Users' Preferences Concerning Privacy Properties of Assistant Systems on the Internet of Things

Completed Research

Jan Zibuschka
Robert Bosch GmbH
jan.zibuschka@de.bosch.com

Michael Nofer
HIVE Financials
michael.nofer@hivefinancials.com

Christian Zimmermann
Robert Bosch GmbH
christian.zimmermann3@de.bosch.com

Oliver Hinz
Goethe-Universität Frankfurt am Main
ohinz@wiwi.uni-frankfurt.de

Abstract

Assistance systems equipped with artificial intelligence are present in many Internet of Things applications to address information overload and provide automation. These assistant systems blur the boundaries between classical and individual information systems; display behavior classically associated with humans, and aggregate a wide range of information sources. While this development certainly promises a lot of utility for individuals interacting with assistant systems, it is also evident that those systems process a significant amount of personal information. This contribution investigates in how far the usage of assistance systems leads to privacy concerns and explores users' privacy preferences for assistant systems on the Internet of Things and ultimately quantifies the willingness to pay for various privacy functions of such assistance system.

Keywords

Assistance systems, willingness to pay, privacy, Internet of Things.

Introduction

Digital technology permeates all areas of life. Devices all around us are increasingly equipped with communication facilities, sensors, and actuators, and collaborate to achieve common goals (Privitera and Li, 2018). This convergence of information systems and everyday objects is referred to as the Internet of Things (IoT) (Atzori et al. 2010). However, the ubiquitous digital environment with its myriads of sensors and actuators can easily lead to information overload.

Assistance systems equipped with artificial intelligence may successfully address this problem (Nasirian et al., 2017). They are present in many IoT scenarios, e.g. proactive in-car assistants (Mihale-Wilson et al., 2019) or Smart Home systems (Menard and Bott, 2018). To address information overload and provide automation, assistance systems act as agents on behalf of the user, retrieving and aggregating information and performing automated actions in the physical or digital world (Sarikaya, 2017). Assistance systems exhibit various degrees of automation, e.g., the user may choose manually, the user may choose a course of action in specific contexts, or the system may act completely autonomously (Barkhuus and Dey, 2003).

One defining characteristic of contemporary assistance systems in the market today is their ability to interact through a natural language interface (Sarikaya, 2017). The most widespread commercial examples of such natural user interfaces - and perhaps the most iconic examples of digital assistants - are Amazon's Alexa, Apple's Siri, Microsoft's Cortana and Google Assistant (López, Quesada, and Guerrero, 2017; Hoy, 2018).

Thus, assistant systems blur the boundaries between classical and individual information systems, they display behavior classically associated with humans, and aggregate a wide range of information sources. While this development certainly promises a lot of utility for individuals interacting with assistant systems, it is also evident that those systems process a significant amount of personal information (Sarikaya, 2017). The details of this processing are not immediately obvious to the user, both with regard to the processed information, and with regard to the purpose for which this information is processed (Menard and Bott, 2018).

IoT systems and specifically assistance systems may process context information and personal information (Menard and Bott, 2018). This personal information may become available to organizations providing assistance services (Mihale-Wilson et al., 2017), which could raise privacy concerns (Radmacher et al., 2007; Menard and Bott, 2018). This study investigates in how far the usage of assistance systems leads to privacy concerns and explores users' privacy preferences for assistant systems on the Internet of Things and ultimately quantifies the willingness to pay (WTP) for various privacy functions of such assistance system.

Research Method

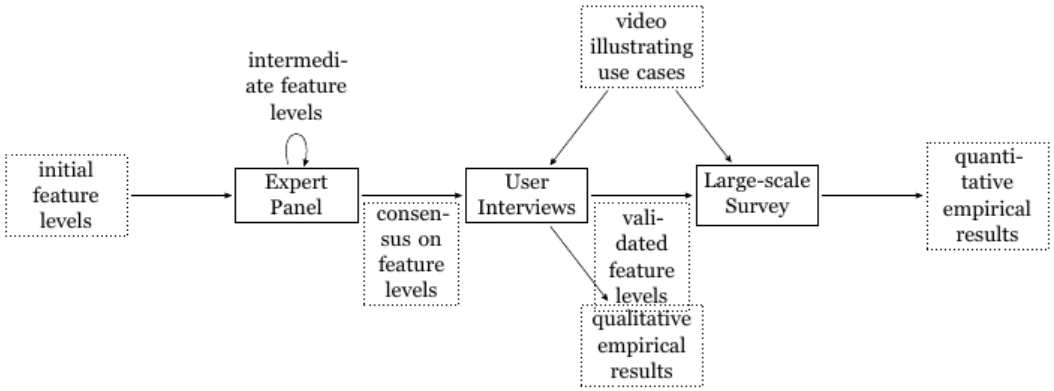

Figure 1. Overview of research method

Figure 1 provides an overview on our research method. Based on an initial, broad selection of privacy properties of assistant systems, an expert panel identified the most relevant ones (while also being allowed to add new features and consolidating a number of features into new constructs). Next, we performed semi-structured interviews to make sure users would understand the features chosen by the experts and gather additional qualitative results. Finally, we conducted a large-scale survey, which allows us to arrive at significant, quantitative results.

Expert Panel

To identify the most relevant security functions of such an assistance system, we surveyed a panel of eight security experts (qualified as experts by either a respective PhD, significant industry experience, or both) in multiple rounds, until a consensus emerged. We employed the Delphi method (Okoli and Pawlowski, 2004) for this step. The experts identified three feature attributes of privacy in assistance systems as most relevant, and the three most relevant levels of each attribute. The chosen feature attributes and attribute levels were:

Access Control

- Fine-granular: The user, for each device and service, determines individually which (other) devices and services it can access, or by which other devices and services it can be accessed.
- Group-wise: Services and devices are grouped, and the user then either determines which group can access which other group, or which devices and services are within a group and will be able to communicate within.

- Intelligent: The system further automates the configuration of access control, either leveraging the intelligence of the assistant, or using some other independent automation strategy transcending the group concept.

Transparency

- One-time: The system informs users about the general processing of personal information when they first activate it. They may be able to retrieve and review the information later.
- Regular: Users receive regular, e.g. weekly, updates about the processing of personal information in the system, e.g. by email.
- Intelligent: The system decides, e.g., leveraging the intelligence of the assistant, whether or not the user currently wants to receive information about the processing.

Location of processing

- System of manufacturer: The assistance system transfers personal information to a server at the manufacturer of the assistant.
- System of service provider: The assistant leverages servers of an external service provider chosen by either the manufacturer or the user.
- At user's home: The personal information resides on a system in the user's home, connected to the Internet.

User Interviews

We validated the understandability of the system instantiations in semi-structured interviews with nine test users with different demographic and professional backgrounds. In addition, during those interviews, we also gathered qualitative feedback, e.g., user statements about their vision of a privacy-friendly assistance system, and main privacy risks they associated with assistance systems.

The structured part also elicited additional information about the interviewees, to get an impression what would be relevant for our investigated preferences. For example, we found that interviewees had an average Internet usage time between 30 min and 4 hours. As the assistant system aims at assisting users also in the smart home domain, we asked interviewees about their living situation. Two interviewees were living in a rented flat, two in der a rented house, one in a self-owned flat and four in self-owned houses. However, only one interviewee was already using smart home devices.

We characterized IoT assistants for the participants (both in the early round interviews and in the quantitative survey) using a short film. The video covered a comprehensive set of use cases for assistant systems on the IoT from the mobility and smart home assistance domains, including navigation systems, home automation, smart heating and predictive maintenance. It comprised speech assistance, proactive, context-sensitive assistance, and step-by-step task assistance. However, the film did not present the assistant as overly adaptive, and the assistant did not learn new use cases during operation. While the system was not capable of having "intelligent" conversations with the user, it was able to follow spoken instructions and to provide verbal descriptions of running assistance tasks. The video also gave examples for multi-user functionality: the system takes into account, for example, the position of other family members when giving instructions for preparing a meal.

The interviewees' exhibited a broad range of initial impressions regarding the assistant ranging from enthusiasm ("ideal solution for the Internet of Things"), indifference ("I'm undeterred, but maybe also not impressed") to concern ("patronizing attitude", "I miss concepts for authorization and security"). Still, before the detailed introduction of the assistance system, all nine participants were willing to use the assistant, assuming the availability of useful applications.

Initial answers already clearly indicated that the interviewees were concerned about security and privacy, with some users expressing fear of losing control over the assistant or giving away health data. To investigate the interviewees' security and privacy attitudes further, we asked them about their privacy preferences and ideas for securing the assistant. When directly asked whether privacy was important for them, all interviewees stated that it indeed was. They were, however, willing to provide personal data for use by personal assistants, if a trustworthy company provides the assistant. This is consistent with the broad

body of literature on institutional trust, privacy concerns and trade-offs (see, e.g., Bélanger and Crossler (2011) and Smith, Dinev, and Xu (2011)).

The interviewees also provided their ideas for security and privacy functions. For example, they proposed isolation between different groups of assistants. Some proposed the use of passwords or biometric information to authenticate the user against the assistant to prevent access by other family members. Interview participants broadly perceived storing data in the cloud as less threatening than exposing information to friends, colleagues and family.

In order to investigate interviewees' preferences regarding assistants' features and design, we provided the design choices regarding access control, data processing and transparency resulting from the expert panel. Users understood the options presented to them, and could articulate clear preferences, e.g., strong support of group-wise access control. All users stated that they would buy the assistant in their preferred design alternative and would be willing to pay an average price of 300€ ($340) per annum.

Large-scale Survey

To investigate users' privacy preferences regarding assistance systems, we used choice-base conjoint analysis (CBC), which characterizes products in terms of feature attributes and levels. CBC requires surveyed users to choose among several hypothetical products characterized by specific feature attributes, levels, and price, or to indicate they would not use any of the presented products. We refer to a set of such products and the non-purchase option as a choice set. Each user completes several choice sets. Figure 2 presents a choice set used in the survey.

Figure 2. Example Choice Set Shown to Users in Survey (translated)

CBC analysis is frequently used because of its greater task similarity between choices and market behavior (Roßnagel et al., 2014). Moreover, several studies indicate that CBC analysis performs better than rating-based conjoint analysis (Karniouchina et al., 2009). CBC is especially suitable for eliciting user preferences during the early stages of product development (Chapman et al., 2008).

In our large-scale survey, we surveyed 293 respondents from Germany. The sample is representative with the full population with respect to age and gender. Of the 293 respondents, 113 (38.6%) never chose to purchase any of the offered assistants. 42 (14.3%) always purchased the assistant, no matter what variants were presented. 138 (47.1%) respondents were influenced in their purchase decision by the various privacy attributes and levels. Hence, given an appropriate design, a maximum of 61.4% of users would be willing to purchase the assistant.

To further explore the extent to which the decision not to purchase the assistant is linked to budget restrictions, we asked respondents whether they would use the assistant if it was provided free of charge, free and advertising-based, or free and financed through the monetization of personal data. We found that only 36% of non-purchaser would use an assistant provided free of charge, indicating 64% of non-purchasers (24% of the overall population) did not see the assistant as useful (which is not bad for a product in general). When the assistant is free and advertising-based, 10 percentage points less of the non-purchasers and 16 percentage points less of purchasers would purchase the assistant. An assistant financed through direct monetization of personal information loses another 55 percentage points of purchasers. These values indicate that privacy has a bigger impact on purchasers than on non-purchasers.

To investigate what drives user behavior, and to have a basis for identifying market segments later, we surveyed several psychographic attributes of the respondents, most notably:

- innovativeness according to Steenkamp and Gielens (2003), representing the probability with which consumers will try out new products,
- technology anxiety according to Meuter et al. (2005), expressing the degree of stress that user experience because of technology without a specific threat,
- risk affinity according to Jackson (1976), describing the readiness of an individual to take risks, and
- attitude towards product according to Ziamou and Ratneshwar (2003), measuring whether the user likes the product or service

We employed constructs (bundles of survey questions) from the aforementioned prior works to measure these demographics, and obtained excellent reliability measures using Cronbach's alpha, which is a function of the average covariance between questions as well as the number of questions in the instrument (Tavakol and Dennick, 2011). Cronbach's alpha indicates the degree to which a set of items measures a single unidimensional latent construct (Tavakol and Dennick, 2011). In all cases, reliability was equal or better than in the studies from which the instruments originated (innovativeness .87, technology affinity .93, risk taking .89, attitude towards product .90).

For non-purchasers (respondents who were not willing to purchase any of the assistant variations), we found that their decision is very significantly correlated with a negative attitude towards the assistant (which is to be expected, given they never chose to purchase the assistant), and a higher age. We did not find significant correlations with, for example, technology anxiety or privacy concern (see Table 1).

Logistic Regression DV: Non-purchaser (0/1)	Coefficient	Standard Error	Significance
Attitude towards product***	-1.603	.234	.000
Age***	.503	.016	.001
Privacy	-.231	.190	.177
Technology	.143	.171	.184
Willingness to innovate	-.151	.264	.566
Risk appetite	-.090	.180	.619
***significant at the 1 percent level			

Table 1. Characteristics of non-purchasers

Since there are many use cases of the assistant system in the smart home domain, we also analyzed the influence of the living situation. Conducting ANOVA analysis, we observe a difference between people who live in an own house or flat and people who live in a rented accommodation. 53.5 percent of participants who own their property purchase the assistant while this value is significantly lower for people renting their accommodation (see Tables 2 and 3).

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Ownership	114	.535	.5010	.0469	.442	.628	0	1
Rented	171	.421	.4952	.4952	.346	.496	0	1
Total	285	.467	.4998	.4998	.408	.525	0	1

Table 2. Descriptives

One reason might be the reluctance to speak with landlords. Furthermore, people might consider the assistance system as a permanent solution in the smart home area that can hardly be transferred to other houses or flats.

	Sum of Squares	df	Mean Square	F	Sig
Between Groups	.889	1	.889	3.594	.059
Within Groups	70.044	283	.248		
Total	70.933	284			

Table 3. ANOVA

For the characteristics of respondents who invariantly purchased the assistant, attitude towards product and age are also significant factors, however, we found that always purchasing the assistant most significantly and positively correlates with privacy concern (see Table 4). This finding was surprising for us. We will offer possible interpretations based on our earlier interviews in the discussion below.

Logistic Regression DV: Always-purchaser (0/1)	Coefficient	Standard Error	Significance
Attitude towards product**	.418	.188	.026
Age**	-.037	.016	.024
Privacy***	.698	.210	.001
Technology	-.086	.163	.599
Willingness to innovate	.204	.299	.495
Risk appetite	.266	.188	.158
***significant at the 1 percent level; **significant at the 5 percent level			

Table 4. Characteristics of always-purchasers

This result fits well with the so-called privacy paradox which means that people are willing to disclose personal information despite privacy concerns. For instance, Spiekermann et al. (2001) compared privacy preferences with the online shopping behavior and found that consumers even forget their concerns during the sales process. Norberg et al. (2007) found a gap between intentions and actual behavior when it comes to the disclosure of personal information to commercial enterprises. We also find evidence for the privacy paradox in such a way that users must disclose personal information when interacting with the assistance system. However, those participants who always purchase the assistant are very privacy sensitive.

We also can distinguish between different kinds of privacy concerns. Young and Quan-Haase (2013) distinguish between institutional and social privacy of users on social network sites. While social privacy refers to concerns about controlling the personal information, institutional privacy describes how companies or third parties deal with this information. The authors found that students are more concerned about social privacy than institutional privacy: Facebook users want to control who can see their personal information but do not restrict Facebook or other companies from using their data for commercial purposes. In our study, we asked participants whether they would use the assistant if it were a) free and advertising-based or b) free and financed through personal data (see Figure 4). In the first case, 81 percent of the users would purchase the assistant while only 26 percent would purchase it if their personal data can be analyzed. Thus, we extend previous findings in the literature by finding evidence for the privacy paradox in an IoT setting.

Based on psychographics and the results of the choice sets, we performed an unsupervised cluster analysis using the elbow method, which observes the marginal gain of explained variance (Ketchen and Shook, 1996). We identified four market segments, with age as the main differentiating factor (see Table 5).

Cluster analysis Internal hit rate: 87.55% Log-marginal density: -1,884.11		Segment 1 (n=42) 'Digital natives'	Segment 2 (n=29) 'Millennials'	Segment 3 (n=51) 'Baby Boomers'	Segment 4 (n=16) 'Seniors'	Entire Sample (n=138)
Psychographic Information (Likert)	Privacy Technology Innovation Risk appetite Attitude towards UPA	3.54 3.26 4.27 4.28 4.89	3.33 2.59 4.37 3.80 5.16	3.46 2.65 4.30 3.87 5.13	3.06 2.34 4.33 3.70 5.20	3.35 2.71 4.32 3.91 5.10
Demographic Information	Age (average) Income (month)	26 yrs 1,500 € – 2,000 €	40 yrs 2,500 € – 3,000 €	51 yrs 2,500 € – 3,000 €	66 yrs 2,000 € – 2,500 €	46 yrs 2,000 € – 2,500 €

Table 5. User Segments

Segment 1 exhibits an average age of 26 years, and a low income. We label this segment „Digital Natives". Similarly, we label the other segments „Millennials", „Baby Boomers", and „Seniors". Note that clustering will not always result in market segments sorted by age. For example, for security and privacy functions of federated identity management systems (an application case that is reasonably similar to the one presented

here, i.e. investigates security and privacy aspects of internet technology) Roßnagel et al. (2014) find market segments based on user psychographics.

In order to avoid distortions in our estimation, we followed Gensler et al. (2012), and removed respondents who invariantly would or would not purchase the assistant, regardless of the system attributes, from the sample. The cleaned-up dataset contains 138 respondents. We can then calculate the WTP in monetary terms (see Roßnagel et al., 2014 for more detail).

As already discussed, respondents answered several choice sets, each containing three alternative assistance system variations which differed regarding access control, location of data processing, transparency, and price (see Figure 2). Respondents could also indicate they would not purchase any of the given system designs. In this case, the price of all products in the choice set would be higher than the respondent's WTP.

		Access control			Data processing			Transparency			Price
	Ranking	Group-wise	Intelligent	Fine-granular	At home	Manufacturer	Service provider	Regular	Intelligent	One-time	WTP (month)
Digital Natives	1st		X			X			X		20.43€
	2nd		X			X				X	19.59€
	3rd		X			X		X			12.65€
Millenials	1st		X				X		X		16.85€
	2nd		X				X			X	15.92€
	3rd		X			X			X		15.24€
Baby Boomers	1st		X			X			X		24.31€
	2nd		X			X				X	23.56€
	3rd		X				X		X		22.11€
Seniors	1st		X				X		X		12.26€
	2nd		X			X			X		12.11€
	3rd		X				X			X	11.26€
Entire Sample	1st		X			X			X		19.75€
	2nd		X			X				X	18.91€
	3rd		X			X		X			14.04€

Table 6. Willingness to Pay and Preferred Products

Table 6 presents the resulting preferred product variations as well as their associated WTPs. It shows the three most preferred product variations in the segments Digital Natives, Millennials, Baby Boomers, Seniors and the entire population along with their associated WTPs. For example, across the entire sample, the most preferred product variation features intelligent access control, data processing at manufacturer, and intelligent transparency, with a WTP of 19.75€/month. From the table, it is immediately obvious that there is very strong support for intelligent access control, data processing at the manufacturer of assistant and devices, and intelligent transparency.

We found the strongest preference for a system on the servers of the manufacturer of the assistant, which leverages the intelligence of the assistant to help with transparency and control of personal information transmitted between any communicating devices and services. The second most preferred variation overall only provides a privacy notice on the use of the processed personal information in the form of a one-time notification when a communication relationship is established.

We also found interest in hosting the system on the server of a service provider chosen by the user or manufacturer. There was limited interest in other system designs within the best three solutions in any market segment we identified. Specifically, we found the lowest overall WTP for hosting the assistant on the user's own devices.

Discussion

The survey identifies the assistant itself as a promising component of privacy solutions, as users are looking to the assistant to help them keep control of their personal information, and offer them at the same time custom-tailored transparency. We can see this from both the strong preference for intelligent access control and intelligent transparency among sometimes-purchasers, and from the fact that those respondents who always purchased any variation are very significantly privacy sensitive.

To get a better understanding of what is going on, we go back to the earlier interviews. The privacy concerns voiced by the users in the interviews mainly concerned other users, e.g. "friends", "colleagues", "people", or "family". One respondent even identified his grandmother (who appeared in the video) as a potential privacy threat, stating that he would be willing to offer information to the company running the assistant to protect against potential unwanted disclosures to her. People in general did not see the disclosure of personal information to the assistant as a privacy threat (with the possible exception of medical information, as stated by several respondents). Interviewees stated that the assistant was "like a maid", and therefore expected to process personal information to be useful. This explains both the preference for hosting in the Cloud and the willingness to rely on intelligent functions for transparency and control. Interviewees also stated that companies are only a threat if they get "too intrusive", which did not apply to the assistant from the interviewees' perspective.

This counterintuitive result matches earlier studies that show that users do not see the platform provider as the most relevant attacker. For example, Krasnova et al. (2009) found (in focus groups) that social network users are far more concerned with individuals (23 coding matches) or external organizations (15 coding matches) accessing their personal information shared on the network rather than collection by the social network provider (2 matches) or affiliated third parties (1 match). Johnson, Egelman, and Bellovin (2012) present similar results, finding that social network users were mostly concerned about "future employers, supervisors, family members, peers, and subordinates" getting access to their information. Mazurek et al. (2010) surveyed what privacy breaches people find the most devastating, and found the attackers in those scenarios were "strangers, acquaintances, bosses, and teachers (…) more surprisingly (…) parents, children, family, friends, and even significant others."

This is also in line with the quantitative study's result that the most preferred assistant resides at the manufacturer, instead of at users' house or at a service provider of the users' choice. Interviewees stated that the intelligent functions must reside in the Cloud to have the appropriate processing power and amount of information to make them useful, and to allow for maintenance not involving the user.

The interviewees also emphasized the increased data security (e.g. physical access control, "firewalls", "backups") that an external service provider could offer. In addition, interviewees stated that they do not want their personal information released to "the Internet" without their control, which may have further reduced the interest in hosting at home, which was perceived less secure. We also asked whether users would like more information or more fine-grained control of the operation of the server hosting the assistant. They stated that both were "too much effort" as long as "a trusted organization" runs the server.

Users' statements that they would like to receive all components of the system from the same supplier to have clear accountability can explain the preference for a server at the manufacturer. In addition, one interviewee (who did not prefer the service provider) stated that he perceived hosting at a service provider as "probably the cheapest option". This perceived low value may have further hurt the service provider alternative. Therefore, it seems reasonable to assume that the manufacturer of the assistance would be the most trusted organization in this context.

Conclusion

We presented an overview of our work eliciting users' preferences for privacy properties of IoT assistant systems. We found users prefer IoT assistants running on the manufacturer's systems, and that offer automation of privacy notices and controls. Our results represent a German sample of prospective users and may not be generalizable to other cultures. However, we want to point out that Germans are less trusting when compared to the US in intercultural surveys (Krasnova and Veltri, 2010).

Our results motivate at least partially automated privacy functions for individual information systems, i.e. in scenarios where users orchestrate complex systems (Baskerville, 2011). This approach has received significant attention in the usable privacy community (Liu et al, 2016). Should we be able to implement appropriate artifacts meeting user preferences, this could mean that the challenges raised by the convergence of personal information in assistant systems on the Internet of Things can be addressed leveraging this same assistance.

The features we surveyed stem from an industry project, and therefore are not directly comparable to earlier work such as (Mihale-Wilson et al., 2017; Menard and Bott, 2018). To validate them, we performed pre-tests for the price, and had an expert panel review the initial features.

We in no way want to downplay the essential importance of privacy safeguards in the information driven IoT economy (Posey et al., 2017), and fully acknowledge that cybersecurity threats have a distinct impact on privacy (Burns and Johnson, 2017). However, privacy and security behavior are distinct (Dincelli et al., 2017). In our exploratory interviews and unsupervised clustering, we did not find support for security over privacy. Further structuring the market according to underlying drivers such as autonomy or acceptance of control (Dincelli et al., 2017) provides a fruitful avenue for future research.

REFERENCES

Atzori, L., Iera, A., and Morabito, G. 2010. "The Internet of Things: A survey." *Computer Networks* (54:15), pp. 2787–2805.

Barkhuus, L., and Dey, A. 2003. "Is Context-Aware Computing Taking Control away from the User? Three Levels of Interactivity Examined," in *UbiComp 2003: Ubiquitous Computing*. Springer, Berlin, Heidelberg, pp. 149–156.

Baskerville, R. 2011. "Design Theorizing Individual Information Systems," in *Pacific Asia Conference on Information Systems, PACIS 2011*. Paper 25. https://aisel.aisnet.org/pacis2011/25.

Bélanger, F. and Crossler, R. E. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly* (35:4), pp. 1017–1042.

Burns, A. J., and Johnson, E. 2018. "The Evolving Cyberthreat to Privacy," *IT Professional* (20:3), pp. 64-72.

Chapman, C. N., Love, E., and Alford, J. L. 2008. "Quantitative Early-Phase User Research Methods: Hard Data for Initial Product Design," in *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)*, Paper 37.

Dincelli, E., Goel, S., Wartenkin, M. 2017. "Understanding Nuances of Privacy and Security in the Context of Information Systems," *Twenty-third Americas Conference on Information Systems (AMCIS 2017)*, Paper 39, https://aisel.aisnet.org/amcis2017/InformationSystems/Presentations/39/

Gensler, S., Hinz, O., Skiera, B., Theysohn, S. 2012. "Willingness-to-Pay Estimation with Choice-Based Conjoint Analysis: Addressing Extreme Response Behavior with Individually Adapted Designs," *European Journal of Operational Research (EJOR)* (219:2), pp. 368-378.

Hoy, M. B. (2018). "Alexa, Siri, Cortana, and More: An Introduction to Voice Assistants," *Medical Reference Services Quarterly* (37:1), pp. 81–88.

Jackson, D. N. 1976. *Jackson Personality Inventory*. English. Port Huron, MI. Port Huron, MI: Research Psychologists Press.

Karniouchina, E. V., Moore, W. L., van der Rhee, B., and Verma, R. 2009. "Issues in the use of ratings-based versus choice-based conjoint analysis in operations management research," *European Journal of Operational Research* (197:1), pp. 340–348.

Ketchen, D. J., and Shook, C. L. 1996. "The Application of Cluster Analysis in Strategic Management Research: An Analysis and Critique," *Strategic Management Journal* (17:6), pp. 441– 458.

Krasnova, H., O. Günther, S. Spiekermann, and K. Koroleva. 2009. "Privacy concerns and identity in online social networks," *Identity in the Information Society* (2:1), pp. 39–63.

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

Liu, B., Andersen, M. S., Schaub, F., Almuhimedi, H., Zhang, S. A., Sadeh, N., Acquisti, A., and Agarwal, Y. 2016. "Follow my recommendations: A personalized privacy assistant for mobile app permissions," in *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pp. 27-41.

López, G., L. Quesada, and Guerrero, L. A. 2017. "Alexa vs. Siri vs. Cortana vs. Google Assistant: A Comparison of Speech-Based Natural User Interfaces," in *Advances in Human Factors and Systems Interaction*, pp. 241–250.

Mazurek, M. L., Arsenault, J. P., Bresee, J., Gupta, N., Ion, I., Johns, C., Lee, D., Liang, Y., Olsen, J., Salmon, B., Shay, R., Vaniea, K., Bauer, L., Cranor, L. F., Ganger, G. R., and Reiter, M. K. 2010. "Access Control for Home Data Sharing: Attitudes, Needs and Practices," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10*), pp. 645–654.

Menard, P., and Bott, G. 2018. "Investigating Privacy Concerns of Internet of Things (IoT) Users," in *Twenty-fourth Americas Conference on Information Systems (AMCIS 2018)*. New Orleans, LA, USA. Paper 41. https://aisel.aisnet.org/amcis2018/Security/Presentations/41/

Meuter, M. L., Bitner, M. J., Ostrom, A. L., and Brown, S. W. 2005. "Choosing Among Alternative Service Delivery Modes: An Investigation of Customer Trial of Self-Service Technologies," *Journal of Marketing* (69:2), pp. 61–83.

Mihale-Wilson, A.C., Zibuschka, J. and Hinz, O. (2017). "About User Preferences and Willingness to Pay for a Secure and Privacy Protective Ubiquitous Personal Assistant," in *Proceedings of the 25th European Conference on Information Systems*, 3, https://aisel.aisnet.org/ecis2017_rp/3

Mihale-Wilson, A.C., Zibuschka, J. and Hinz, O. (2019). "User preferences and willingness to pay for in-vehicle assistance" *Electronic Markets* (29:1), pp. 37–53.

Nasirian, F., Ahmadian, M. and Lee, O. 2017. "AI-Based Voice Assistant Systems: Evaluating from the Interaction and Trust Perspectives,"in *Twenty-third Americas Conference on Information Systems (AMCIS 2017)*, Paper 27, https://aisel.aisnet.org/amcis2017/AdoptionIT/Presentations/27/

Norberg, P. A., Horne, D. R., and Horne, A. A. 2007. The privacy paradox: personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs (*41:1), pp. 100-126.

Okoli, C., and Pawlowski, S. D. 2004. "The Delphi Method as a Research Tool: An Example, Design Considerations and Applications," *Information & Management* (42:1), pp. 15–29.

Posey, C., Raja, U., Crossler, R. E., and Burns, A. J. 2017. "Taking stock of organisations' protection of privacy: categorising and assessing threats to personally identifiable information in the USA," *European Journal of Information Systems* (26:6), pp. 585-604.

Privitera, D. and Li, L. 2018. "Can IoT Devices Be Trusted? An Exploratory Study." in *Twenty-fourth Americas Conference on Information Systems (AMCIS 2018)*, New Orleans, LA, USA. Paper 44. https://aisel.aisnet.org/amcis2018/Security/Presentations/44/

Radmacher, M., Zibuschka, J., Scherner, T., Fritsch, L. and Rannenberg, K. 2007. "Privatsphären-freundliche topozentrische Dienste unter Berücksichtigung rechtlicher, technischer und wirtschaftlicher Restriktionen," in *Wirtschaftsinformatik Proceedings 2007*, Paper 18, https://aisel.aisnet.org/wi2007/18

Roßnagel, H., Zibuschka, J., Hinz, O., and Muntermann, J. 2014. "Users' willingness to pay for web identity management systems," *European Journal of Information Systems*, (23:1), pp. 36–50.

Sarikaya, R. 2017. "The Technology Behind Personal Digital Assistants: An overview of the system architecture and key components," *IEEE Signal Processing Magazine*, (34:1), pp. 67–81.

Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review." *MIS Quarterly*, (35:4), pp. 989–1016.

Spiekermann, S., Grossklags, J., and Berendt, B. 2001. E-privacy in second generation e-commerce: privacy preferences versus actual behavior. *In: Proceedings of the 3rd ACM Conference on Electronic Commerce,* New York.

Steenkamp, J.-B. E. M., and Gielens, K. 2003. "Consumer and Market Drivers of the Trial Probability of New Consumer Packaged Goods." *Journal of Consumer Research* (30:3), 368– 384.

Tavakol, M., and Dennick, R. 2011. "Making sense of Cronbach's alpha." *International Journal of Medical Education* (2), pp. 53–55.

Warkentin, M., Goel, S., and Menard, P. 2017. "Shared Benefits and Information Privacy: What Determines Smart Meter Technology Adoption?," *Journal of the Association for Information Systems* (18:11), Article 3.

Young, A. L., and Quan-Haase, A. 2013. Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society* (16:4), pp. 479-500.

Ziamou, P., and Ratneshwar, S. 2003. "Innovations in Product Functionality: When and Why Are Explicit Comparisons Effective?" *Journal of Marketing* (67:2), pp. 49–61.