

## Consumer Privacy Concerns and Preferences for Certification and Accreditation of Intelligent Assistants in the Internet of Things.

K. Valerie Carl<sup>1</sup> and A. Cristina Mihale-Wilson<sup>2</sup>

**Abstract:** Interoperable Intelligent Assistant Systems (IAS) could help realize the advantages of the Internet of Things (IoT). Yet, due to their insufficient skill set and persistent privacy concerns on the consumers' side, such IAS experience only limited popularity. While enabling IAS to communicate and exchange data with each other could help such systems improve performance, certifications and accreditations can help build user's trust by addressing some of the consumers' privacy concerns. To better understand the incentives necessary to instigate the mass adoption of interoperable IAS, this paper presents a study exploring consumer privacy concerns and preferences for privacy certifications. The ultimate purpose of this paper is to provide certification recommendations for intelligent IoT networks in general and IAS in particular.

**Keywords:** Internet of Things, Intelligent Assistant Systems, certification and accreditation, privacy concerns

### 1 Introduction

The Internet of Things (IoT) paradigm envisions that objects, devices, machines, buildings, and several other items are equipped with microprocessors, sensors, tags, actuators, and software. Although invisible to individuals, the computational capabilities of things, along with their connectivity to the Internet, enable each of them to continually gather and send vast amounts of information [LL15]. Although this is useful for the optimized operation of some devices, the real value of IoT can be reached only if all devices and data are connected into an Internet of Everything (IoE) [LL15] that is then orchestrated by Intelligent Assistants Systems (IAS). However, currently, the realization of the IoE still hinges on technical and non-technical challenges [WF15] of seamless interoperability. Privacy-related aspects and potential users' privacy concerns are amongst such challenges. And although privacy consists of both technical and non-technical aspects, the focus of this study lies on privacy in the non-technical context.

Due to the central role of privacy concerns in the consumer adoption of IoT enabled products, this study explores consumers' attitudes and preferences for certifications and accreditations that might help gain user's trust by addressing some of the consumers'

---

<sup>1</sup> TU Darmstadt, Fachbereich Rechts- und Wirtschaftswissenschaften, Hochschulstraße 1, Darmstadt, 64289, valerie.carl@web.de

<sup>2</sup> Goethe University Frankfurt, Professur für Wirtschaftsinformatik und Informationsmanagement, Theodor-W.-Adorno-Platz 4, Frankfurt am Main, 60323, mihale-wilson@wiwi.uni-frankfurt.de

privacy concerns. In doing so, we wish to gain insights and provide certification recommendations for intelligent IoT networks in general, and interoperable IAS in particular.

## 2 Theoretical Background and Related Work

Studying consumers' attitudes and behavior has a long history in academia [Oi13], [Ve03], such that, to date, there are numerous theories dedicated to understanding the essential antecedents of consumers' technology adoption behavior. Despite the different settings and technologies prior research has considered, consumers' privacy concerns and trust have repeatedly loomed to be at the center of the debate concerning technologies adoption [APA18], [CCT13], [GKS03]. Similarly, prior research has shown that consumers' privacy concerns are closely related to consumers' trust and thus to their propensity to adopt or reject Internet or e-commerce technology [Lu02]. In general, consumers' privacy concerns refer, amongst others, to improper access, improper collection, inadequate monitoring, improper analysis, improper transfer. For more dimensions of privacy concerns, see also Hong and Thong [HT13].

The previously mentioned infringements are not exhaustive but rather exemplary for the violations users can face when using technology and especially IAS. More specifically, since IAS' support performance (skill set, support quality) hinges on the amount of (personal) data it can gather and process, we argue that users' privacy concerns might be especially salient when using such intelligent assistants. On the one hand, to orchestrate and combine the amenities of a variety of IoT devices, services, and other intelligent agents to personalized and meaningful support for their users, IAS must gather and combine a variety of personal data and context-relevant information. Yet, on the other hand, the collection, processing, and storage of such data by a central entity such as an IAS raise several severe data privacy and security related concerns.

Given consumers' well-documented concerns towards the unauthorized and or opaque collection and processing of their data [Lu02], [MZH17], scholars proposed various mechanisms to support the trust-building process and thus enhance the chances of adoption. In this context, scholars reported that technology and service providers could foster consumers' trust with institution-based mechanisms (e.g., digital certifications, accreditations [Lu02]), process-based mechanisms (e.g., repeated purchases [Lu02] and return policy [CCT13]), or characteristic-based mechanisms (e.g., consumer age, sex, socio-demographic background [CCT13]).

Notably, not all trust-building mechanisms address consumers' privacy concerns equally effectively. In this regard, institution-based mechanisms are the most effective way to address consumers' privacy concerns [Lu02]. With its formal and marketable structure, institution-based trust mechanisms address privacy concerns through third-party guarantors pledging integrity and fairness [Lu02]. Since users can usually not see, understand or evaluate whether IAS or other services they use are handling their data

appropriately and as agreed, trust can theoretically be established by acquiring membership in an association, professional credentials, third-party certifications or through intermediary mechanisms, such as insurance, escrows, legal regulations [CCT13].








In theory, third-party certifications are expected to address some of the consumers' privacy concerns and thus instill their trust by testifying compliance with a variety of best practices or rules. In practice, however, both providers and consumers are facing a plethora of certification and accreditation programs and seals issued by industrial, national, international, private, or governmental institutions. These accreditations suggest compliance with underlying data protection principles. As such third-party certifications and seals vary significantly in terms of duration, quality requirements, and certification subject, consumers are increasingly unable to evaluate the value of such institution-based trust mechanisms. Therefore, understanding consumers' view on certifications as a trust-building mechanism becomes increasingly essential.

### **3 Study Design and Participants**

To investigate consumers' privacy concerns and preferences for certifications of IAS in IoT, we designed a survey based on an exemplary case study that visualizes the amenities of IAS in a networked IoT environment spanning the areas of smart public transportation, smart home, and connected car. All IoT areas were orchestrated by an IAS, which was in constant data exchange with IoT devices and other services to assist their user in a personalized way.

After introducing all participants to the IAS and IoT concept via the use case mentioned above, the participants were asked to answer a set of questions that documented their general attitude towards the IAS, their privacy concerns and preferences for trust-building mechanisms such as third-party certification, reputation, and return policy [CCT13], [MCK02]. Further, participants were shown a set of randomly selected EU and German seals (see Tab. 1) and were asked to indicate which of the presented seals they knew, whether they knew what the seals were certifying in detail, and whether they tend to trust or distrust such certifications. Ultimately, the participants were also asked to answer a set of questions that documented their demographic and socioeconomic status.

The online survey was implemented with Dynamic Intelligent Survey Engine (DISE) [SS12]. A marketing research entity that was hired to provide a sample representative of the population of Germany administered the survey to 400 individuals, from which 229 answered the questionnaire thoroughly. The final participant sample (N=229) closely mimics the German population.

Seal	Brief description
	Private company certifying online shops, performing cybersecurity assessments, and many other data security and privacy assessments.
	Private company certifying conformity assessments in the field of data protection and information security. The focus lies on IT systems, products, procedures, and processes.
	Registered association. Companies can use the seal if the affiliation is established by acquiring membership in the association.
	Registered association focused on small and medium-sized IT providers in Germany. Again, affiliation necessary in order to use the seal.
	Registered association. Companies can use the seal if they are members of the association, and the data of their products and services are hosted in Germany, and the hosting contract is governed exclusively by German law.
	Public organization. Certification based on the ISO standard 27001, which focuses on information security management systems.
	Private company. Attests a product's compliance with a list of ePrivacyseal criteria that are supposed to reflect the requirements imposed by the EU General Data Protection Regulation (GDPR). However, the seal is not an accredited procedure within the meaning of article 42, 43 GDPR.

Tab. 1: Overview third-party certifications shown in the study

#### 4 Users' Preferences for Certification and Accreditation

The results underscore existing theories postulating that privacy concerns are crucial for consumers' decision to adopt or reject new products and services. Further, it corroborates almost half (i.e., 51.5%) of the participants are still unsure if they would like to adopt such an IAS and IoT networked environment. 63% of the participants feel uncomfortable if the IAS would know their personal preferences. 79% of the participants are afraid that their personal information could be misused. Lastly, 42% of participants are fearful that IAS and IoT networks, could bring them into uncontrollable and dangerous situations. These findings reflect consumers' current state of distrust in IAS, IoT networks, and perhaps, by extension, in their providers.

Furthermore, the analysis results show that from the prompted certifications, the majority of participants know the established third-party seals issued by the TUEV (76%), 32% know the ISO certification seal, 22% are familiar with the BSI certification logo, and 17% know the "software made in Germany" logo. The remaining certifications are widely unknown, with less than 10% of the participants knowing one of them. Additionally, when asked about their detailed knowledge of the certifications with which they are familiar, participants admit that they do not know exactly which certifications

testify what, in detail. Even so, despite participants' lack of detailed knowledge on the individual certifications, 35% of the individuals in our survey would tend to trust certificates and hence certified products and providers. Thereby, it does not seem to matter whether certificates are issued by a non-profit association, a federal organization, or a private profit-driven third-party. What matters more is the sheer existence of a certification or accreditation of products, while the certification entity and the accreditation process itself only seems secondary, if at all important.

Group comparisons between participants who reported to be willing to adopt an IAS like the one presented in the study, with the groups of participants who were undecided, or would not adopt the IAS show that adopters and non-adopters differ from each other mainly in their willingness to trust certifications they do not know. In this regard, our analyses show that adopters are, on average, more willing to trust unknown certifications than non-adopters are eager to. What is also surprising is that the origin of the IAS and IoT technology provider, or the location where the data of the IAS is hosted does not seem to matter. On the contrary, our data shows that participants would value the price-performance ratio of technological products more than product origin. □

## 5 Discussion

The primary purpose of this paper was to provide certification recommendations for smart IoT networks in general and IAS in particular. Based on our participant sample, our study corroborates that technology adopters and non-adopters distinguish themselves significantly in terms of privacy concerns. In this regard, our study showed that adopters display lower levels of privacy concerns, while non-adopters are much more skeptical against IAS and networked IoT environments. Additionally, our results also suggest that trust-building mechanisms might be a powerful tool to address consumers' privacy concerns and thus foster technology adoption. More particularly, our data set shows that consumers have a high propensity and willingness to trust certifications, regardless of the issuer, the type of certifying entity, or the certification process. What seems to matter more is the sheer existence of a certification or accreditation. Against this background, it is advisable that companies developing and launching new intelligent systems and IoT environments try to leverage trust-building mechanisms, and in particular institution-based mechanisms in the form of third-party certifications to their advantage. Besides, with consumers having a high tendency to trust seals they do not know, companies and business networks might even want to think about founding their own certification association and issue their own certification seals.

Despite our efforts to ensure the validity and robustness of the presented results, the study has been conducted only with German participants. This might be an issue given the Germans' increased awareness regarding data security, data safety, and informational empowerment. Furthermore, the study presents only a snapshot in time and only for the given, fictional use case. Additionally, since the participants' attitudes and beliefs

captured in this study might depend on the use case shown, and thus might vary in another smart assistance scenario, future work should focus on other suitable use cases than the one presented in this study. Ultimately, because the IAS and IoT paradigm is yet to be materialized in the future while consumers' attitudes are changing over time, the research question addressed in this study should be repeated at a later stage in the development of such artifacts.

### **Acknowledgment**

This work has been funded by the German Federal Ministry for Economic Affairs and Energy (BMWi) as Part of the ENTOURAGE Project (01MD16009F).

### **Bibliography**

- [APA18] Adjerid, I., Peer, E.; Acquisti, A.: Beyond the privacy paradox: Objective versus relative risk in privacy decision making. *MIS Quarterly* 42/2, pp. 465–488, 2018.
- [CCT13] Chang, M. K., Cheung, W.; Tang, M.: Building trust online: Interactions among trust building mechanisms. *Information & Management* 50/7, pp. 439–445, 2013.
- [GKS03] Gefen, D., Karahanna, E.; Straub, D. W.: Trust and TAM in online shopping: an integrated model. *MIS Quarterly* 27/1, pp. 51–90, 2003.
- [HT13] Hong, W.; Thong, J. Y.: Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly* 37/1, pp. 275–298, 2013.
- [LL15] Lee, I.; Lee, K.: The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons* 58/4, pp. 431–440, 2015.
- [Lu02] Luo, X.: Trust production and privacy concerns on the Internet: A framework based on relationship marketing and social exchange theory. *Industrial Marketing Management* 31/2, pp. 111–118, 2002.
- [MCK02] McKnight, D. H., Choudhury, V.; Kacmar, C.: Developing and validating trust measures for e-commerce: An integrative typology. *Information systems research* 13/3, pp. 334–359, 2002.
- [MZH17] Mihale-Wilson, C., Zibuschka, J.; Hinz, O.: 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 (ECIS)*, Guimarães, Portugal, June 5-10, 2017, pp. 32–47, 2017.
- [Oi13] Oinas-Kukkonen, H.: A foundation for the study of behavior change support systems. *Personal and ubiquitous computing* 17/6, pp. 1223–1235, 2013.
- [SS12] Schlereth, C.; Skiera, B.: DISE: dynamic intelligent survey engine. In: *Quantitative marketing and marketing management*. Gabler Verlag, Wiesbaden, pp. 225–243, 2012.
- [Ve03] Venkatesh, V., Morris, M. G., Davis, G. B.; Davis, F. D.: User acceptance of information technology: Toward a unified view. *MIS Quarterly* 27/3, pp. 425–478, 2003.
- [WF15] Wortmann, F.; Flüchter, K.: Internet of things. *Business & Information Systems Engineering* 57/3, pp. 221–224, 2015.