TOWARDS EXPLAINING THE WILLINGNESS TO DISCLOSE PERSONAL SELF-TRACKING DATA TO SERVICE PROVIDERS

Research in Progress

Buchwald, Arne, EBS Business School, Germany, arne.buchwald@ebs.edu

Letner, Albert, University of Bayreuth, Germany, albert.letner@uni-bayreuth.de

Urbach, Nils, University of Bayreuth, Germany, nils.urbach@uni-bayreuth.de

Von Entreß-Fürsteneck, Matthias, University of Bayreuth, Germany, matthias.entress-fuersteneck@uni-bayreuth.de

The authors are listed alphabetically and they contributed equally to the paper.

Abstract

Users of digital self-tracking devices increasingly benefit from multiple services related to their self-tracking data. Simultaneously, service providers are dependent from these data to offer such services. Thereby, the willingness of users to provide such personal data heavily depends on benefits and risks associated with the disclosure. In this regard, the aim of our research is to investigate the factors influencing the willingness to disclose personal self-tracking data to service providers. So far, IS research has largely focused on private information disclosure in social media and little in the health and behavior context. To advance research in this area, we develop a conceptual model based on the privacy calculus by building on established information disclosure and privacy theories. With our research, we aim at contributing to both a better theoretical understanding in the fields of privacy and information disclosure and giving practical implications for service provider.

Keywords: Privacy calculus, self-tracking, personal data, service provider, user behavior.

1 Introduction

In the digital age, services become more and more dependent on data. They drive personalization of already established services or enable the creation of innovate new ones. Self-tracking data are a type of such data. They are used in contexts such as social networking services or fitness analytics and become of increasing interest for services provided – for example by physicians or health insurances. The collection of such data is done by self-tracking devices. In general, self-tracking, (also known as life-logging, quantified-self, personal analytics, and personal informatics) is the current trend to collect data about specific features of life through mobile and wearable digital devices (Lupton, 2014a). Self-tracking devices are placed in the category of wearable electronics and/or multi-sensor platforms in the field of the Internet of Things (Swan, 2012). These devices can take the shape of smartwatches, wristband sensors, wearable sensor patches, artificial reality-augmented glasses, brain computer interfaces, or wearable body metric textiles (Swan, 2012). They enable the individual to capture data about daily activities, exercises, vital parameters, disease symptoms, or nutrition, among others (Gimpel et al., 2013). Due to the development of new technologies and decreasing sensor sizes, self-tracking becomes not only increasingly convenient (Gimpel et al., 2013; Lupton, 2014b), but also enables users to capture more and more aspects of life.

Major players in the consumer electronic market, such as Apple, Google and Microsoft, as well as specialized producers, like fitbit or Jawbone, launched their own self-tracking devices (e.g., Apple Watch, Android Wear, Fitbit Charge, Jawbone UP and Microsoft Band) and start to build up software and hardware ecosystems around their devices with open APIs, enabling third parties to offer services based on the collected data (e.g. runtastic, nike+). Considering the expectation that the shipment of solely wearable self-tracking devices will grow from 102 million units in 2016 to more than 224 million units in 2020 (IDC, 2016), we expect the service sector around such devices to grow as well.

However, without the agreement of the service recipients to share their individual self-tracking data, the service providers cannot (fully) deliver their services. Thus, the willingness of the service recipient to share the personal data gathered through a self-tracking device is essential for the success of the service provider. In contrast to other types of private information, self-tracking devices record highly personal (and thus confidential) vital, body and fitness data. Hence, the privacy and security as well as the type and extent of the incentives by the service providers might be important factors for the service success. However, we currently do not know to what extent the different factors influence the willingness to disclose information, to what extent the sensitivity and criticality of the data affect these relationships and which role the type of service provider plays. While we draw on the privacy research stream to inform our research, the phenomenon in this specific context – the conscious disclosure of highly personal vital, body and fitness data to third parties – has not been addressed by research so far. With our study, we want to close this research gap by answering the following research question:

RQ: What are the factors that influence the willingness of an individual to disclose personal self-tracking data to service providers?

To do so, we develop a research model that is based on the comprehensive APCO Macro Model (Antecedents, Privacy Concerns, Outcomes) of Smith et al. (2011), but focusing solely on the link between the privacy calculus and the behavioral reactions. In addition, we contribute to the specific context of self-tracking by adapting the characteristics of the privacy calculus accordingly and integrate two moderators which contribute to the criticality and sensitivity of the self-tracking data.

We organize this article as follows: Section 2 outlines the theoretical foundations of our study by introducing established and related theories in the field of privacy and information disclosure. In Section 3, we describe the research context, the development of our constructs and propositions and finally synthesize them into a conceptual model. In Section 4, we conclude with the limitations, the future research process and point out our main contributions.

2 Foundations

With rising demand for personal services, such as healthcare, education, and entertainment (Barrett et al., 2015), providers create new and improve old services. Through innovative features, often customized to the individual, more and more private information about the person are required. For instance, in case of self-tracking data, insurance companies would be able to calculate risks associated with insurance takers more accurately by considering the health status of a policy group and thereby the current monetary risk associated with this group. Physicians would be enabled to offer additional services, such as continuous remote monitoring of the health status, reducing the need for personal consultations. Companies within the e-commerce or social media industry could advertise products specifically linked to the tracked fitness activity of a person. To realize such advantages, service providers need to understand a person's behaviour regarding information privacy. Privacy of information comprises individuals' means and capabilities for controlling to what extent their data and information are exchanged with and utilized by others (Culnan and Bies, 2003; Stone et al., 1983).

With the establishment of laws to protect private data (Smith et al., 2011), privacy was considered to be a human right and people became able to decide to what extent information about themselves should be disclosed. Self-disclosure describes the action of uncovering personal information, such as

locations or activities (Posey et al., 2010). There, according to communication privacy management theory (CPM), people face a conflict between privacy and disclosure while determining whether to reveal private data and information or not (Petronio, 1991). Even though people report high concerns regarding their privacy, they voluntarily give in personal information in numerous events. This observation is known as the privacy paradox (Norberg et al., 2007). The reason for this lies in people viewing privacy less as a right but rather as commodity (Campbell and Carlson, 2002; Davies, 1997; Garfinkel, 2001; Smith et al., 2011). Within this view as a commodity, it is possible to assign privacy an economic value, which is the basis for cost-benefit analysis and trade-offs (Campbell and Carlson, 2002; Davies, 1997; Smith et al., 2011). Consumers, which are asked for providing private information to receive a product or service, perform cost-benefit analysis to evaluate the consequences they would encounter in return for the disclosed information, and respond accordingly. Such consequences are the perceived benefits as well as risks. Exemplary benefits are a better service through personalization or financial rewards. However, any information exchange entails considerable uncertainty or is subject to opportunistic behaviors of the receiver. For instance, the receiver of the private data may utilize them for different purposes, then those declared. Therefore, the following consequences of the information disclosure may be too complex to anticipate beforehand and contain a personal risk. Results by Keith et al. (2013) suggest these perceived risks to be more important for explaining information disclosure compared to perceived benefits. This process of comparing benefits and risks is understood as privacy calculus, with drivers and inhibitors effecting the decision process at the same time regarding whether to disclose information or not (Culnan and Bies, 2003; Dinev et al., 2009).

Since concepts such as benefits and risks from information disclosure differ from situation to situation, it is vital to analyze information disclosure context specific in order to comprehend the person's information sharing behavior (Culnan and Bies, 2003; Smith et al., 2011), especially how sensitive and critical the data to be shared are. In this respect, the disclosure of self-tracking associated data is of medical and behavioral nature, which can be considered one of the most private data possible. Based on those information, several stakeholders may gain an intention to change their relationship with a person, e.g. service personalization (Awad and Krishnan, 2006). For instance, a health insurance company may charge a different fee based on a person's health and activity status or a physician may increase the quality of his service through personalization of treatments due to more health information. Additionally, data can be shared via social networking services with the social environment to receive a social rewards (Le Wang et al., 2017).

Because of the higher risks and implications involved in comparison to other private information such as shopping behavior or social media usage, it is likely, that peoples' disclosing behavior differs from other private information contexts. This study aims at answering this questions in a highly personal data context by analyzing private information disclosure in the self-tracking domain.

In addition, there is a difference regarding to what extent people are aware of giving away private data. Research regarding private information disclosure primarily analyses sharing information within the domain of social media or to some extent within the e-commerce and smart phone app area (Green et al., 2016; Huang, 2016; Contena et al., 2015; Chen, 2013; Forest and Wood, 2012). There is evidence for users unconsciously accepting terms and conditions about their privacy disclosure (Buck et al., 2014; Kim, 2016). Thus, users are not aware of the extent of private information disclosure (Stutzman et al., 2013). To our knowledge, little research has been carried out in the area of full awareness about information disclosure, where people are completely informed about the type of data, anonymity level, purpose of information etc. This is particular of relevance to distinguish the influence of constructs on disclosing behavior between the different service provider to share self-tracking data with (physicians, insurance, etc,).

3 Conceptual Development

After having outlined a brief summary of current research in the area of privacy, we will now proceed to explaining the research context, the different constructs, propositions, and the research model we will draw upon for explaining an individual's willingness to disclose information.

3.1 Research context

As indicated earlier and described by Smith et al. (2011), it is "impossible to develop a one size-fits-all conceptualization of general privacy" (p. 1002). Hence, we subsequently describe the specific research context of private information disclosure we consider in our model. As underlying theory, we follow the privacy calculus concept (Culnan and Bies, 2003; Dinev et al., 2009), which is grounded on the calculus of behavior theory (Laufer and Wolfe, 1977; Culnan and Armstrong, 1999). On this basis, we concentrate on the individual and private usage of self-tracking devices, which have a focus on the collection, processing and analysis of activity, vital and body data. These tasks are covered by devices such as smartwatches, wristbands, patches, clip-on devices, wireless weight scales or blood pressure monitors (Lupton, 2013; Swan, 2012). Further, depending on the service, self-tracking data can be shared in different ways referring to the aggregation level, e.g. the variety, the volume and the velocity. Within our study, we set the context that the data can be assigned to the user, is shared instantly without any aggregation and includes all collected data. Finally, concerning the third-party exchange partners (usually service providers), we expect significant different results for our research model depending on which exchange partner is considered. Nowadays, users of self-tracking devices can share data with service providers which enable them to connect to their social group, e.g. family and friends, social media or special online platforms such as fitness-tracking platforms (e.g. runtastic, nike+). Prospectively, it can be assumed that in the near future, it will be possible to share data with a larger group of exchange partners which offer common services such as physicians, health insurance companies, pharmacies, research institutes or sport and fitness clubs. We assume that users will evaluate the risks and benefits for each service provider separately and calculate the privacy calculus accordingly. Hence, within the validation of our model we will cluster the research participants beforehand in terms of the considered service provider.

3.2 Constructs and propositions

We investigate the relation between characteristics of the privacy calculus and the behavioral reactions of self-tracking users instead of intentions, because past research indicates that behaviors do not match actual intentions due to the interference of the privacy paradox (Smith et al., 2011; Norberg et al., 2007). Behavioral reactions can become visible as one's willingness to disclose information and/or the engagement in commerce (Smith et al., 2011). However, services in the self-tracking domain usually do not engage in typical commerce interactions. We therefore relate to the willingness to disclose information as the dependent variable. For our independent variables, we focus on the characteristics of the privacy calculus, which splits into privacy risks and privacy benefits. While privacy risks are treated as a single-dimensional construct, the privacy benefits further divide into the constructs – financial rewards (e.g. Hann et al., 2007; Hui et al., 2006; Xu et al., 2009), personalization benefits (Chellappa and Sin, 2005; White, 2004) and social adjustment benefits (Lu et al., 2004). Within our research, we rely on these three benefits constructs but adapt personalization benefits to service improvement benefits to fit to the context of self-tracking. We further add two new moderating constructs in the context of self-tracking into our model – data criticality and data sensitivity. Both constructs are integrated on the assumption that users of self-tracking devices consider the fact that highly personal vital, body and fitness data are the subject of sharing, which could cause unfavorable implications for the user.

Privacy risks

Privacy risks are defined as "the degree to which an individual believes that a high potential for loss is associated with the release of personal information to a firm" (Smith et al., 2011, p. 1001). The manifestation of the risk is the result of a calculation of the likelihood of negative consequences and the perceived severity of those consequences (Peter and Tarpey, 1975). Several studies verified the negative effect of perceived risk on intentions or willingness to disclose information (e.g. Zimmer et al., 2010; Dinev and Hart, 2006; Pavlou and Gefen, 2002). Following them, we assume, that privacy risks are also a key negative influencer for the willingness to disclose information in the self-tracking context, since users share highly personal activity, vital and body data. In the case of a loss of control over these personal data, the severity of consequences can be serious and influences one's social and financial status sustainably. For example, health insurance companies could increase fees of a client or employers could disadvantage an employee if they get access to self-tracking data that is not in favor of its user. Hence, we posit:

P1: Privacy risks have a negative effect on the willingness to disclose information.

Social adjustment benefits

Social adjustment benefits are named as one of three privacy benefits factors, which positively influence the willingness to disclose information. (Smith et al., 2011). It is defined as "the establishment of social identity by integrating into desired social groups" (Lu et al., 2004, p. 572). Lu et al. (2004) showed that not only financial rewards but also social adjustment benefits can be used by Internet businesses to induce customers to disclose their personal information. With social adjustment benefits, people can fulfil their need for affiliation, a key driver for human behavior. There are three major reasons why people seek for affiliation – positive stimulation, attention and social comparison (Lu et al., 2004). Positive stimulation can be achieved when people get gratification from harmonious relationships and a sense of communion, while attention comes from an enhanced feeling of self-worth when others focus on them. Lastly, social comparison can be reached when people reduce the ambiguity about their social context when they can compare themselves with reference groups (Lu et al., 2004).

We argue, that in the context of self-tracking all three reasons for affiliation can be fulfilled by disclosing self-tracking data via service-providers. Positive stimulation is given by the possibility to connect to others who share the same interest in self-tacking, for example by sharing data via a fitness-tracking platform. Also, third-parties can react to the provided self-tracking data (e.g. with recommendations or appreciation), therefore attention as a social reward is given as well. Lastly social comparison in the context of self-tracking is also possible directly and indirectly. By comparing data via fitness-tracking platforms with friends, family and others who also use self-tracking devices, users can directly relate their data to them. Indirectly, users can compare their data to an unknown peer-group, e.g. when they share the data to physicians or health insurance companies to get feedback to their health condition or reduced insurance fees. Consequently, we see social adjustment benefits as a key driver to the willingness to disclose information and posit:

P2: Social adjustment benefits have a positive effect on the willingness to disclose information.

Service improvement benefits

Benefits from service improvements through service personalization are described as the second type of privacy benefits, to positively influence the willingness to disclose information (Smith et al., 2011). They refer to Chellappa and Sin (2005) who define personalization as "the ability to proactively tailor products and product purchasing experiences to tastes of individual consumers based upon their personal and preference information" (p. 181). White shows that personalization benefits support the customer willingness to disclose their personal and preference information (White, 2004).

While personalization is based in the context of commerce, we adapt it to the context of self-tracking by redefining it as "the ability to tailor common services to the needs of self-tracking users based upon

their self-tracking data" and rename the variable to service improvement benefits. We argue, when self-tracking data is shared with certain service providers, they are able to customize their services to the advantage of the user. For example, users could share their data with a personal fitness coach, who can therefore align the training schedule or with physicians, who can then derive abnormalities in the data and customize the treatment accordingly. Hence, we posit:

P3: Service improvement benefits have a positive effect on the willingness to disclose information.

Financial rewards

Financial rewards are stated as the third type of privacy benefits to positively influence the willingness to disclose information (Smith et al., 2011). Financial rewards can have various forms, such as discounts, vouchers or free gifts (Hui et al., 2006). Several studies confirmed that financial rewards have a positive impact on the motivation to disclose information (e.g. Hann et al., 2007; Hui et al., 2006; Xu et al., 2009). We assume that in the context of self-tracking, financial rewards are also a relevant benefit. For example, financial rewards could be granted by health insurance companies to customers for providing their self-tracking data to demonstrate health-promoting behavior. We therefore also adopt the variable into our model and posit:

P4: Financial rewards have a positive effect on the willingness to disclose information.

Data criticality

With data criticality, we integrate a moderating variable into our research model that is specific in the context of self-tracking. We define it as one's concern that the disclosure of his or her health, well-being and fitness data give rise to negative consequences. We argue, that self-tracking users who are in general healthy and have a decent fitness level, thus do have uncritical data, do not expect negative consequences when disclosing their data. In contrast, users who are less healthy and fit and therefore have critical data, have a higher tendency to expect negative consequences by third parties and therefore value this fact when they evaluate the risks and benefits of information disclosure. We posit:

P5a: The data criticality positively moderates the effect between privacy risks and the willingness to disclose information.

P5b: The data criticality negatively moderates the effect between social adjustment benefits and the willingness to disclose information.

P5c: The data criticality negatively moderates the effect between service improvement benefits and the willingness to disclose information.

P5d: The data criticality negatively moderates the effect between financial rewards and the willingness to disclose information.

Data sensitivity

Data sensitivity is a second new moderating variable we integrated in the specific context of self-tracking. While data criticality considers the collected data, data sensitivity refers to the data type. We define it as one's consideration of the type of data within the privacy calculus. It addresses that self-tracking users do not only share information such as contact information or usage patterns (e.g. website usage) but highly personal data that is directly linked to their health, well-being and fitness. Yet, even though the data is highly personal, there are still increments of data types present. Basic self-tracking devices measure mainly activity data such as walking distance, steps, calories burned or the sleep rhythm, while more sophisticated or specialized devices also measure vital and body data, such as heart rate, blood pressure, stress level, weight, body fat, muscle mass or the body mass index. While activity data allows to derive general assumptions about one's well-being or fitness, vital and body data in contrast enable to draw conclusions about the health status or possible diseases and is thus more sensitive. We assume, that users of self-tracking devices take this fact into account when they

calculate the risks and benefits of information disclosure. Hence, we posit data sensitivity as a positive moderator for privacy risks and a negative moderator for the privacy benefits:

P6a: The data sensitivity positively moderates the effect between privacy risks and the willingness to disclose information.

P6b: The data sensitivity negatively moderates the effect between social adjustment benefits and the willingness to disclose information.

P6c: The data sensitivity negatively moderates the effect between service improvement benefits and the willingness to disclose information.

P6d: The data sensitivity negatively moderates the effect between financial rewards and the willingness to disclose information.

3.3 Research Model

Summarizing, we primarily drew upon the comprehensive APCO Macro Model of Smith et al. (2011) but focusing on the link between the privacy calculus, characterized by privacy risks and privacy benefits, and the behavioral reactions, described as the willingness to disclose information. The model is shown in Figure 1.

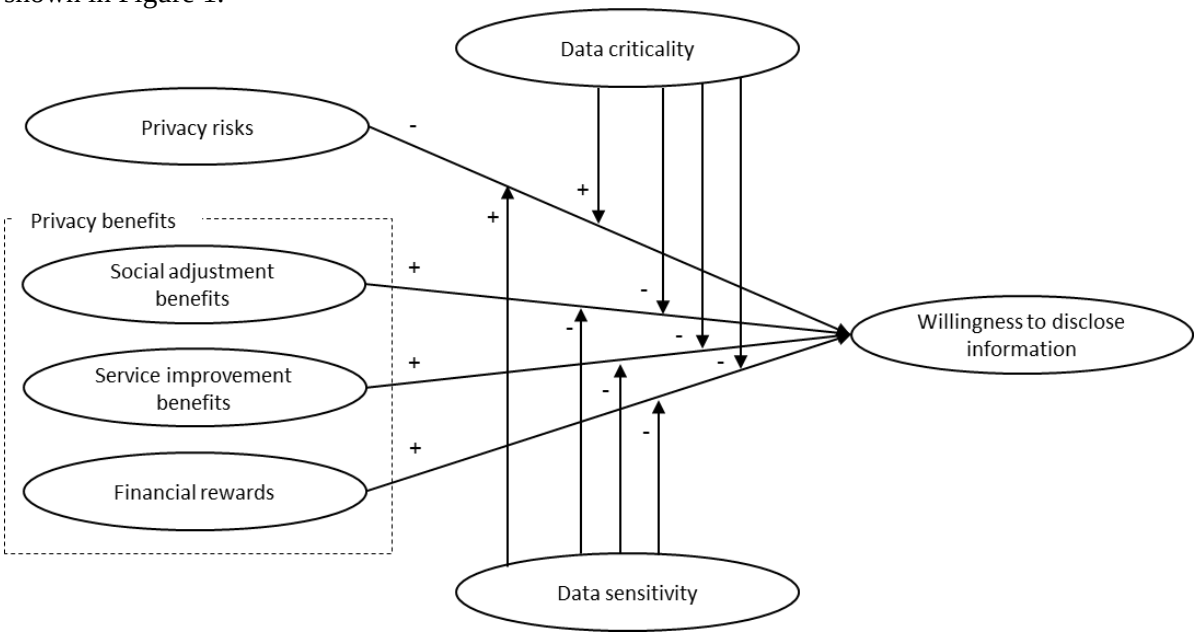

Figure 1. Research model

4 Conclusion and Outlook

We set out to deductively build up a conceptual model with which we aim to explain an individual's conscious willingness to disclose highly personal self-tracking data to service providers. While the privacy research is already established, we elaborate on the self-tracking context as a promising new aspect within this research area and suggests a concentrated model that will be put forward to an empirical evaluation. We acknowledge two limitations. Firstly, our study, to this extent, only depicts a conceptual model for which we do not have any empirical evidence as to how far our propositions reflect the reality and as to how strong the proposed relationships between constructs are. Thus, while the model is deductively derived on theoretical accounts, the empirical validation remains for future research. Second, research identified several other possible influencing factors, especially negative in

nature such as privacy concerns. We summarized the negative variables under privacy risks to avoid a too broad model. Succeeding research may then narrow down the focus in this specific aspect.

Regarding the specific next steps to test our conceptual model, we will derive the measurement model and develop a suitable survey instrument, before data will be collected and analyzed using structural equation modeling approach (Straub, 1989; Urbach and Ahlemann, 2010). Data for our four independent variables and the two moderators will be gathered drawing on 7-point Likert-scales; data for our dependent variable, the willingness to disclose information, will be gathered in a binary format at the very end of the survey. The willingness to disclose information is given for the purpose of our study if, for instance, the users uploads a self-tracking data export file, manually inputs data (e.g., steps per day/week/month, average heart beat per day/week/month), or agrees to the retrieval of information from a self-tracking data broker (e.g., Apple Health). Dropouts at this final stage in the survey would be interpreted as unwillingness to disclose information.

With our research, we expect to give both a further theoretical understanding in the field of information privacy and practical implications for practitioners in the field of self-tracking. As stated before, theoretical privacy research with a focus on private medical or behaviour information had little attention so far. By directing our research on the field of highly personal data of self-tracking, we transfer the current research into the probably most private consumer context. In this sense, we integrate two new moderator variables (data sensitivity and data criticality) which refer specifically to this context and will help to gain a deeper understanding of the determinants of the willingness to disclose data to service providers. In addition, while past research has usually focused on users being unaware about the full extent of information disclosure, our research examines the behaviour when people are informed about purpose, anonymity etc. of their information disclosure. For developers of third-party applications and services in the context of self-tracking, our research will give a deeper understanding which factors concerning the disclosure of self-tracking data are important for users. Hence, they will be able to adapt their services accordingly.

References

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

Barrett, M., E. Davidson, J. Prabhu and S. L. Vargo (2015). "Service innovation in the digital age: Key contributions and future directions." *MIS Quarterly* 39 (1), 135–154.

Buck, C., C. Horbel, C. C. Germelmann and T. Eymann (2014)."The Unconscious App Consumer: Discovering and Comparing the Information-seeking Patterns among Mobile Application Consumers." In: *Proceedings of the Twenty Second European Conference on Information Systems*. Tel Aviv.

Campbell, J. E. and M. Carlson (2002). "Panopticon.com: Online Surveillance and the Commodification of Privacy." *Journal of Broadcasting & Electronic Media* 46 (4), 586–606.

Chellappa, R. K. and R. G. Sin (2005). "Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma." *Information Technology and Management* 6 (2-3), 181–202.

Chen, R. (2013). "Living a private life in public social networks: An exploration of member self-disclosure." *Decision Support Systems* 55 (3), 661–668.

Contena, B., Y. Loscalzo and S. Taddei (2015). "Surfing on Social Network Sites." *Computers in Human Behavior* 49, 30–37.

Culnan, M. J. and P. K. Armstrong (1999). "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation." *Organization Science* 10 (1), 104–115.

Culnan, M. J. and R. J. Bies (2003). "Consumer Privacy: Balancing Economic and Justice Considerations." *Journal of Social Issues* 59 (2), 323–342.

Davies, S. G. (1997). "Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity." *Technology and Privacy: The New Landscape*, 143–165.

Dinev, T., M. Bellotto, P. Hart, V. Russo, I. Serra and C. Colautti (2009). "Internet Users' Privacy Concerns and Beliefs About Government Surveillance." In: *Handbook of Research on Information Management and the Global Landscape*. Ed. by M. G. Hunter and F. B. Tan. IGI Global, p. 229–257.

Dinev, T. and P. Hart (2006). "An Extended Privacy Calculus Model for E-Commerce Transactions." *Information Systems Research* 17 (1), 61–80.

Forest, A. L. and J. V. Wood (2012). "When social networking is not working: individuals with low self-esteem recognize but do not reap the benefits of self-disclosure on Facebook." *Psychological science* 23 (3), 295–302.

Garfinkel, S. (2001). *Database nation:* The death of privacy in the 21st century. 1. paperback ed. Beijing u.a.: O'Reilly.

Gimpel, H., M. Nissen and R. Goerlitz (2013)."Quantifying the Quantified Self: A Study on the Motivations of Patients to Track Their Own Health." In: *Proceedings of the Thirty Fourth International Conference on Information Systems*. Milan.

Green, T., T. Wilhelmsen, E. Wilmots, B. Dodd and S. Quinn (2016). "Social anxiety, attributes of online communication and self-disclosure across private and public Facebook communication." *Computers in Human Behavior* 58, 206–213.

Hann, I.-H., K.-L. Hui, S.-Y. Lee and I. Png (2007). "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach." *Journal of Management Information Systems* 24 (2), 13–42.

Huang, H.-Y. (2016). "Examining the beneficial effects of individual's self-disclosure on the social network site." *Computers in Human Behavior* 57, 122–132.

Hui, K.-L., B. C. Tan and C.-Y. Goh (2006). "Online Information Disclosure: Motivators and Measurements." *ACM Transactions on Internet Technology* 6 (4), 415–441.

IDC (2016). *Worldwide Smartwatch Market Will See Modest Growth in 2016 Before Swelling to 50 Million Units in 2020*. URL: http://www.idc.com/getdoc.jsp?containerId=prUS41736916 (visited on 11/27/2016).

Keith, M. J., S. C. Thompson, J. Hale, P. B. Lowry and C. Greer (2013). "Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior." *International Journal of Human-Computer Studies* 71 (12), 1163–1173.

Kim, H.-S. (2016). "What drives you to check in on Facebook?: Motivations, privacy concerns, and mobile phone involvement for location-based information sharing." *Computers in Human Behavior* 54, 397–406.

Laufer, R. S. and M. Wolfe (1977). "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory." *Journal of Social Issues* 33 (3), 22–42.

Le Wang, J. Yan, J. Lin and W. Cui (2017). "Let the users tell the truth: Self-disclosure intention and self-disclosure honesty in mobile social networking." *International Journal of Information Management* 37 (1), 1428–1440.

Lu, Y., B. Tan and K. L. Hui (2004)."Inducing Customers to Disclose Personal Information to Internet Businesses with Social Adjustment Benefits." In: *Proceedings of the Twenty-Fifth International Conference on Information Systems*. Washington DC, USA.

Lupton, D. (2013). "Understanding the Human Machine." *IEEE Technology and Society Magazine* (Winter), 25–30.

Lupton, D. (2014a)."Self-tracking Cultures: Towards a Sociology of Personal Informatics." In: *Proceedings of the Australian Conference on Human-Computer Interaction (HCI)*. Sydney.

Lupton, D. (2014b)."Self-tracking Modes: Reflexive Self-Monitoring and Data Practices." In: *Proceedings of the Imminent Citizenships: Personhood and Identity Politics in the Informatic workshop*. Canberra.

Norberg, P. A., D. R. HORNE and D. A. HORNE (2007). "The privacy paradox: Personal information disclosure intentions versus behaviors." *Journal of consumer affairs official publication of the American Council on Consumer Interests* 41 (1), 100–126.

Pavlou, P. and D. Gefen (2002)."Building Effective Online Marketplaces with Institution-Based Trust." In: *Proceedings of the Twenty-Third International Conference on Information Systems*. Barcelona.

Peter, J. P. and L. X. Tarpey (1975). "A Comparative Analysis of Three Consumer Decision Strategies." *Journal of Consumer Research* 2 (1), 29–37.

Petronio, S. (1991). "Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information Between Marital Couples." *Communication Theory* 1 (4), 311–335.

Posey, C., P. B. Lowry, T. L. Roberts and T. S. Ellis (2010). "Proposing the online community self-disclosure model: The case of working professionals in France and the U.K. who use online communities." *European Journal of Information Systems* 19 (2), 181–195.

Smith, H. J., T. Dinev and H. Xu (2011). "Information Privacy Research: An Interdisciplinary Review." *MIS Quarterly* 35 (4), 989–1015.

Stone, E. F., H. G. Gueutal, D. G. Gardner and S. McClure (1983). "A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations." *Journal of Applied Psychology* 68 (3), 459–468.

Straub, D. W. (1989). "Validating Instruments in MIS Research." *MIS Quarterly* 13 (2), 147–169.

Stutzman, F., R. Gross and A. Acquisti (2013). "Silent Listeners: The Evolution of Privacy and Disclosure on Facebook." *Journal of Privacy and Confidentiality* 4 (2), 7–41.

Swan, M. (2012). "Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0." *Journal of Sensor and Actuator Networks* (1), 217–253.

Urbach, N. and F. Ahlemann (2010). "Structural Equation Modeling in Information Systems Research Using Partial Least Squares." *Journal of Information Technology Theory and Application* 11 (2), 5–40.

White, T. B. (2004). "Consumer Disclosure and Disclosure Avoidance: A Motivational Framework." *Journal of Consumer Psychology* 14 (1/2), 41–51.

Xu, H., H.-H. Teo, B. C. Y. Tan and R. Agarwal (2009). "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services." *Journal of Management Information Systems* 26 (3), 135–174.

Zimmer, J. C., R. E. Arsal, M. Al-Marzouq and V. Grover (2010). "Investigating online information disclosure: Effects of information relevance, trust and risk." *Information & Management* 47 (2), 115–123.