Ongoing Research: Trust in Automation in the Context of Privacy

Alina Stöver
Technische Universität Darmstadt
Darmstadt, Germany
stoever@psychologie.tu-darmstadt.de

CONF '22, Jan 1 - Dec 31 2022, Authorberg.
 ACM 978-1-xxxx-yyyy-z/zz/zz…$zz.00.
unique doi string will go here

Abstract
This extended abstract introduces the new research topic of trust in automation in the context of privacy. Since in the course of digitalization more and more user data are being captured, users value their privacy and at the same time feel desperate. To help users with navigating in this more complex environment we envision an automated system (called AlterEgo) to represent the users' interests. In order to gain a meaningful user-system-interaction, the establishment of a trustful relationship is crucial. Therefore, we aim to investigate the role of trust in automation in the context of privacy in three sequential studies.

Author Keywords
Trust in automation; Privacy; privacy assistant; Human-centered-design; Privacy-enhancing technology

ACM Classification Keywords
Security and privacy~Usability in security and privacy • Security and privacy~Privacy protections • Human-centered computing~Empirical studies in HCI

Definition 1: Privacy "*The claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." [16]*

Definition 2: Privacy-Enhancing Technologies *"[…] include any technology that protects or enhances an individual's privacy, including facilitating individuals' access to their rights under the Data Protection Act 2004."* [3]

Definition 3: Automation *"Technology that actively selects data, transforms information, makes decisions, or controls processes."* [1]

Definition 4: Trust "*The willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party.*" [12]

Introduction

In today's world that is shaped by digitalization and connecting people, products and services the organizations' hunger for data increases as many companies have shifted to a business model that is formed around their users' data. In contrast, for many users the privacy (s. Definition 1) of their personal information, their online communication and their online behavior is very important [3]. At the same time, there is a discrepancy between privacy attitude and behavior. This phenomena is widely discussed in research literature and referred to as *privacy paradox* [5]. Users perceive a loss of control over how companies collect and use their data [13]. There are different approaches to empower users and protect their privacy. From a legal perspective, the EU general data protection regulation is an important approach. From a technical perspective, privacy-enhancing technologies (s. Definition 2) play an important role. From a user perspective, the use of an automated system (s. Definition 3) that functions as a digital representative of the user (called AlterEgo) could support users in an obscure and overstraining issue of privacy protection.

Digital Representative of the User (AlterEgo)

We envision the AlterEgo (s. Figure 1) to be an automated system that understands the users´ beliefs and intended behavior regarding their privacy protection. The AlterEgo should support users to resolve the privacy paradox and make better decisions regarding their privacy protection. At the same time, the AlterEgo relieves the users by making decisions for them. In order to gain a meaningful user-AlterEgo-interaction, the establishment of a trustful relationship is crucial.

The Role of Trust

Trust (s. Definition 4) in this case has a double function: On the one hand, we are dealing with trust in the context of privacy, and on the other hand, since AlterEgo is going to be an automated system, the users trust in automation needs to be built.

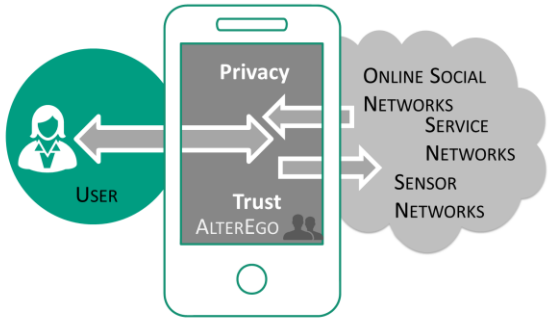

Figure 1: The concept of AlterEgo - a digital representative of the user that supports her/him in privacy protection.

Theoretical Background

Privacy and Trust

Research literature shows that the concept of trust and the concept of privacy often depend on each other [6, 9]. The decision of sharing a private information often goes with the intention to trust the person or entity with the shared information [6, 8]. Studies have shown that a well-integrated privacy mechanism can support the establishment of user trust [6, 8].

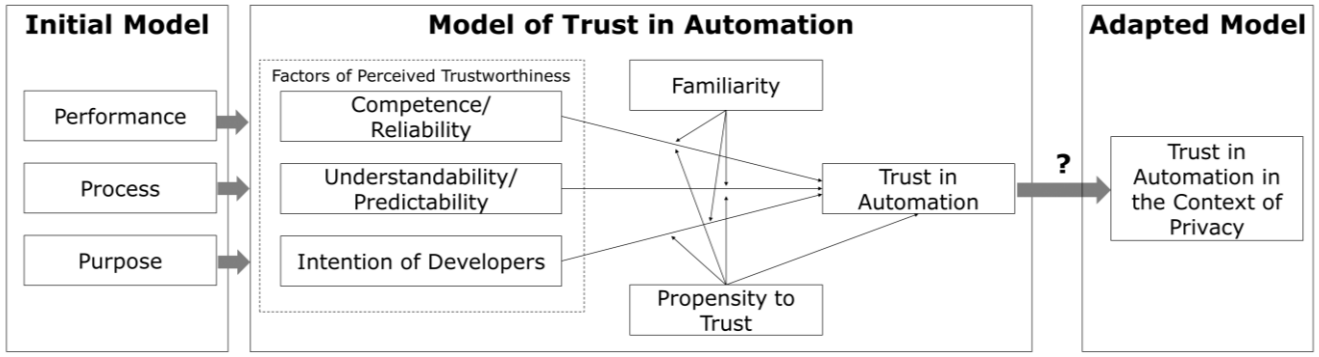

Figure 2. Past research leads to the question if trust in automation also supports trust in automation in the context of privacy. The displayed initial model is invented by Lee and See [5] and enhanced by Körber [7]. The figure is based on Körber [7].

Trust in Automation

Trust in the context of technology is a primary reason for acceptance and can also define how people interact with technology [4, 9, 15]. Building a model of trust in automation, Lee and See [7] follow the trust definition of Mayer et al. (s. Definition 4) and adapt it to the context of automation. They define three dimensions, performance, process, and purpose, as the basis for trust in automation. Building on that, Körber [10] defines trust in automation as *"the attitude of a user to be willing to be vulnerable to the actions of an automated system based on the expectation that it will perform a particular action important to the user, irrespective of the ability to monitor or to intervene."* [10]. He also suggests three factors of perceived trustworthiness (s. Figure 2). In addition, Körber defines the propensity to trust as a determinant for trust and familiarity as a moderator.

Research Goal

Researchers have heavily investigated trust in automation and trust in the context of privacy. Research that combines those two areas is still missing. To address this gap, we aim to investigate the role of trust in automation in the context of privacy.

Research Design

In order to meet the research objectives three studies will be conducted. The studies aim to (a) create a better understanding of trust in automation in the context of privacy, (b) develop and evaluate a prototype of AlterEgo, and (c) empirically investigate the magnitude of influence of the different factors on trust in automated systems in the context of privacy.

Study 1

Objective

Through Study 1 we aim to gain a better understanding of the role of trust in automation in the context of privacy from a users' perspective. We aim to investigate whether Körbers (s. Figure 2) model of trust in automation is appropriate for the context of privacy.

Method

In order to gain an understanding of the subject, semi-structured interviews with users will be conducted [2].

The answers will be evaluated using qualitative content analysis [11].

Results
As a result, we expect to gain a deeper understanding what needs to be considered in order to establish a trustworthy user-AlterEgo-relationship. Furthermore, we will extend the trust in automation model of Körber [10] to the context of privacy.

Study 2

Objective
Study 2 will accompany the development and evaluation of a prototype of AlterEgo.

Method
The development and evaluation of a prototype of AlterEgo will follow a user-centered-design process [1]. Therefore, we will follow five steps:

1. Specifying user requirements with the method "Focus groups" [14]
2. Developing a computer-based prototype of AlterEgo
3. Conducting a heuristic evaluation with usability experts
4. Revising the prototype
5. Testing the prototype with the method "User Test" [14]

Results
The result of Study 2 will be an evaluated prototype of AlterEgo that meets users' needs and whom users will trust.

Study 3

Objective
Study 3 will build on the enhanced trust in automation model (result of Study 1), using the prototype of AlterEgo (result of Study 2). Study 3 aims to empirically examine the influence of individual factors on trust in automation in the context of privacy.

Method
In a laboratory experiment, the test subjects will interact with AlterEgo. The experimental conditions will differ to the extent that individual aspects of the AlterEgo are modified (e.g. degree of reliability, understandability). Trust in automation will then be surveyed with a questionnaire [10].

Results
Empirical evidence of the magnitude of influence of different factors of trust in automation in the context of privacy will be gathered to support the current research and spark further research questions. The findings will be used to further enhance the AlterEgo and increase its practical relevance.

Acknowledgments

This work has been funded by the DFG as part of project "A.2: User Sensitization for Privacy and Trust" within the RTG 2050 "Privacy and Trust for Mobile Users".

References

[1] Chadia Abras, Diane Maloney-Krichmar, and Jenny Preece. 2004. User-centered design. *Bainbridge, W. Encyclopedia of Human-Computer Interaction. Thousand Oaks: Sage Publications* 37, 4, 445–456.

[2] Alexander Bogner, Beate Littig, and Wolfgang Menz. 2014. *Interviews mit Experten: eine praxisorientierte Einführung*. Springer-Verlag.

[3] European Commission. 2016. *ePrivacy: consultations show confidentiality of communications and the challenge of new technologies are key questions* (2016). Retrieved May 31, 2019 from https://ec.europa.eu/digital-single-market/en/news/eprivacy-consultations-show-confidentiality-communications-and-challenge-new-technologies-are.

[4] Gefen, Karahanna, and Straub. 2003. Trust and TAM in Online Shopping: An Integrated Model. *MIS Quarterly* 27, 1, 51. DOI: https://doi.org/10.2307/30036519.

[5] Nina Gerber, Paul Gerber, and Melanie Volkamer. 2018. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security* 77, 226–261. DOI: https://doi.org/10.1016/j.cose.2018.04.002.

[6] Giovanni Iachello and Jason Hong. 2007. End-User Privacy in Human-Computer Interaction. *FNT in Human-Computer Interaction* 1, 1, 1–137. DOI: https://doi.org/10.1561/1100000004.

[7] John D. Lee and Katrina A. See. 2004. Trust in Automation: Designing for Appropriate Reliance. *Human factors,* 46(1), 50–80.

[8] D. N. Jutla and P. Bodorik. 2005. Sociotechnical Architecture for Online Privacy. *IEEE Secur. Privacy Mag.* 3, 2, 29–39. DOI: https://doi.org/10.1109/MSP.2005.50.

[9] Bastian Könings, Florian Schaub, and Michael Weber. 2016. Privacy and Trust in Ambient Intelligent Environments. In *Next Generation Intelligent Environments*, Stefan Ultes, Florian Nothdurft, Tobias Heinroth and Wolfgang Minker, Eds. Springer International Publishing, Cham, 133–164. DOI: https://doi.org/10.1007/978-3-319-23452-6_4.

[10] Moritz Körber. Theoretical considerations and development of a questionnaire to measure trust in automation. *Proceedings 20th Triennial Congress of the IEA* 2019.

[11] Udo Kuckartz. 2016. *Qualitative Inhaltsanalyse. Methoden, Praxis, Computerunterstützung (Grundlagentexte Methoden, 3., überarbeitete Auflage)*. Weinheim: Beltz Juventa.

[12] Roger C. Mayer, James H. Davis, and F. D. Schoorman. 1995. An integrative model of organizational trust. *Academy of management review* 20, 3, 709–734.

[13] Lee Rainie, Sara Kiesler, Ruogu Kang, and Madden Mary. 2013. *Anonymity, Privacy, and Security Online* (2013). Retrieved May 31, 2019. from https://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/.

[14] Michael Richter and Markus D. Flückiger. 2016. *Usability und UX kompakt: Produkte für Menschen* (4. Aufl. 2016), Berlin, Heidelberg.

[15] Keng Siau, Hong Sheng, Fiona Nah, and Sid Davis. 2004. A qualitative investigation on consumer trust in mobile commerce. *IJEB* 2, 3, 283. DOI: https://doi.org/10.1504/IJEB.2004.005143.