide the types of data for which they had indicated a willingness to share. This was also made clear in the debriefing at the end of the study. Trust in data privacy (Cronbach's α = .90) and willingness to share data (Cronbach's α = .90) were assessed

analogously to Studies 1 and 2. Participants' trust in the smart product—more specifically, in their smartphone in Study 3—was assessed with a single line item on a 7-point scale (from 1 = "trust not at all" to 7 = "fully trust": "How much do you trust your smartphone?").

Results

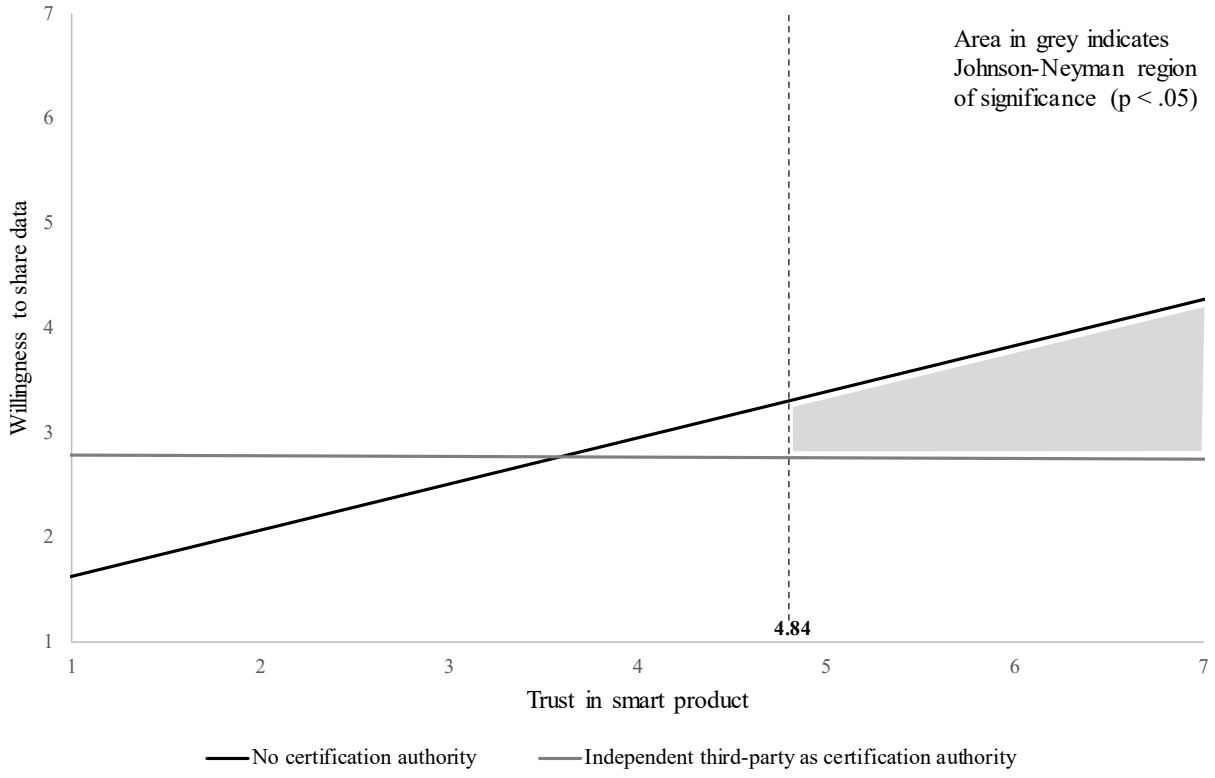
As in Study 2, there was a significant difference in trust in data privacy between the two experimental conditions ($t(73) = 4.10$, $p < .001$, $d = .95$, $M_{control} = 2.63$, $M_{thirdparty} = 3.86$), but not with regard to the willingness to share data ($t(73) = 1.35$, $p = .18$, $d = .31$, $M_{control} = 3.18$, $M_{thirdparty} = 2.84$).

PROCESS Model 5 (Hayes, 2018; $N_{bootstrapping} = 5{,}000$) was used for the regression analysis, with certification as the independent variable, trust in data privacy as the mediator, trust in the smart product as the moderator on the path from certification to the willingness to share data, and willingness to share data as the dependent variable. While the existence of a third-party certification authority had a significantly positive effect on trust in data privacy ($b_{certification\_trustdataprivacy} = 1.23$, SE = .30, 95% CI = [.63, 1.84]), higher trust in data privacy did not lead to greater willingness to share data ($b_{trustdataprivacy\_willingnesstoshare} = .12$, SE = .10, 95% CI = [-.08, .31]). Moreover, trust in data privacy did not mediate the effect of certification on the willingness to share data ($b_{indirect} = .15$, SE = .15, 95% CI [-.11; .46]). Thus, H2 has to be rejected, contrary to the results of studies 1 and 2. Moreover, the regression results revealed a non-significant effect of certification on the willingness to share data ($b_{certification\_willingnesstoshare} = 1.60$, SE = 1.12, 95% CI = [-.63, 3.83]), but a significantly negative effect of trust in the smart product on the willingness to share data ($b_{trustsmartproduct\_willingnesstoshare} = -.44$, SE = .16, 95% CI = [.12, .75], $M_{trustsmartproduct} = 4.81$). Additionally, there was a significant certification*trust in the smart product interaction effect ($b_{interaction} = -.44$, SE = .22, 95% CI = [-.88, .00]). Thus, trust in the smart product moderated the effect of certification on the willingness to share data. The Johnson-Neyman technique (Hayes & Matthes, 2009; Johnson & Neyman, 1936) revealed that the presence of a certification authority significantly decreases participants' willingness to share data if the value for trust in the smart product is higher than or equal to 4.84 ($p < .05$, see Figure 2).

For all calculations in Study 3, participants' smartphone brand was included as a control variable (with 1 = iPhone from Apple, 0 = other smartphone brand). This is due to the fact that the majority of study participants owned an iPhone; such persons often exhibit

especially high brand attachment and have a high opinion of the brand (Schmalz & Orth, 2012).

Figure 2: Johnson-Neyman technique



Discussion

In line with Study 2, participants in Study 3 differed with regard to their trust in data privacy, but not with regard to their willingness to share data. Moreover, even though the difference was not statistically significant, the willingness to share data was lower in the certification compared to the control condition, as also indicated in Study 2. As hypothesized, the regression results show that in situations involving high product trust, participants were less willing to share data in the case of certification compared to no certification. Moreover, in the case of low product trust, the existence of a certification authority increased participants' willingness to share data. Thus, H3 was accepted. However, these results contrast with the findings of Aiken and Boush (2006), Nam et al. (2006), and Wang et al. (2004), who all concluded that certification increased consumers' willingness to share information.

Further, trust in data privacy could not be confirmed as the mediator from certification on the willingness to share data in this study, in contrast to the two prior experiments—leading to the rejection of H2. Thus, this result does not help to resolve the conflicting evidence for the indirect-only and competitive mediation found in studies 1 and 2 respectively. Instead, it emphasizes the need for further research. This also applies to whether and how trust in data privacy and trust in the smart product relate to and influence one another and how this possible interaction affects the willingness to disclose information. In sum, the results of Study 3 suggest that differences in trust in data privacy—due to the absence or presence of a certification authority—do not help to explain why trust in the smart product impacted the willingness to share data differently in the certification and in the no certification condition. However, when interpreting the results of Study 3, some limitations have to be kept in mind. These include the small sample size per study condition and the fact that compared to the other two experimental studies described here, participants were asked to remember that they would need to share certain types of data at the end of the study if they had previously indicated their willingness to do. This requirement might have manifested in a lower average willingness to share data compared to studies 1 and 2 and might also have impacted the statistical results, at least to some degree.

Overall, the results of Study 3 indicate that consumers strongly trusting their smart product do not need additional control entities, such as a data certification authority. The reason for this might be that an independent third-party certification authority would be an additional entity that receives consumer data and that could use, distribute, or abuse these data. Participants' open text comments support this notion. For instance, "Basically, I don't see a big benefit in having my data stored with another instance. It seems to me that this would unnecessarily complicate the data privacy situation." Or: "While this would seem to ensure a higher level of data privacy, I see the danger of adding another weak spot where the data could be accessed unauthorized" (both comments translated from German). This is also in line with findings in the literature, according to which more data recipients lead to a lower willingness of consumers to disclose information (Schudy & Utikal, 2017). Thus, in sum, installing a third-party certification authority for smart product data certification should be well considered and thoroughly evaluated to avoid possible detrimental effects for manufacturers.

General Discussion

This paper has explored whether the approach proposed in various forms in the literature—i.e., to install a certification authority in-between the data transfer process from a smart product to the respective manufacturer—might be used to increase both consumers' trust in data privacy and their willingness to share data. This idea, along with the question of which entity would be a suitable data certification authority, was investigated in four empirical studies. Moreover, the role of trust in data privacy as the mediator of the effect of certification on the willingness to share information was explored. Further, a boundary condition of when certification positively or negatively affected the willingness to disclose information was analyzed.

The statistical analysis showed that an independent third-party is the most suitable certification authority. However, the results concerning the decision of whether or not to implement a certification authority for data certification in order to positively influence consumer behavior are ambiguous. While the existence of an independent third-party for data certification significantly increased trust in data privacy, this effect could not be found regarding consumers' willingness to provide information. Further, while studies 1 and 2 support the hypothesis of trust in data privacy mediating the effect of third-party certification on the willingness to share information, this could not be confirmed in Study 3. Moreover, the results of this last study revealed that third-party certification does not only not increase the willingness to share consumer data, but can even be detrimental to companies if the level of consumer trust in a smart device is high. In this case, consumers are less inclined to share data if a certification intermediary exists, as they perceive this as an additional entity that, in their opinion, unnecessarily has access to their information. Data certification was only found to increase the consumers' willingness to share information in the case of a low level of trust in the smart product, as third-party certification then provides consumers with an additional sense of data privacy.

Theoretical contribution

This paper contributes to the literature on signaling, certification, trust, data privacy and data disclosure. The issue of data privacy when using digital technologies has emerged as an important research topic in recent years in various literature streams, such as marketing or information systems. While consumers have been found to highly value their data privacy, evidence suggests that they can be persuaded to share their data in

exchange for rewards (Olivero & Lunt, 2004). The present paper has shown how and under which conditions certification as a signaling means influences consumers' willingness to share information in the context of smart products. As such, it provides first quantitative insights from a consumer behavior perspective. In the past, numerous signaling measures have been studied, with certification being one of them. With the continuous evolution of digitalization and the digital age, certification as a signaling means might once again attract attention after having long been successfully employed in many different industries.

As this paper and various others (e.g., Chang et al., 2013; Yang et al., 2006) have shown, certification is an important factor for creating trust. However, the relationship between the two types of trust analyzed here is not entirely clear with regard to several dimensions, such as the relation between these types of trust and certification, their influence on one another and on consumers' willingness to share information. In the literature, trust has been identified as one of the drivers of consumers' willingness to share data (e.g., Milne & Culnan, 2004; Schoenbachler & Gordon, 2002). This result, however, is only partially supported by the experimental studies reported here. Taken together, this paper shows that certification only increases consumers' willingness to share data under certain conditions—contrary to various other research results (e.g., Aiken & Boush, 2006; Wang et al., 2004).

Managerial implications

From a managerial perspective, installing a certification authority for smart product data certification to persuade consumers to disclose more data proves to be only partially successful. The fact that data certification was not found to increase consumers' willingness to share data, but even decreases it in certain cases, is detrimental for companies as it means that data certification does not necessarily provide manufacturers with access to an increased amount of consumer data. However, they need this information to generate income and develop new products, among others (Tao et al., 2019). Thus, companies should rather look for other ways of mitigating the tension between consumers wanting to protect their data and smart product manufacturers aiming to collect as much information as possible. One potentially fruitful approach compared to third-party certification is, for example, for companies to issue privacy statements (Hui et al., 2007).

In general, managers should thoroughly analyze whether their proposed measures not only benefit consumers in theory, but are also accepted by them and adjusted to their needs (Roeber et al., 2015). If not, such approaches, especially complex ones as the one introduced above, may have negative consequences for companies. For example, for the certification authority described here, two of the most frequent criticisms voiced in the feedback sections of the experiments were that the data transfer and certification process were too complex and that an additional party has access to the smart product data. This additional entity is especially critical as respondents often felt that transferring their data to the manufacturer was already too much. Another issue that raised skepticism among participants was who would pay for such a data certification service. In this direction, Moiso and Minerva (2012) found that only few consumers are willing to pay for using a similar entity to the one described above.

Moreover, companies currently active in the testing, inspection, and certification market should reconsider their opportunities within the field of data certification and data privacy protection, as their services only seem to add limited value for both companies and consumers. Further points to take into account include regulatory and legal challenges and the necessary agreement of manufacturers to transfer smart product data via a certification authority to them. As this would mean that companies thus lose their direct access to consumer data, obtaining their consent to this data transfer process will be a challenging task. In conclusion, implementing a data certification authority when transferring data between the smart product and the respective manufacturer is not entirely feasible. Companies might therefore choose to refrain from adopting this approach or, if they do, to at least combine it with other signaling measures.

Limitations and future research

This paper has analyzed German consumers' willingness to share personal information from their smart products with the respective manufacturers under the aspect of data certification. The results offer detailed insights into the effect of certification on consumer behavior in a digital, data-driven environment as well as into the general need for such a certification authority. Nevertheless, one of the major limitations of this paper is the geographical focus on Germany and the exclusion of any cross-country comparisons. However, differences between countries can be significant, as several authors have shown with regard to trust, the perception of third-party certification (Kim, 2008), and the willingness to share personal data (Gupta et al., 2010). Regarding the role

of the data certification authority, future studies are advised to consider other alternatives, such as non-governmental organizations. This is recommended because although the independent third-party was chosen as the certification authority in this paper, the evidence in this respect is equivocal, calling for more research and clarification.

An additional limitation concerns consumers' willingness to disclose information: When the willingness to share data was used as the dependent variable in the experimental studies reported here, an average value per person was computed across several types of data. However, previous research has found that the willingness to share data also depends on the type of data requested (Leon et al., 2013; Milne et al., 2012; Phelps et al., 2000; Prince, 2018; Ward et al., 2005) and on the sensitivity of the information (Lwin et al., 2007). Moreover, in the experiments reported above, trust in data privacy was analyzed as the mediating variable. However, the evidence if this variable is the only mediator is not clear-cut and partly also points toward the possibility of an omitted mediator. Possible examples of such an omitted mediator include perceived control (Hajli & Lin, 2016), perceived risk (Gupta et al., 2010; Lee et al., 2004), perceived value, or satisfaction (Leppäniemi et al., 2017). Moreover, as this is a rather new field of research in consumer behavior, it might be of interest to explore further possible boundary conditions around data certification and its effect on consumers' willingness to share information.

In sum, the research topics studied in this paper will evolve over time, as not only social structures and technological preferences are subject to change, but also the willingness to disclose information, as data will increasingly be seen as a good that can be used for exchange (Milne et al., 2012).

References

Acquisti, A., John, L. K., & Loewenstein, G. (2012). The impact of relative standards on the propensity to disclose. *Journal of Marketing Research*, *49*(2), 160–174. https://doi.org/10.1509/jmr.09.0215

Aiken, K. D., & Boush, D. M. (2006). Trustmarks, objective-source ratings, and implied investments in advertising: Investigating online trust and the context-specific nature of internet signals. *Journal of the Academy of Marketing Science*, *34*(3), 308–323. https://doi.org/10.1177/0092070304271004

Albersmeier, F., Schulze, H., Jahn, G., & Spiller, A. (2009). The reliability of third-party certification in the food chain: From checklists to risk-oriented auditing. *Food Control*, *20*(10), 927–935. https://doi.org/10.1016/j.foodcont.2009.01.010

Ali, J., & Kapoor, S. (2009). Understanding consumers' perspectives on food labelling in India. *International Journal of Consumer Studies*, *33*(6), 724–734. https://doi.org/10.1111/j.1470-6431.2009.00825.x

Anders, S., Souza-Monteiro, D., & Rouviere, E. (2010). Competition and credibility of private third-party certification in international food supply. *Journal of International Food and Agribusiness Marketing*, *22*(3), 328–341. https://doi.org/10.1080/08974431003641554

Atkinson, L., & Rosenthal, S. (2014). Signaling the green sell: The influence of eco-label source, argument specificity, and product involvement on consumer trust. *Journal of Advertising*, *43*(1), 33–45. https://doi.org/10.1080/00913367.2013.834803

Babula, E., Mrzygłód, U., & Poszewiecki, A. (2017). Consumers' need of privacy protection – Experimental results. *Economics & Sociology*, *10*(2), 74–86. https://doi.org/10.14254/2071-789X.2017/10-2/6

Bahmanziari, T., Odom, M. D., & Ugrin, J. C. (2009). An experimental evaluation of the effects of internal and external e-assurance on initial trust formation in B2C e-commerce. *International Journal of Accounting Information Systems*, *10*(3), 152–170. https://doi.org/10.1016/j.accinf.2008.11.001

Beldad, A., De Jong, M., & Steehouder, M. (2011). A comprehensive theoretical framework for personal information-related behaviors on the internet. *The Information Society*, *27*(4), 220–232. https://doi.org/10.1080/01972243.2011.583802

Benndorf, V., & Normann, H. (2018). The willingness to sell personal data. *The Scandinavian Journal of Economics*, *120*(4), 1260–1278. https://doi.org/10.1111/sjoe.12247

Bloom, P. N., & Reve, T. (1990). Transmitting signals to consumers for competitive advantage. *Business Horizons*, *33*(4), 58–66. https://doi.org/10.1016/0007-6813(90)90059-K

Brandtzaeg, P. B., Pultier, A., & Moen, G. M. (2019). Losing control to data-hungry apps: A mixed-methods approach to mobile app privacy. *Social Science Computer Review*, *37*(4), 466–488. https://doi.org/10.1177/0894439318777706

Cao, Q. H., Khan, I., Farahbakhsh, R., Madhusudan, G., Lee, G. M., & Crespi, N. (2016). A trust model for data sharing in smart cities. *Proceedings of the 2016 IEEE International Conference on Communications*, 1–7. https://doi.org/10.1109/ICC.2016.7510834

Cao, Q. H., Madhusudan, G., Farahbakhsh, R., & Crespi, N. (2020). Policy-based usage control for a trustworthy data sharing platform in smart cities. *Future Generation Computer Systems*, *107*, 998–1010. https://doi.org/10.1016/j.future.2017.05.039

Cao, Q. H., Madhusudan, G., Farahbakhsh, R., & Crespi, N. (2015). Usage control for data handling in smart cities. *Proceedings of the 2015 IEEE Global Communications Conference*, 1–6. https://doi.org/10.1109/GLOCOM.2015.7417270

Chang, M. K., Cheung, W., & Tang, M. (2013). Building trust online: Interactions among trust building mechanisms. *Information & Management*, *50*(7), 439–445. https://doi.org/10.1016/j.im.2013.06.003

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management*, *6*(2–3), 181–202. https://doi.org/10.1007/s10799-005-5879-y

Cheung, C. M., & Lee, M. K. (2003). An integrative model of consumer trust in internet shopping. *Proceedings of the 11th European Conference on Information Systems*, 1–15.

Choi, J. K., & Ji, Y. G. (2015). Investigating the importance of trust on adopting an autonomous vehicle. *International Journal of Human-Computer Interaction*, *31*(10), 692–702. https://doi.org/10.1080/10447318.2015.1070549

Cukier, K., & Mayer-Schoenberger, V. (2013). The rise of big data: How it's changing the way we think about the world. *Foreign Affairs*, *92*(3), 28–40. https://doi.org/10.1016/j.soncn.2018.03.008

Dawid, H., Decker, R., Hermann, T., Jahnke, H., Klat, W., König, R., & Stummer, C. (2017). Management science in the era of smart consumer products: Challenges and research perspectives. *Central European Journal of Operations Research*, *25*(1), 203–230. https://doi.org/10.1007/s10100-016-0436-9

Derikx, S., De Reuver, M., & Kroesen, M. (2016). Can privacy concerns for insurance of connected cars be compensated? *Electronic Markets*, *26*(1), 73–81. https://doi.org/10.1007/s12525-015-0211-0

Dinmohammadi, F., Page, V., Flynn, D., Robu, V., Fisher, M., Patchett, C., Jump, M., Tang, W., & Webster, M. (2018). Certification of safe and trusted robotic inspection of assets. *Proceedings of the 2018 Prognostics and System Health Management Conference*, 276–284. https://doi.org/10.1109/PHM-Chongqing.2018.00054

Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research*, *59*(8), 877–886. https://doi.org/10.1016/j.jbusres.2006.02.006

Gupta, B., Iyer, L. S., & Weisskirch, R. S. (2010). Facilitating global e-commerce: A comparison of consumers' willingness to disclose personal information online in the U.S. and in India. *Journal of Electronic Commerce Research*, *11*(1), 41–52.

Hajli, N., & Lin, X. (2016). Exploring the security of information sharing on social networking sites: The role of perceived control of information. *Journal of Business Ethics*, *133*(1), 111–123. https://doi.org/10.1007/s10551-014-2346-x

Hann, I.-H., Hui, K.-L., Lee, S.-Y. T., & Png, I. P. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems*, *24*(2), 13–42. https://doi.org/10.2753/MIS0742-1222240202

Happ, C., Melzer, A., & Steffgen, G. (2016). Trick with treat – Reciprocity increases the willingness to communicate personal data. *Computers in Human Behavior*, *61*, 372–377. https://doi.org/10.1016/j.chb.2016.03.026

Hayes, A. F. (2018). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach* (2nd ed.). The Guilford Press.

Hayes, A. F., & Matthes, J. (2009). Computational procedures for probing interactions in OLS and logistic regression: SPSS and SAS implementations. *Behavior Research Methods*, *41*(3), 924–936. https://doi.org/10.3758/BRM.41.3.924

Head, M. M., & Hassanein, K. (2002). Trust in e-commerce: Evaluating the impact of third-party seals. *Quarterly Journal of Electronic Commerce*, *3*(3), 307–325.

Head, M. M., Yuan, Y., & Archer, N. (2001). Building trust in e-commerce: A theoretical framework. *Proceedings of the Second World Congress on the Management of Electronic Commerce*, 17–19.

Heck, P., Klabbers, M., & Van Eekelen, M. (2010). A software product certification model. *Software Quality Journal*, *18*(1), 37–55. https://doi.org/10.1007/s11219-009-9080-0

Holland, S. (2016). Lending credence: Motivation, trust, and organic certification. *Agricultural and Food Economics*, *4*(1), 14–32. https://doi.org/10.1186/s40100-016-0058-5

Houston, R. W., & Taylor, G. K. (1999). Consumer perceptions of CPA WebTrust assurances: Evidence of an expectation gap. *International Journal of Auditing*, *3*(2), 89–105. https://doi.org/10.1111/1099-1123.00051

Hui, K.-L., Hock, H. T., & Lee, S.-Y. T. (2007). The value of privacy assurance: An exploratory field experiment. *MIS Quarterly*, *31*(1), 19–33. https://doi.org/10.2307/25148779

Hull, R., Kumar, B., Lieuwen, D., Patel-Schneider, P. F., Sahuguet, A., Varadarajan, S., & Vyas, A. (2004). Enabling context-aware and privacy-conscious user data sharing. *Proceedings of the 2004 IEEE International Conference on Mobile Data Management*, 187–198. https://doi.org/10.1109/MDM.2004.1263065

IBM Support (2020). *The calculation of Bonferroni-adjusted p-values*. https://www.ibm.com/support/pages/calculation-bonferroni-adjusted-p-values. Last accessed Jul. 7, 2020.

John, L. K., Acquisti, A., & Loewenstein, G. (2011). Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of Consumer Research*, *37*(5), 858–873. https://doi.org/10.1086/656423

Johnson, P. O., & Neyman, J. (1936). Tests of certain linear hypotheses and their application to some educational problems. *Statistical Research Memoirs*, *1*, 57–93.

Kamins, M. A., & Marks, L. J. (1991). The perception of kosher as a third party certification claim in advertising for familiar and unfamiliar brands. *Journal of the Academy of Marketing Science*, *19*(3), 177–185. https://doi.org/10.1177/009207039101900303

Kaplan, S. E., & Nieschwietz, R. J. (2003). A web assurance services model of trust for B2C e-commerce. *International Journal of Accounting Information Systems*, *4*(2), 95–114. https://doi.org/10.1016/S1467-0895(03)00005-8

Katopodis, S., Spanoudakis, G., & Mahbub, K. (2014). Towards hybrid cloud service certification models. *Proceedings of the 2014 IEEE International Conference on Services Computing*, 394–399. https://doi.org/10.1109/SCC.2014.59

Kim, D. J. (2008). Self-perception-based versus transference-based trust determinants in computer-mediated transactions: A cross-cultural comparison study. *Journal of Management Information Systems*, *24*(4), 13–45. https://doi.org/10.2753/MIS0742-1222240401

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems*, *44*(2), 544–564. https://doi.org/10.1016/j.dss.2007.07.001

Kim, K., & Kim, J. (2011). Third-party privacy certification as an online advertising strategy: An investigation of the factors affecting the relationship between third-party certification and initial trust. *Journal of Interactive Marketing*, *25*(3), 145–158. https://doi.org/10.1016/j.intmar.2010.09.003

Kimery, K. M., & McCord, M. (2002). Third-party assurances: Mapping the road to trust in e-retailing. *Journal of Information Technology Theory and Application*, *4*(2), 63–82.

Lauer, T. W., & Deng, X. (2007). Building online trust through privacy practices. *International Journal of Information Security*, *6*(5), 323–331. https://doi.org/10.1007/s10207-007-0028-8

Lee, J. D., & See, K. A. (2004). Trust in automation: Designing for appropriate reliance. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *46*(1), 50–80. https://doi.org/10.1518/hfes.46.1.50_30392

Lee, S. M., Choi, J., & Lee, S.-G. (2004). The impact of a third-party assurance seal in customer purchasing intention. *Journal of Internet Commerce*, *3*(2), 33–51. https://doi.org/10.1300/J179v03n02_03

Leon, P. G., Ur, B., Wang, Y., Sleeper, M., Balebako, R., Shay, R., Bauer, L., Christodorescu, M., & Cranor, L. F. (2013). What matters to users? Factors that affect users' willingness to share information with online advertisers. *Proceedings of the Ninth Symposium on Usable Privacy and Security*, 1–19. https://doi.org/10.1145/2501604.2501611

Leppäniemi, M., Karjaluoto, H., & Saarijärvi, H. (2017). Customer perceived value, satisfaction, and loyalty: The role of willingness to share information. *The International Review of Retail, Distribution and Consumer Research*, *27*(2), 164–188. https://doi.org/10.1080/09593969.2016.1251482

Lewicki, R. J., & Bunker, B. B. (1996). Developing and maintaining trust in working relationships. In R. M. Kramer & T. R. Tyle (Eds.), *Trust and Organizations: Frontiers of Theory and Research* (1st ed., pp. 114–139). Sage Publications.

Libert, T. (2018). An automated approach to auditing disclosure of third-party data collection in website privacy policies. *Proceedings of the 2018 World Wide Web Conference*, 207–216. https://doi.org/10.1145/3178876.3186087

Lins, S., Grochol, P., Schneider, S., & Sunyaev, A. (2016). Dynamic certification of cloud services: Trust, but verify! *IEEE Security & Privacy*, *14*(2), 66–71. https://doi.org/10.1109/MSP.2016.26

Liu, C., Marchewka, J. T., Lu, J., & Yu, C.-S. (2005). Beyond concern – A privacy-trust-behavioral intention model of electronic commerce. *Information & Management*, *42*(2), 289–304. https://doi.org/10.1016/j.im.2004.01.003

Lohr, L., & Krissoff, B. (2002). Consumer effects of harmonizing international standards for trade in organic foods. In B. Krissoff, M. Bohman, & J. A. Caswell (Eds.), *Global Food Trade and Consumer Demand for Quality* (1st ed., pp. 209–228). Springer. https://doi.org/10.1007/978-1-4757-5329-5_12

Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses: A power-responsibility equilibrium perspective. *Journal of the Academy of Marketing Science*, *35*(4), 572–585. https://doi.org/10.1007/s11747-006-0003-3

Lytton, T. D. (2014). Competitive third-party regulation: How private certification can overcome constraints that frustrate government regulation. *Theoretical Inquiries in Law*, *15*(2), 539–572. https://doi.org/10.1515/til-2014-0211

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336–355. https://doi.org/10.1287/isre.1040.0032

MarketsandMarkets (2019). *Testing, inspection, & certification market*. https://www.marketsandmarkets.com/Market-Reports/testing-inspection-certification-market-5352498.html. Last accessed Feb. 26, 2020.

Martínez Caro, L., & Martínez García, J. A. (2009). Does ISO 9000 certification affect consumer perceptions of the service provider?. *Managing Service Quality: An International Journal*, *19*(2), 140–161. https://doi.org/10.1108/09604520910943152

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. https://doi.org/10.1016/j.bushor.2019.07.008

McAllister, D. J. (1995). Affect- and cognition-based trust as foundations for interpersonal cooperation in organizations. *Academy of Management Journal*, *38*(1), 24–59. https://doi.org/10.5465/256727

McKnight, D. H., Kacmar, C. J., & Choudhury, V. (2004). Shifting factors and the ineffectiveness of third party assurance seals: A two-stage model of initial trust in a web business. *Electronic Markets*, *14*(3), 252–266. https://doi.org/10.1080/1019678042000245263

Meuwissen, M. P., Velthuis, A. G., Hogeveen, H., & Huirne, R. B. (2003). Traceability and certification in meat supply chains. *Journal of Agribusiness*, *21*(2), 167–181. https://doi.org/10.22004/ag.econ.14666

Milne, G. R., & Boza, M.-E. (1999). Trust and concern in consumers' perceptions of marketing information management practices. *Journal of Interactive Marketing*, *13*(1), 5–24. https://doi.org/10.1002/(SICI)1520-6653(199924)13:1<5::AID-DIR2>3.0.CO;2-9

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, *18*(3), 15–29. https://doi.org/10.1002/dir.20009

Milne, G. R., Gabisch, J. A., Markos, E., & Phelps, J. E. (2012). Changes in consumer willingness to provide information over the last decade: A cohort analysis. *International Journal of Integrated Marketing Communications*, *4*(2), 44–59.

Minard, P. (2016). Signalling through the noise: Private certification, information asymmetry and Chinese SMEs' access to finance. *Journal of Asian Public Policy*, *9*(3), 243–256. https://doi.org/10.1080/17516234.2015.1083412

Moiso, C., & Minerva, R. (2012). Towards a user-centric personal data ecosystem – The role of the bank of individuals' data. *Proceedings of the 2012 16th International Conference on Intelligence in Next Generation Networks*, 202–209. https://doi.org/10.1109/ICIN.2012.6376027

Moon, Y. (2000). Intimate exchanges: Using computers to elicit self-disclosure from consumers. *Journal of Consumer Research*, *26*(4), 323–339. https://doi.org/10.1086/209566

Nam, C., Song, C., Lee, E., & Park, C. I. (2006). Consumers' privacy concerns and willingness to provide marketing-related personal information online. In C. Pechmann & L. Price (Eds.), *NA - Advances in Consumer Research* (Vol. 33, pp. 212–217). Association for Consumer Research.

Norman, G., Pepall, L., Richards, D., & Tan, L. (2016). Competition and consumer data: The good, the bad, and the ugly. *Research in Economics*, *70*(4), 752–765. https://doi.org/10.1016/j.rie.2016.09.002

Nöteberg, A., Christiaanse, E., & Wallage, P. (2003). Consumer trust in electronic channels: The impact of electronic commerce assurance on consumers' purchasing likelihood and risk perceptions. *E-Service Journal*, *2*(2), 46–67. https://doi.org/10.1353/esj.2003.0014

Olivero, N., & Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology*, *25*(2), 243–262. https://doi.org/10.1016/S0167-4870(02)00172-1

Ortega, D. L., Wang, H. H., Wu, L., & Olynk, N. J. (2011). Modeling heterogeneity in consumer preferences for select food safety attributes in China. *Food Policy*, *36*(2), 318–324. https://doi.org/10.1016/j.foodpol.2010.11.030

Özpolat, K., Gao, G. G., Jank, W., & Viswanathan, S. (2013). The value of third-party assurance seals in online retailing: An empirical investigation. *Information Systems Research*, *24*(4), 1100–1111. https://doi.org/10.1287/isre.2013.0489

Park, I., Bhatnagar, A., & Rao, H. R. (2010). Assurance seals, on-line customer satisfaction, and repurchase intention. *International Journal of Electronic Commerce*, *14*(3), 11–34. https://doi.org/10.2753/JEC1086-4415140302

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, *19*(1), 27–41. https://doi.org/10.1509/jppm.19.1.27.16941

Pinchot, J., Chawdhry, A. A., & Paullet, K. (2018). Data privacy issues in the age of data brokerage: An exploratory literature review. *Issues in Information Systems*, *19*(3), 92–100.

Portz, K., Strong, J. M., & Sundby, L. (2001). To trust or not to trust: The impact of WebTrust on the perceived trustworthiness of a web site. *Review of Business Information Systems*, *5*(3), 35–50. https://doi.org/10.19030/rbis.v5i3.5357

Prince, C. (2018). Do consumers want to control their personal data? Empirical evidence. *International Journal of Human-Computer Studies*, *110*, 21–32. https://doi.org/10.1016/j.ijhcs.2017.10.003

Rifon, N. J., LaRose, R., & Choi, S. M. (2005). Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures. *The Journal of Consumer Affairs*, *39*(2), 339–362. https://doi.org/10.1111/j.1745-6606.2005.00018.x

Rijsdijk, S. A., & Hultink, E. J. (2003). "Honey, have you seen our hamster?" Consumer evaluations of autonomous domestic products. *Journal of Product Innovation Management*, *20*(3), 204–216. https://doi.org/10.1111/1540-5885.2003003

Roeber, B., Rehse, O., Knorrek, R., & Thomsen, B. (2015). Personal data: How context shapes consumers' data sharing with organizations from various sectors. *Electronic Markets*, *25*(2), 95–108. https://doi.org/10.1007/s12525-015-0183-0

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, *23*(3), 393–404. https://doi.org/10.5465/amr.1998.926617

Sayre, S., & Horne, D. (2000). Trading secrets for savings: How concerned are consumers about club cards as a privacy threat? In S. J. Hoch & R. J. Meyer (Eds.), *NA - Advances in Consumer Research* (Vol. 27, pp. 151–155). Association for Consumer Research.

Schmalz, S., & Orth, U. R. (2012). Brand attachment and consumer emotional response to unethical firm behavior. *Psychology & Marketing*, *29*(11), 869–884. https://doi.org/10.1002/mar.20570

Schoenbachler, D. D., & Gordon, G. L. (2002). Trust and customer willingness to provide information in database-driven relationship marketing. *Journal of Interactive Marketing*, *16*(3), 2–16. https://doi.org/10.1002/dir.10033

Schudy, S., & Utikal, V. (2017). "You must not know about me" – On the willingness to share personal data. *Journal of Economic Behavior & Organization*, *141*, 1–13. https://doi.org/10.1016/j.jebo.2017.05.023

Seifert, A., Christen, M., & Martin, M. (2018). Willingness of older adults to share mobile health data with researchers. *GeroPsych*, *31*(1), 41–49. https://doi.org/10.1024/1662-9647/a000181

Sha, W. (2009). Types of structural assurance and their relationships with trusting intentions in business-to-consumer e-commerce. *Electronic Markets*, *19*(1), 43–54. https://doi.org/10.1007/s12525-008-0001-z

Sporleder, T. L., & Goldsmith, P. D. (2001). Alternative firm strategies for signaling quality in the food system. *Canadian Journal of Agricultural Economics*, *49*(4), 591–604. https://doi.org/10.1111/j.1744-7976.2001.tb00329.x

Sturgess, J., Nurse, J. R., & Zhao, J. (2018). A capability-oriented approach to assessing privacy risk in smart home ecosystems. *Proceedings of the 2018 Living in the Internet of Things: Cybersecurity of the IoT Conference*, 37–44. https://doi.org/10.1049/cp.2018.0037

Tanner, B. (2000). Independent assessment by third-party certification bodies. *Food Control*, *11*(5), 415–417. https://doi.org/10.1016/S0956-7135(99)00055-9

Tao, H., Bhuiyan, M. Z., Rahman, M. A., Wang, G., Wang, T., Ahmed, M. M., & Li, J. (2019). Economic perspective analysis of protecting big data security and privacy. *Future Generation Computer Systems*, *98*, 660–671. https://doi.org/10.1016/j.future.2019.03.042

Tessem, B., & Nyre, L. (2013). The influence of social media use on willingness to share location information. In S. Furnell, C. Lambrinoudakis, & J. Lopez (Eds.), *Trust, Privacy, and Security in Digital Business* (pp. 161–172). Springer.

Thomson, M. (2006). Human brands: Investigating antecedents to consumers' strong attachments to celebrities. *Journal of Marketing*, *70*(3), 104–119. https://doi.org/10.1509/jmkg.70.3.104

Truong, N. B., Cao, Q. H., Um, T.-W., & Lee, G. M. (2016). Leverage a trust service platform for data usage control in smart city. *Proceedings of the 2016 IEEE Global Communications Conference*, 1–7. https://doi.org/10.1109/GLOCOM.2016.7841951

Van Dijke, J., Van Schijndel, M., Nashashibi, F., & De la Fortelle, A. (2012). Certification of automated transport systems. *Procedia – Social and Behavioral Sciences*, *48*, 3461–3470. https://doi.org/10.1016/j.sbspro.2012.06.1310

Vanitha, M., & Raju, R. (2013). Data sharing: Efficient distributed accountability in cloud using third party auditor. *International Journal of Innovative Technology and Exploring Engineering*, *2*(5), 135–138.

Wang, S., Beatty, S. E., & Foxx, W. (2004). Signaling the trustworthiness of small online retailers. *Journal of Interactive Marketing*, *18*(1), 53–69. https://doi.org/10.1002/dir.10071

Ward, S., Bridges, K., & Chitty, B. (2005). Do incentives matter? An examination of on-line privacy concerns and willingness to provide personal and financial information. *Journal of Marketing Communications*, *11*(1), 21–40. https://doi.org/10.1080/1352726042000263575

Wells, J. D., Valacich, J. S., & Hess, T. J. (2011). What signal are you sending? How website quality influences perceptions of product quality and purchase intentions. *MIS Quarterly*, *35*(2), 373–396. https://doi.org/10.2307/23044048

West, J. L. (2015). A mixed method analysis of the Better Business Bureau's third-party seal and the extent to which it inculcates trust among consumers. *Journal of Research in Interactive Marketing*, *9*(3), 214–238. https://doi.org/10.1108/JRIM-09-2014-0055

Windhorst, I., & Sunyaev, A. (2013). Dynamic certification of cloud services. *Proceedings of the 2013 International Conference on Availability, Reliability and Security*, 412–417. https://doi.org/10.1109/ARES.2013.55

Wu, L., Yin, S., Xu, Y., & Zhu, D. (2014). Effectiveness of China's organic food certification policy: Consumer preferences for infant milk formula with different organic certification labels. *Canadian Journal of Agricultural Economics*, *62*(4), 545–568. https://doi.org/10.1111/cjag.12050

Xu, H., Crossler, R. E., & Bélanger, F. (2012). A value sensitive design investigation of privacy enhancing tools in web browsers. *Decision Support Systems*, *54*(1), 424–433. https://doi.org/10.1016/j.dss.2012.06.003

Yang, S.-C., Hung, W.-C., Sung, K., & Farn, C.-K. (2006). Investigating initial trust toward e-tailers from the elaboration likelihood model perspective. *Psychology & Marketing*, *23*(5), 429–445. https://doi.org/10.1002/mar.20120

Yousafzai, S. Y., Pallister, J. G., & Foxall, G. R. (2005). Strategies for building and communicating trust in electronic banking: A field experiment. *Psychology & Marketing*, *22*(2), 181–201. https://doi.org/10.1002/mar.20054

Zang, J., Dummit, K., Graves, J., Lisker, P., & Sweeney, L. (2015). Who knows what about me? A survey of behind the scenes personal data sharing to third parties by mobile apps. *Technology Science*, *30*, 1–53.

Zhang, H. (2005). Trust-promoting seals in electronic markets: Impact on online shopping decisions. *Journal of Information Technology Theory and Application*, *6*(4), 29–40.

Zhao, X., Lynch, J. G., & Chen, Q. (2010). Reconsidering Baron and Kenny: Myths and truths about mediation analysis. *Journal of Consumer Research*, *37*(2), 197–206. https://doi.org/10.1086/651257

Zimmer, J. C., Arsal, R., Al-Marzouq, M., Moore, D., & Grover, V. (2010). Knowing your customers: Using a reciprocal relationship to enhance voluntary information disclosure. *Decision Support Systems*, *48*(2), 395–406. https://doi.org/10.1016/j.dss.2009.10.003

Appendix A: Repeated measures ANOVA with Bonferroni correction: Pairwise comparisons

I	J	Mean Difference (I-J)	SE	*p* [1, 2]	95% CI for difference[1]
Independent third-party	Government	.62	.06	< .001	[.43, .81]
	Cloud service provider	.91	.07	< .001	[.70, 1.12]
	Technology company	.96	.07	< .001	[.75, 1.17]
	University	.11	.05	.60	[-.04, .27]
	Start-up company	1.05	.07	< .001	[.84, 1.25]
	Software company	.75	.07	< .001	[.55, .95]
Government	Independent third-party	-.62	.06	< .001	[-.81, -.43]
	Cloud service provider	.29	.07	.001	[.08, .51]
	Technology company	.34	.07	< .001	[.12, .56]
	University	-.50	.06	< .001	[-.68, -.32]
	Start-up company	.43	.07	< .001	[.22, .64]
	Software company	.13	.06	.80	[-.06, .33]
Cloud service provider	Independent third-party	-.91	.07	< .001	[-1.12, -.70]
	Government	-.29	.07	.001	[-.51, -.08]
	Technology company	.05	.05	1.00	[-.11, .21]
	University	-.80	.07	< .001	[-1.01, -.59]
	Start-up company	.14	.05	.11	[-.01, .29]
	Software company	-.16	.05	.05	[-.32, .00]
Technology company	Independent third-party	-.96	.07	< .001	[-1.17, -.75]
	Government	-.34	.07	< .001	[-.56, -.12]
	Cloud service provider	-.05	.05	1.00	[-.21, .11]
	University	-.85	.07	< .001	[-1.06, -.63]
	Start-up company	.09	.06	1.00	[-.08, .26]
	Software company	-.21	.05	< .001	[-.36, -.06]
University	Independent third-party	-.11	.05	.60	[-.27, .04]
	Government	.50	.06	< .001	[.32, .68]
	Cloud service provider	.80	.07	< .001	[.59, 1.01]
	Technology company	.84	.07	< .001	[.63, 1.06]
	Start-up company	.93	.07	< .001	[.73, 1.14]
	Software company	.64	.07	< .001	[.44, .84]
Start-up company	Independent third-party	-1.05	.07	< .001	[-1.25, -.84]
	Government	-.43	.07	< .001	[-.64, -.22]
	Cloud service provider	-.14	.05	.11	[-.29, .01]
	Technology company	-.09	.06	1.00	[-.27, .08]
	University	-.93	.07	< .001	[-1.14, -.73]
	Start-up company	-.30	.06	< .001	[-.47, -.12]
Software company	Independent third-party	-.75	.07	< .001	[-.95, -.55]
	Government	-.13	.06	.80	[-.33, .06]
	Cloud service provider	.16	.05	.05	[.00, .32]
	Technology company	.21	.05	< .001	[.06, .36]
	University	-.64	.07	< .001	[-.84, -.44]
	Start-up company	.30	.06	< .001	[.12, .47]

Notes:

Based on estimated marginal means.

[1] Adjustment for multiple comparisons: Bonferroni.

[2] *P*-values of 1.00 are shown due to the approach SPSS uses to calculate Bonferroni adjusted *p*-values (for an explanation, see: IBM Support (2020), https://www.ibm.com/support/pages/calculation-bonferroni-adjusted-p-values).

Appendix B: Correlation table

		Attitude toward smart product(s)	Trust in smart product(s)	Satisfaction with smart product(s)	Awareness of privacy practices	Willingness to share data	Importance of data privacy	Trust propensity	Independent third-party	Government	Cloud service provider	Technology company	University	Start-up company	Software company
Attitude toward smart product(s)	r (604)	1.00													
	p														
Trust in smart product(s)	r (604)	.75	1.00												
	p	< .001													
Satisfaction with smart product(s)	r (604)	.61	.59	1.00											
	p	< .001	< .001												
Awareness of privacy practices	r (604)	.14	.02	.27	1.00										
	p	< .001	.63	< .001											
Willingness to share data	r (604)	.32	.41	.18	-.23	1.00									
	p	< .001	< .001	< .001	< .001										
Importance of data privacy	r (604)	.08	-.02	.16	.78	-.26	1.00								
	p	.06	.63	< .001	< .001	< .001									
Trust propensity	r (604)	.26	.39	.14	-.09	.47	-.08	1.00							
	p	< .001	< .001	< .001	.04	< .001	.06								
Independent third-party	r (604)	.32	.37	.30	.02	.33	-.06	.31	1.00						
	p	< .001	< .001	< .001	.71	< .001	.12	< .001							
Government	r (604)	.27	.33	.16	-.07	.42	-.10	.44	.60	1.00					
	p	< .001	< .001	< .001	.09	< .001	.02	< .001	< .001						
Cloud service provider	r (604)	.33	.40	.18	-.10	.53	-.14	.43	.50	.48	1.00				
	p	< .001	< .001	< .001	.01	< .001	< .001	< .001	< .001	< .001					
Technology company	r (604)	.36	.47	.23	-.17	.56	-.19	.43	.50	.49	.73	1.00			
	p	< .001	< .001	< .001	< .001	< .001	< .001	< .001	< .001	< .001	< .001				
University	r (604)	.29	.31	.25	-.03	.32	-.10	.33	.70	.63	.49	.48	1.00		
	p	< .001	< .001	< .001	.45	< .001	.01	< .001	< .001	< .001	< .001	< .001			
Start-up company	r (604)	.28	.38	.15	-.12	.54	-.13	.49	.48	.50	.73	.66	.49	1.00	
	p	< .001	< .001	< .001	.004	< .001	.001	< .001	< .001	< .001	< .001	< .001	< .001		
Software company	r (604)	.37	.47	.21	-.16	.56	-.15	.44	.54	.57	.71	.75	.53	.64	1.00
	p	< .001	< .001	< .001	< .001	< .001	< .001	< .001	< .001	< .001	< .001	< .001	< .001	< .001	

Note:

Pearson correlations, p-values 2-tailed.

Appendix C: Scenario descriptions for studies 1–3

Exemplary screenshots from Study 1:

Analogous scenarios to those presented below were used for studies 2 and 3 with a smartphone instead of a smart speaker as the focal smart product.

1. Control condition

Screenshot of the scenario description

Bei der **Verwendung Ihres smarten Lautsprechers** entstehen viele **Daten**, durch welche weitreichende **Informationen über Sie gewonnen werden** können, beispielsweise über die Verwendung Ihres smarten Lautsprechers, aber auch über Sie als Nutzer.

Diese Daten werden in Zukunft **direkt an den Hersteller** des smarten Lautsprechers **übertragen** und dort gespeichert.

Hierbei ist **unklar**,

- welche Daten der Hersteller **speichert und verwendet** und in welcher Situation welche Arten von Daten übertragen werden (keine personalisierten Einstellungen),
- ob die Daten **an dritte Parteien**, z.B. Partnerunternehmen des Herstellers, **weitergegeben** werden,
- ob die Daten **anonymisiert** sind (also keiner bestimmten Person zuordenbar),
- ob die Daten **kommerziell verwendet** werden, oder nur aus Sicherheitsgründen gespeichert werden (z.B. Datenbackup),
- ob die Daten **auf Sicherheit geprüft** werden (beispielsweise Hacking-Angriffe oder Datenmanipulation) etc.

English translation

When **using a smart speaker,** a lot of **data** are generated that can be used to obtain extensive **information about you**, for example, about the use of your smart speaker, but also about you as a user.

These data are **transmitted directly to the** smart speaker **manufacturer** and stored there.

It is **unclear**,

- which data the manufacturer **stores and uses** and in which situation which types of data are transmitted (i.e., no personalized settings),

- whether the data are **passed on to further entities**, e.g., partner companies of the manufacturer,
- whether the data are **anonymized** (i.e., cannot be assigned to a specific person),
- whether the data are **used commercially** or only stored for safety and security reasons (e.g., data backup),
- whether the data are **checked for security** (e.g., hacking attacks or data manipulation), etc.

2. Experimental condition

Screenshot of the scenario description

Bei der **Verwendung Ihres smarten Lautsprechers** entstehen viele **Daten**, durch welche weitreichende **Informationen über Sie gewonnen werden** können, beispielsweise über die Verwendung Ihres smarten Lautsprechers, aber auch über Sie als Nutzer.

Diese **Daten** werden in Zukunft **zuerst an [xxx] als Datentreuhänder übertragen, bevor von Ihnen ausgewählte Daten an den Hersteller** Ihres smarten Lautsprechers **übertragen** werden.

Als Datentreuhänder **garantiert [xxx] dafür**, dass

- nur die Arten von Daten an den Hersteller **übertragen und verwendet** werden, die Sie in Ihren **personalisierten Einstellungen** zur Weitergabe **freigegeben** haben,
- nur **autorisierte Daten an dritte Parteien**, z.B. Partnerunternehmen des Herstellers, **weitergegeben** werden,
- die Daten **anonymisiert** werden (also keiner bestimmten Person zuordenbar sind),
- die Daten von [xxx] **nicht kommerziell verwendet** werden, sondern nur aus Sicherheitsgründen gespeichert werden (z.B. Datenbackup),
- die Daten **auf Sicherheit geprüft** werden (beispielsweise Hacking-Angriffe oder Datenmanipulation) etc.

English translation

When **using a smart speaker**, a lot of **data** are generated that can be used to obtain extensive **information about you**, for example, about the use of your smart speaker, but also about you as a user.

These **data will first be transferred to [xxx][1] as the certification authority before the data you have selected are transferred to the** smart speaker **manufacturer**.

As the certification authority, **[xxx] guarantees** that

- only those types of data are **transferred** to the manufacturer and **used** that you have **authorized** for transfer **in your personalized settings**,

[1] Name of the certification authority depending on the study scenario: German testing, inspection, and certification company (i.e., an independent third-party), German government, German commercial entity.

- only **authorized data are passed on to further entities**, e.g., partner companies of the manufacturer,
- the data are anonymized (i.e., cannot be assigned to a specific person),
- the data are **not used commercially** by [*xxx*], but only stored for safety and security reasons (e.g., data backup)
- the data are checked for security (e.g., hacking attacks or data manipulation)), etc.

Appendix D: Detailed regression results of studies 1-3

	Study 1			Study 2			Study 3		
	b	**SE**	**95% CI**	***b***	**SE**	**95% CI**	***b***	**SE**	**95% CI**
Certification → Trust in data privacy	Third-party: .48 Government: .26 Commercial enterprise: .30	Third-party: .19 Government: .19 Commercial enterprise: .19	Third-party: [.11, .85] Government: [-.10, .63] Commercial enterprise: [-.06, .67]	.35	.13	[.10, .61]	1.23	.30	[.63, 1.84]
Trust in data privacy → Willingness to share data	.69	.03	[.64, .74]	.58	.03	[.52, .64]	.12	.10	[-.08, .31]
Indirect effect	Third-party: .33 Government: .18 Commercial enterprise: .21	Third-party: .13 Government: .13 Commercial enterprise: .13	Third-party: [.09, .59] Government: [-.07, .44] Commercial enterprise: [-.04, .47]	.21	.08	[.06, .36]	.15	.15	[-.11, .46]
Direct effect	Third-party: -.11 Government: -.20 Commercial enterprise: -.14	Third-party: .13 Government: .13 Commercial enterprise: .13	Third-party: [-.37, .14] Government: [-.45, .04] Commercial enterprise: [-.39, .11]	-.23	.09	[-.41, -.05]	1.60	1.12	[-.63, 3.83]
Total effect	Third-party: .22 Government: -.02 Commercial enterprise: .07	Third-party: .18 Government: .18 Commercial enterprise: .18	Third-party: [-.14, .57] Government: [-.37, .33] Commercial enterprise: [-.28, .43]	-.03	.12	[-.26, .21]	-	-	-
Trust in smart product → Willingness to share data	-	-	-	-	-	-	.44	.16	[.12, .75]
Interaction: Certification*Trust in smart product	-	-	-	-	-	-	-.44	.22	[-.88, .00]