Please quote as: Knote, R. (2019): Towards Solving the Personalization-Privacy Paradox for Smart Personal Assistants. In: Hawaii International Conference on System Sciences (HICSS). Maui, HI, USA.

Towards Solving the Personalization-Privacy Paradox for Smart Personal Assistants

Robin Knote
University of Kassel
robin.knote@uni-kassel.de

Abstract

The digital age has yielded information systems (IS) that reduce the complexity of our everyday lives. As such, smart personal assistants (SPAs) like Amazon's Alexa or Apple's Siri combine the comfort of intuitive natural language interaction with the utility of personalized and situation-dependent information and service provision. These systems collect and analyze users' personal data which raises information privacy concerns. The situational trade-off between enjoying personalization benefits and taking privacy risks is known as personalization-privacy paradox (PPP). Although approaches exist to solve the PPP by system design, SPAs novelty and technical sophistication require to research for adequate solutions. Hence, this research-in-progress report shows where we stand on our way towards solving the PPP for SPAs.

1. Motivation and Research Question

Within the sphere of technological advancements, IS' ability to collect and analyze users' personal and context data has long become useful for delivering personalized (i.e. user-tailored and context-dependent) services [6, 9]. Service providers use consumer data to improve services by learning about usage patterns and issues, deliver additional value to consumers, monetize their services and, consequently, gain competitive advantage [22, 40]. Furthermore, prior research has found that users are more likely to value and adopt IS if they provide personalized information and services [15, 36, 47]. However, the collection, storage and analysis of users' personal data in conjunction with a lack of trust and transparency about which data are collected and how they are used triggers users' privacy concerns [22, 41]. These concerns lead users to preserve information boundaries which prevent them from disclosing personal information [1, 2, 22, 31, 36]. However, since personal data is needed to provide personalized services and information, users find themselves confronted with situational trade-offs between personalization benefits and privacy risks, known as the *personalization-privacy paradox* [3, 22, 38]. The PPP theorizes that the intention of individuals to enjoy personalization benefits and, consequently, the willingness to be profiled for such purposes is a function of their disposition towards privacy. In other words, individuals who have a high disposition to value privacy often have a low willingness to share personal data for personalization benefits and vice-versa [3, 22, 31, 38].

While collecting personal data for personalization purposes has yet become common practice in online marketing and advertising [3, 38, 47], e-commerce [36] and other (foremost mobile) contexts [e.g., 28], recent technology developments build a new frontier of personalized information and service delivery through smart systems such as SPAs like Amazon Alexa, Apple's Siri, Microsoft Cortana and Samsung Bixby. These systems combine the comfort of intuitive natural language interaction with the utility of personalized service provision. In practice, SPAs unfold their potential in various forms and contexts [7], such as in smart home environments [10], in cars [5], in service encounters [46], or as support for the elderly or impaired [10]. The worldwide number of SPA users is expected to grow from 390 million in 2015 to 1.8 billion worldwide in 2021 [39]. As the user count increases, more and more anecdotal evidence appears suggesting that personalization benefits are accompanied by information privacy fears, such as that devices would 'listen' without being activated by the wake word and that providers analyze personal speech and text data [e.g., 1, 2]. This fear of privacy infringements combined with the lack of transparency will likely lead to distrust, reluctant usage behavior or even disuse. However, the growing user count indicates that social risks are often overseen, underestimated or condoned as they are outweighed by personalization benefits [3, 47].

Against this backdrop, my work is devoted to solving the PPP for SPAs by appropriate system design. Developing systems that are both as beneficiary and as privacy-protective as possible is important for at least two major reasons: first, from a normative perspective, protecting individuals from social risks resulting from system use is foremost the

responsibility of system design [18]. Second, from a behavioral perspective, users are more likely to adopt personalized *and* privacy-safe systems [38]. Hence, my goal is to answer the following research question:

RQ: How can the PPP be solved by design for smart systems such as SPAs?

With my completed research, I aim to contribute to theory by expanding the existing scope of PPP research to smart systems, a class of systems which is novel and technically sophisticated. Further, solving the PPP for the class of smart systems yield to prescriptive knowledge as part of a nascent design theory [13, 14]. From a practical perspective, the application of the results for IS development will lead to smart systems that provide personalization benefits while reducing privacy risks. Therefore, this research-in-progress report will set the stage by introducing the background, explain the methodology and present and discuss preliminary results.

2. Theoretical Background

2.1. The Personalization-Privacy Paradox

While the terms to describe the inherit conflict of the PPP differ from benefit vs. risk, gain vs. loss, approach vs. avoidance, the PPP always reflects an internal consumer conflict during decision making [27]. Prior studies have shown, that individuals who value information transparency are less likely to participate in personalized services [3, 22]. Especially in the digital age the degree of personalization of a service positively correlates with the number of data that must be collected from the user [32]. However, in case it becomes obvious that organizations gain financial profit out of personal data, users tend to avoid personalized services [30].

Awad and Krishnan's [3] survey among 400 online consumers shows that, especially where benefits are more apparent to consumers, information privacy concerns are mitigated in return for the advantages they enjoy from personalization [3, 17]. Other studies indicate privacy concerns' negative impact on the intention to adopt personalized services, while no significant relationship could be observed between privacy concerns and non-personalized services [36]. Xu et al. [47] as well as Sutanto et al. [38] investigate the PPP in the context of personalized marketing and found that, although personalization could somehow override privacy concerns [47], users of both personalized and privacy-safe applications engage in higher application usage behavior and saved adverts more frequently than those whose applications lack features of privacy protection. However, the PPP has not yet been addressed with regard to SPAs.

2.2. Smart Personal Assistants

Although SPAs have recently gained success on the consumer market, personal assistance provided by IS is not a novel research topic. In the past, research around question answering systems like BASEBALL [12], ELIZA [44], and LUNAR [45] was mainly conducted in the field of artificial intelligence and focused on expert systems in relatively limited domains [23]. However, technical evolutions such as cloud-based scalable infrastructures, natural language processing, semantic reasoning, voice recognition and voice synthesis have paved the way for this novel type of smart systems. SPAs interact with the user via natural language interfaces and offer many opportunities of service and information provision to reduce effort and complexity of users' everyday tasks [7]. They can broadly be defined as systems that use *"input such as the user's voice […] and contextual information to provide assistance by answering questions in natural language, making recommendations and performing actions"* [4, p. 223]. More technical definitions draw on the term agent. For example, Fuckner et al. [11, p. 89] consider an SPA to be a "*specialized intelligent artificial agent that helps users to do their activities […* as an *...] intermediary between humans and other agents in a multiagent environment.*" The term agent stresses that the SPA is an autonomous entity capable of perceiving and taking actions within its environment to achieve a certain goal [35], namely to assist the user conducting a specific task. Further, the SPA as an agent (e.g., Alexa) is able to interact with other agents, such as technical agents (e.g., a smart fridge) and human agents (users).

3. Methodology

Finding a solution for the PPP in SPA usage is a design research problem. I thus conduct a multi-step approach which basically follows the design research cycle of Vaishnavi and Kuechler [8]. Of the five phases the authors propose, this research-in-progress report presents results of the first two steps.

In the *Awareness of Problem* step, an exhaustive literature review [42, 43] of 115 SPA papers in IS, computer science and human-computer-interaction was conducted to identify functional principles and recurring design characteristics of SPAs [24]. An additional literature review was conducted to identify prior approaches to solve the PPP in other contexts to inform the design in the subsequent phases.

Based on the findings, an interdisciplinary, collaborative workshop [26, 29] with three academic IS experts (between 3 and 25 years of experience) and three academic public law and information privacy experts (between 2 and 40 years of experience) was conducted in the *Suggestion* phase. Therein, experts developed a shared understanding of SPA design, outlined different SPA usage scenarios and discussed general personalization benefits and privacy risks for the functional principles and the different design characteristics. As of now, a second workshop will follow in which the same group of experts together with experienced IS development practitioners conceptualize solutions for the PPP, specify system requirements and build a low-fidelity prototype of a personalized, privacy-safe SPA.

The next steps are as follows: Taking the prototype as a starting point, the actual artifact will be built in the *Development* stage. The goal is to develop an SPA which can be used for experimental performance measurement in the *Evaluation* stage. In other words, the to-be-developed SPA will allow for modular (de-)activation of personalization and privacy features. In this way, an experiment with a 2 x 3 factorial design will be conducted with the treatments personalization (low, high) and privacy-protection (or adequate proxy such as information-use transparency [22]; low, medium, high). Results are reflected and abstracted to the class of smart systems as design science knowledge in the *Conclusion* phase.

4. Preliminary Results

4.1. PPP in Current SPA Design

Within the interdisciplinary workshop, experts have contrasted personalization benefits and privacy risks according to SPA characteristics [24].

Context-awareness is the basic condition for providing personalized services. SPAs may be able to infer a user's situation including personal information from gathered context data. Information privacy, however, aims at avoiding the collection of such data and reducing personal reference. Further, although the collection of context data requires the user's consent, the typical length of privacy policies has been criticized to impose unrealistic cognitive burdens on individuals, so that only few actually consult them [21]. In addition, these policies and terms of services often lack transparency of data collection and utilization. A yet unanswered question is, however, whether increased transparency would positively or negatively influence use behavior.

Self-evolution relies on the processing of personal data to improve assistance over time according to individual usage patterns. For the case of SPAs, learning from user behavior is intimately connected with context-awareness. Hence, the more personal data a learning algorithm will process the better a user can be profiled and the steeper is the learning curve regarding which system behavior is appropriate in a given situation. Therefore, however, a vast amount of personal data is collected, combined and analyzed in the provider's data centers which is critical to information privacy. Therefore, some approaches suggest that purely local (i.e. on-device) processing of personal data for personalization purposes is more privacy-safe than remote processing [38]. However, analyzing rich media material such as video and audio requires a lot of computational resources and effort which makes technical feasibility of on-device learning problematic.

Anthropomorphism, or human-likeness, allows users to establish social structures with and around SPAs [33]. Although not directly referred to personal data collection and processing, human-like traits are suggested to have a social impact, e.g., by influencing social norms, which may increase the willingness to disclose personal data compared to interactions with non-anthropomorphic systems. Human-likeness may further offer increased transparency and trust by explaining system behavior in an empathic manner.

Multimodality, the provision of various interaction channels, is likely to have a positive impact on objective usability. However, each input is a potential entry point for data with personal reference. For example, an SPA could identify a person by the combination of voice and visual characteristics. Access to the system must be limited to a selected group of individuals.

Platform integration and extensibility means the connection of both physical objects and online profiles, which, despite of obvious comfort advantages, represent additional sources of personal data streams. For example, Alexa is connected to Amazon Web Services, which also serves as infrastructure for the Amazon shop. Hence, the SPA has access to existing data on the personal profile, shopping behavior and payment options. A personalized, privacy-safe SPA must provide the user control and transparency over data streams across connected infrastructures.

4.2. Prior PPP Solution Approaches

Most of the solutions for the PPP proposed by prior research focus on the usage of *privacy profiles* in which privacy settings for various situations, contexts, or certain applications can be defined [e.g.,

37]. Many other approaches to solve the PPP encompass *client-sided personalization*, i.e. saving private information on the respective user's device and using them for personalization purposes without disclosing them to software providers [e.g., 16, 37]. Another concept to align personalization and privacy demands is the *anonymization of user data* before their analyzation. The concept of anonymity is defined in varying degrees, so that users are either identifiable, pseudonymous, or totally anonymous [25, 34]. In this regard, two main alternatives of anonymity can be distinguished: either the user information are perturbed or multiple users with similar context-dependent parameters are combined to user groups which then receive personalized services based on the group data [20]. Other approaches to solve the PPP involve enabling users to *alter their personal data* prior to their analyzation. Thus, personal information can be specified or distorted depending on the individual user's privacy preferences [19]. Adapting prior PPP solution approaches for SPA design will be the main part of the upcoming interdisciplinary workshop with IS developers.

5. References

[1] https://www.wired.com/2017/02/murder-case-tests-alexas-devotion-privacy/, accessed 7-14-2018.

[2] https://www.wired.com/2016/12/alexa-and-google-record-your-voice/, accessed 7-14-2018.

[3] Awad, N.F. and M.S. Krishnan, "The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization", MIS Quarterly, 30(1), 2006, pp. 13–28.

[4] Baber, C., "Developing interactive speech technology", Taylor & Francis, Inc, 1993.

[5] Bengler, K., K. Dietmayer, B. Farber, M. Maurer, C. Stiller, and H. Winner, "Three Decades of Driver Assistance Systems: Review and Future Perspectives", IEEE Intelligent Transportation Systems Magazine, 6(4), 2014, pp. 6–22.

[6] Casillo, M., F. Colace, M. de Santo, S. Lemma, and M. Lombardi, "A Context-Aware Mobile Solution for Assisting Tourists in a Smart Environment", in Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS) 2017. 2017.

[7] Cowan, B.R., N. Pantidi, D. Coyle, K. Morrissey, P. Clarke, S. Al-Shehri, D. Earley, and N. Bandeira, ""What can i help you with?": Infrequent Users' Experiences of Intelligent Personal Assistants", in Proceedings of the 19th International Conference on Human-Computer Interaction with Mobile Devices and Services - MobileHCI '17, Vienna, Austria. 2017.

[8] http://www.desrist.org/design-research-in-information-systems/, accessed 7-14-2018.

[9] Dey, A.K. and G.D. Abowd, "Towards a Better Understanding of Context and Context-Awareness", in Proceedings of the PrCHI 2000 Workshop on the What, Who, Where, When and How of Context-Awareness, Conference on Human Factors in Computing Systems (CHI 2000), New York, NY. 2000.

[10] Fernando, N., F.T.C. Tan, R. Vasa, K. Mouzaki, and I. Aitken, "Examining Digital Assisted Living: Towards a Case Study of Smart Homes for the Elderly", in Proceedings of the 24th European Conference on Information Systems (ECIS). 2016: Istanbul, Turkey.

[11] Fuckner, M., J.-P. Barthes, and E.E. Scalabrin, "Using a personal assistant for exploiting service interfaces", in Proceedings of the 2014 IEEE 18th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Hsinchu, Taiwan. 2014.

[12] Green Jr., B.F., A.K. Wolf, C. Chomsky, and K. Laughery, "Baseball: An automatic question-answerer", Proceedings of the Western Joint Computer Conference, 1961.

[13] Gregor, S. and A.R. Hevner, "Positioning and Presenting Design Science Research for Maximum Impact", MIS Quarterly, 37(2), 2013, pp. 337–355.

[14] Gregor, S. and D. Jones, "The Anatomy of a Design Theory", Journal of the Association for Information Systems, 8(5), 2007, pp. 312–335.

[15] Guo, X., X. Zhang, and Y. Sun, "The privacy-personalization paradox in mHealth services acceptance of different age groups", Electronic Commerce Research and Applications, 16, 2016, pp. 55–65.

[16] Ha, J., J.-H. Lee, and S. Lee, "EPE: An Embedded Personalization Engine for Mobile Users", IEEE Internet Computing, 18(1), 2014, pp. 30–37.

[17] Hann, I.-H., K.-L. Hui, T. Lee, and I. Png, "Online information privacy: Measuring the cost-benefit trade-off", in Proceedings of the 23rd International Conference on Information Systems, Barcelona, Spain, December 15-18. 2002.

[18] Hoffmann, A., T. Schulz, J. Zirfas, H. Hoffmann, A. Roßnagel, and J.M. Leimeister, "Legal Compatibility as a Characteristic of Sociotechnical Systems", Business & Information Systems Engineering, 57(2), 2015, pp. 103–113.

[19] Iqbal, Z., J. Noll, S. Alam, and M.M.R. Chowdhury, Toward User-Centric Privacy-Aware User Profile Ontology for Future Services, Athens/Glyfada, Greece, 2010.

[20] Ishitani, L., V. Almeida, and W. Meira, "Masks: Bringing anonymity and personalization together - Security & Privacy Magazine, IEEE", IEEE Security and Privacy, 99(3), 2003, pp. 18–23.

[21] Jensen, C., C. Potts, and C. Jensen, "Privacy Practice of Internet Users: self-reports versus observed behavior",

International Journal of Human-Computer Studies, 63(1), 2005, pp. 203–227.

[22] Karwatzki, S., O. Dytynko, M. Trenz, and D. Veit, "Beyond the Personalization–Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization", Journal of Management Information Systems, 34(2), 2017, pp. 369–400.

[23] Kincaid, R. and G. Pollock, "Nicky: Toward a Virtual Assistant for Test and Measurement Instrument Recommendations", in 2017 IEEE 11th International Conference on Semantic Computing (ICSC). 2017.

[24] Knote, R., A. Janson, L. Eigenbrod, and M. Söllner, "The What and How of Smart Personal Assistants: Principles and Application Domains for IS Research", Multikonferenz Wirtschaftsinformatik (MKWI).

[25] Kobsa, A. and J. Schreck, "Privacy through pseudonymity in user-adaptive systems", ACM Transactions on Internet Technology, 3(2), 2003, pp. 149–183.

[26] Kolfschoten, G.L., P.B. Lowry, D.L. Dean, Vrede de GJ, and R.O. Briggs, "Patterns in Collaboration", in Collaboration systems: Concept, value, and use, J.F. Nunamaker, N.C. Romano, and R.O. Briggs, Editors. 2014. Routledge: London, New York.

[27] Lee, J.-M. and J.-Y. Rha, "Personalization–privacy paradox and consumer conflict with the use of location-based mobile commerce", Computers in Human Behavior, 63, 2016, pp. 453–462.

[28] Lee, N. and O. Kwon, "A privacy-aware feature selection method for solving the personalization-privacy paradox in mobile wellness healthcare services", Expert systems with applications, 42(5), 2015, pp. 2764–2771.

[29] Leimeister, J.M., Collaboration Engineering: IT-gestützte Zusammenarbeitsprozesse systematisch entwickeln und durchführen, Springer, Berlin, 2014.

[30] Liu, Z., J. Shan, R. Bonazzi, and Y. Pigneur, Privacy as a Tradeoff: Introducing the Notion of Privacy Calculus for Context-Aware Mobile Applications, Waikoloa, USA, 2014.

[31] Norberg, P.A., D.R. Horne, and D.A. Horne, "The privacy paradox: Personal information disclosure intentions versus behaviors", Journal of Consumer Affairs, 41(1), 2007, pp. 100–126.

[32] Pappas, I.O., M.N. Giannakos, and V. Chrissikopoulos, Personalized Services in Online Shopping: Enjoyment and Privacy, London, UK, 2012.

[33] Purington, A., J.G. Taft, S. Sannon, N.N. Bazarova, and S.H. Taylor, ""Alexa is my new BFF"", in Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems, Denver, Colorado, USA. 2017. ACM Press: New York, New York, USA.

[34] Qian, H. and C.R. Scott, "Anonymity and Self-Disclosure on Weblogs", Journal of Computer-Mediated Communication, 12(4), 2007, pp. 1428–1451.

[35] Russell, S.J. and P. Norvig, Artificial intelligence: A modern approach, Prentice Hall, New Jersey, 2003.

[36] Sheng, H., F.F.-H. Nah, and K. Siau, "An experimental study on ubiquitous commerce adoption: Impact of personalization and privacy concerns", Journal of the Association for Information Systems, 9(6), 2008, p. 344.

[37] Shou, L., H. Bai, K. Chen, and G. Chen, "Supporting Privacy Protection in Personalized Web Search", IEEE Transactions on Knowledge and Data Engineering, 26(2), 2014, pp. 453–467.

[38] Sutanto, J., E. Palme, C.-H. Tan, and C.W. Phang, "Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users", MIS Quarterly, 37(4), 2013, pp. 1141–1164.

[39] https://www.tractica.com/newsroom/press-releases/the-virtual-digital-assistant-market-will-reach-15-8-billion-worldwide-by-2021/, accessed 8-20-2017.

[40] Thirumalai, S. and K.K. Sinha, "To Personalize or Not to Personalize Online Purchase Interactions: Implications of Self-Selection by Retailers", Information Systems Research, 24(3), 2013, pp. 683–708.

[41] Treiblmaier, H. and I. Pollach, "Users' Perceptions of Benefits and Costs of Personalization", in Proceedings of the Twenty-Eighth Conference on Information Systems, Montreal, Canada. 2007.

[42] Vom Brocke, J., A. Simons, K. Riemer, B. Niehaves, R. Plattfaut, and A. Cleven, "Standing on the Shoulders of Giants: Challenges and Recommendations of Literature Search in Information Systems Research", Communications of the Association for Information Systems, 37(1), 2015.

[43] Webster, J. and R.T. Watson, "Analyzing the Past to Prepare for the Future: Writing a Literature Review", MIS Quarterly, 26(2), 2002, pp. xiii–xxiii.

[44] Weizenbaum, J., "ELIZA—a computer program for the study of natural language communication between man and machine", Communications of the ACM, 9(1), 1966, pp. 36–45.

[45] Woods, W.A. and R. Kaplan, "Lunar rocks in natural English: Explorations in natural language question answering", Linguistic structures processing, 5, 1977, pp. 521–569.

[46] Xu, A., Z. Liu, Y. Guo, V. Sinha, and R. Akkiraju, "A New Chatbot for Customer Service on Social Media", in Proceedings of the Annual CHI Conference on Human Factors in Computing Systems, Denver, Colorado, USA. 2017. ACM: New York, NY.

[47] Xu, H., X.R. Luo, J.M. Carroll, and M.B. Rosson, "The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing", Decision support systems, 51(1), 2011, pp. 42–52.