Available online at www.sciencedirect.com

ScienceDirect

Procedia Manufacturing 3 (2015) 815 – 822

Procedia MANUFACTURING

6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015) and the Affiliated Conferences, AHFE 2015

Like us on Facebook! – Analyzing user preferences regarding privacy settings in Germany

Sylvia Kowalewski[a,]*, Martina Ziefle[a], Henrik Ziegeldorf[b], Klaus Wehrle[b]

RWTH Aachen University, HCIC – Human Computer Interaction Center, Campus Boulevard 57, 52074 Aachen, Germany
RWTH Aachen University, ComSys – Communication & Distributed Systems, Ahornstr. 55, 52074 Aachen, Germany

Abstract

Social networking sites (SNS) provide great benefits for internet users all over the world. People can stay in touch, inform themselves on what is happening, or share with others what they are doing. Despite the great popularity of SNS like Facebook, more and more criticism arises in Europe toward permanently changing privacy regulations and easing of data protection. In order to support users in their right of privacy in the SNS, it has to be evaluated whether the problem is on the operator's side or on the users' side. A problem for the user could be insufficient knowledge or control of the options for privacy settings in the own SNS profile. In this case, need of action implies enhancing users' competencies or the user interface of the SNS. A problem on the operator's side could be that users fear an operator, e.g., sells personal data to other big companies. In this case, policy regulations have to be developed to protect users. This study focused on these aspects and shows that, in general, users' fear of misuse of personal data by the operator is greater than the fear of unwanted exposure to other network members. Furthermore, this study analyzed which factors influence these fears and what the most critical points that would cause users to leave the SNS are.

Keywords: Facebook; Privacy; User preferences; Contextual integrity

* Corresponding author.
E-mail address: kowalewski@comm.rwth-aachen.de

doi:10.1016/j.promfg.2015.07.336

1. Introduction and theoretical background

Social network sites (SNS) allow people to share personal information and content with friends, family, acquaintances, or the Internet's wide public. As of 2014, three out of four persons are using SNS. Users routinely provide personal information on profiles that can be viewed by a large number of unknown people and potentially be used in harmful ways. SNS like Facebook allow users to control the privacy level of their profile by, e.g., limiting access to this information. When asked about the importance of their own privacy settings, most users state privacy as the first and most important aspect [1]. In times in which Facebook's approach to privacy is hotly contested, questions arise how competent SNS users really are und how they can be supported adjusting in their privacy settings. Recent studies in the US showed that privacy behavior is an upshot of both social influences and personal incentives [2]. Furthermore, several studies revealed that Internet skills are highly correlated with making modifications to privacy settings, e.g., [3,4]. Most of the results in the international literature represent the actual privacy research in the US, e.g. [5,6]. Based on the assumption that privacy is a dynamic construct that is influenced by cultural factors, it seems not reasonable to transfer results one-to-one. Although Germany developed into one of the protest strongholds of privacy in Europe right after the first Snowden revelations, still few studies investigated user privacy behavior in social networks in Germany [7]. Understanding the antecedents of privacy concerns provides a foundation for developing effective policies and practices to reduce such concerns. Computer scientists have several algorithms and technologies to support users in protecting their privacy; but precisely in the context of social networks, several aspects play together that complicate an adequate privacy support for users.

First of all, it is not clear whether users experience privacy concerns regarding the operator or regarding other members. This aspect is essential for developing an adequate support for users in their privacy control and thus in their right for privacy. Mistrust in the operator and the way personal data are handled implies the need for action on policy level whereas concern regarding the correctness of the configuration of the personal profile settings implies action on developer level [8]. Another point is that users differ immensely in their skills, knowledge, and risk behavior and thus express different levels of privacy concern: the more experienced users are in regard to frequency and manner of Facebook use, the less they have privacy concerns [9,10]. These results imply that awareness campaigns and educational work might be a further parameter to support users in their privacy protection.

This study focused on Facebook members because it is the most widespread SNS. Facebook started in 2004 as a college network and then began to support other schools and colleges until it became available for everyone in 2005 [11]. In the fourth quarter of 2014, Facebook had 1.12 billion active users with 22 million in Germany [12]. Thus, at least every fourth person in Germany has a Facebook account.

1.1. Definition of privacy, culture, and the privacy paradox

Privacy within social networking sites is not really defined, yet [13]. Even for the concept of internet privacy no uniform definition exists but various in the literature. According to Nissenbaum's *theory of contextual integrity,* there is no such thing as universal privacy norms as they are distinct to each situation and assist to maintain a contextual integrity [14]. With contextual integrity a desirable state is described that people strive towards by keeping perceived private information according to the context. Thus, privacy is not static but a dynamic construct, defined by the context and therefore also by culture. For example, in some cultures the yearly salary is perceived as private, within others it is normal to share this information.

Understanding personal privacy concerns requires a contextually grounded awareness of the situation and culture, not merely a known set of characteristics of the context. A study by Krasnova et al. [7] compared privacy concerns of Facebook members in the US and Germany. Results indicate that German users expect more damage and attribute higher probability to privacy-related violations. On the other hand, even though American users show a higher level of privacy concern, they extract more benefits from their social networking activities, have more trust in the service provider and legal assurances as well as perceive more control. These factors may explain the higher level of self-disclosure indicated by American users. Additionally, these results corroborate the assumption of privacy as a dynamic construct that is determined by context and culture and emphasize the need for culture specific research in this area.

Another important issue within this context and the search for an adequate understanding of privacy is the great difference between attitude and actual behavior. This so-called *privacy paradox* describes people's inconsistent behavior of information disclosure, on the one side, and privacy concern, on the other side [15]. The assumption of privacy as a flexible flow of information that might be private in one context and public in the other context enables another point of view on the *privacy paradox*. Privacy in this sense does not mean that users should not benefit from sharing information with others and keep it all for themselves. It implies the users' right to control the flow of information in a way that goes in line with their own values and norms and at the same time to profit from the unlimited opportunities of the world wide web.

Our interdisciplinary work aims at developing technical support for users to enhance their privacy. In a first step, a deeper understanding of privacy concerns of Internet-users in Germany and SNS users in particular is needed. In a further step, the value of private information and norms of appropriate information flow have to be analyzed. This study deals with the first part of our research aim to answer the question of the key players in privacy concerns.

1.2. Related studies

Privacy settings on Facebook can be controlled in various ways. With a valid e-mail address, everybody can easily register on Facebook. The user has the opportunity to adjust his privacy settings according to his wishes/preferences. But if a person uses a similar application, user will be able to access parts of profiles which are viewable to everyone from each other. Additionally, within the last years, the default privacy settings of Facebook have been changing quite frequently and have been opening more and more parts of the profile in their default [16]. Thus, it is essential for users to check their privacy settings regularly and be aware of the importance of these settings. Many studies showed that some skills of users facilitate handling of these settings and as a consequence these users show less privacy concerns. Internet skills are an important factor [3,4] as are knowledge about ways to control visibility and searchability of the profile [17]. On the technical side, usability of the user interface (UI) features prominently. The more comprehensible the UI, the higher the trust in the operator of a site and the lower the privacy concerns [18].

In contrast to these findings, a study from the University of Vienna monitored people who have left Facebook on the Quit Facebook Day in May 2010 and compared them to active Facebook members [19]. Although Facebook quitters perceived higher privacy concerns and showed higher awareness than Facebook users, they also had a higher score on internet addiction which is equivalent to Internet skills. The authors conclude that one main reason for quitting Facebook might be reducing the amount of time spent on the SNS. In contrast, the qualitative part of the study revealed that users stated privacy concerns as the most important reason to leave; the feeling of getting addicted to Facebook was mentioned in last place.

1.3. Research questions

In order to get a better understanding of how German users value their privacy on SNS like Facebook, how they behave, and what can be done to improve feelings of safety, this study focused on three main aspects. For each aspect, a separate research question was formulated:

- Q1: Privacy concerns in general: What do people fear? Data misuse on side of the operator or inadvertently providing information to other users like colleagues or family members?

Answering this question might give useful advice on how to improve privacy for SNS users. When the problem is missing trust in the handling of data on the operator's side, policymakers have to become active and improve, e.g., privacy policies. On the other hand, usability and comprehensibility of the privacy settings menu have to be improved when users do not feel safe and sure about their profile's privacy settings.

- Q2: What influences privacy concerns: Control, knowledge, or usability of privacy settings?

With regard to concern of unwanted exposure of information to other users, it is assumable that all three factors might have an influence. In contrast to that, the fear of data misuse by the operator might be relevant for people with less perceived control on their own usage behavior.

- Q3: What is the most critical point that causes people to leave the social network?

Since its beginning, Facebook has changed the privacy policies nearly every year. The main reason might be the interest trade-off between great criticism from users and policies, on the one hand, and commercial interest in user data on the other side. In May 2010, an online initiative was started – "Quit Facebook day." More than 34.000 users declared to quit Facebook on a particular day in May [19]. The most important reason for this initiative was the handling of the users' privacy. Now, five years later, we want to investigate what might be reasons today for users to leave Facebook. To get a methodological cross check for the importance of privacy, an explorative approach was chosen in which users can state their reasons in open questions.

2. Methodology

2.1. Questionnaire

Survey questions were created to capture socio-demographics, experience with SNS, privacy behavior in SNS, and general privacy concern consisting of two latent constructs, *data misuse* and *unwanted exposure*.

Data misuse (α = .79) was measured by two items: "I am afraid that my personal data will be given to a third party against my will" and "I am afraid that my personal data will be used for other purposes against my will." *Unwanted exposure* was measured by two items as well: "I am afraid that other members might see something about me that I do not want them to" and "I am afraid that the privacy settings of my profile are not the way I would prefer."

Items addressing *knowledge* were, for example: "I know where I can change the privacy settings of my profile" and "From time to time, privacy settings change automatically on Facebook." *Control* was measured, for example, by: "I check my privacy settings regularly and adapt them if necessary" and "I control precisely who can see what I post." With "The privacy settings of my Facebook profile fit my needs" and "The privacy settings are clearly arranged," *usability* was measured. All questions were measured on a 4-point Likert-scale with 1 = "I totally agree" and 4= "I totally disagree."

At the end of the questionnaire, participants were asked about reasons that could cause them to leave Facebook. They were asked to answer this question in an open textbox.

2.2. Procedure and sample

The study was conducted in Germany during winter 2014. Via different Facebook posts, participants were invited to take part in this study.

Altogether, 110 people took part in this study. All were Facebook users and the mean time of membership was 4.2 years (SD = 2.3). 58 participants were female, 52 were male; their mean age was 30.5 years (SD = 12.12). For further analysis, the participants were divided into two age groups with the younger group aged from 20 to 30 years (N= 54) and an older group from 30 to 66 years (N= 56).

3. Results

The result section is structured according to the research questions described in section 1.3. It starts with an analysis of general privacy concerns in SNS. Afterwards, it will be analyzed what precisely influences privacy concern in SNS. The last part in this sections deals with the open question of what would be a reason for users to leave the social network. All analyses will also consider user factors like age and gender.

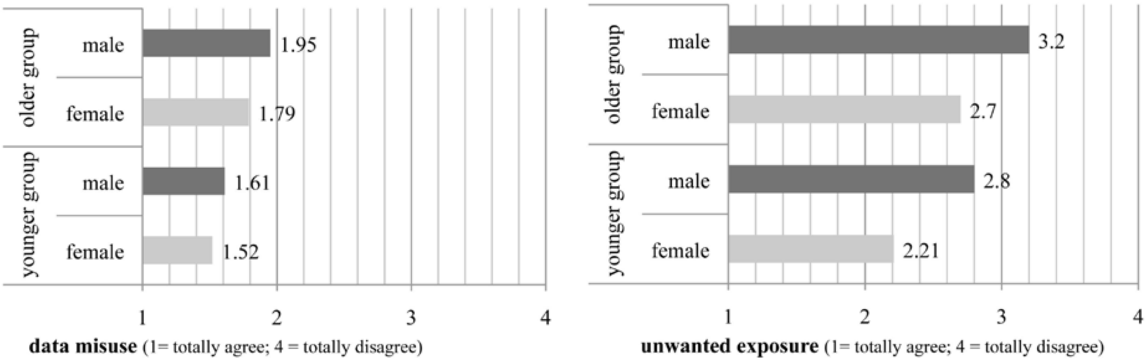

Fig. 1. Mean scores for fear of *data misuse* (left) and *unwanted exposure* (right), separated by age and gender.

3.1. Privacy concern in general

General privacy concern in terms of fear of *data misuse* on the operator's side is relatively high in the sample with a mean of 1.72 (SD= .79). In contrast to that, concern over *unwanted exposure* is less pronounced with a mean of 2.71 (SD = .98). ANOVA with repeated measures reveals that participants differ significantly in their rating on the two aspects of general privacy concern (F(1,108)= 66.92; p < .000).

In a further step, both constructs were analyzed for age and gender effects. The fear of *data misuse* is not affected by an interaction between age and gender (F(2,224) = .07; p = .87), but there is a significant difference between younger and older participants (F(1,108)= 4.4; p<.05). Altogether, younger participants expressed higher fears of data misuse (M= 1.55; SD .64) than the older ones (M=1.87; SD=.72). As Figure 1 shows, in both age groups, women have higher concerns than men although ANOVA revealed no significant gender effect.

With regard to the fear of *unwanted exposure*, there is no significant interaction between age and gender (F(2, 223) = .05; p = .82). But when considered separately, it turned out that age groups (F(1,108) = 6.16; p<.05) as well as gender groups (F(1,108) = 6.58; p<.05) differ in their concerns. Figure 2 shows that, in both age groups, women express higher concern regarding unwanted exposure but the younger group is, in general, more concerned (M = 2.44; SD = .9) than the older group (M = 2.98; SD = 1.0).

3.2. Knowledge, control, or usability: Predictors of privacy concern

In this section, the influence of control, knowledge, and perceived usability of privacy settings in the SNS on the general privacy concern is analyzed. Table 1 gives an overview of descriptive statistics for the three constructs separated by age groups. As gender revealed no significant influence, results are only provided for age groups in Table 1. The table shows that the younger group experiences a significantly higher degree of control and has better knowledge of the privacy settings in their social network profile. In contrast, the older age group evaluates the usability of the privacy settings better than the younger group, even though this effect is not significant.

Table 1. Descriptive statistics for usability, control, and knowledge for both age groups.

	Younger group (20-30 years) N = 54		Older group (31-66 years) N = 56		
	M	*SD*	*M*	*SD*	*p*
Usability	2.72	.66	2.46	.78	.09
Control	1.81	.84	2.21	.88	.04
Knowledge	1.9	.87	2.31	.95	.04

Furthermore, multiple linear regressions were used to analyze the hypothetical relationships. For the fear of *data misuse* by the operator, *usability* turns out to be the only predictor that is explains at least 14% of variance in the dependent variable (F(3,106) = 6.3; p < .001). The negative *ß*-value clearly shows that people who rate the privacy setting options in their SNS profile as usable experience less concern of data misuse by the operator (Table 2).

Table 2. Multiple regression with concern of *data misuse* as dependent variable.

Dependent variable: ***data misuse***				
Predictor	**Adj. R^2**	***ß***	***p***	***t*-Value**
Usability		- 0.35	0.01	-3.58
Control	0.14	- 0.06	0.41	-.074
Knowledge		0.12	0.13	1.52

Regarding the fear of *unwanted exposure of* personal information, multiple regression analysis, as shown in Table 2, revealed *usability* and *knowledge* as key predictors that explain a moderate proportion of 16% of variance (F(3,104) = 5.88; p < .001).

Table 3. Multiple regression with concern of *unwanted exposure* to other users as dependent variable.

Dependent variable: ***unwanted exposure***				
Predictor	**Adj. R^2**	***ß***	***p***	***t*-Value**
Usability		- 0.34	0.01	-3.41
Control	0.16	- 0.06	0.93	-0.08
Knowledge		- 0.24	0.02	-2.35

Again, usability is the strongest predictor but, in general, the results show that the better the usability evaluation and the higher one's knowledge, the lower is the fear of unwanted exposure.

3.3. Reasons to leave the SNS

In the last part of the questionnaire, people were asked to state reasons that would cause them to leave the social network. Altogether, 62% of the sample provided responses. Answers were divided into 8 categories and one named "others." Figure 2 shows a word cloud with all categories. The bigger the word or fragment appears, the more often it was named. The issue that *privacy setting options will be reduced* was the most frequently mentioned reason to leave the SNS. *Data misuse* as well as the possibility that *friends would use another SNS* were the second most often stated causes. Should the SNS be charged *with additional costs*, users would leave; *stalking or harassment* would be strong reasons as well. Interestingly, some participants stated that they *wanted to leave anyway* whereas others pronounced that there would be no reason that could ever cause them to leave.

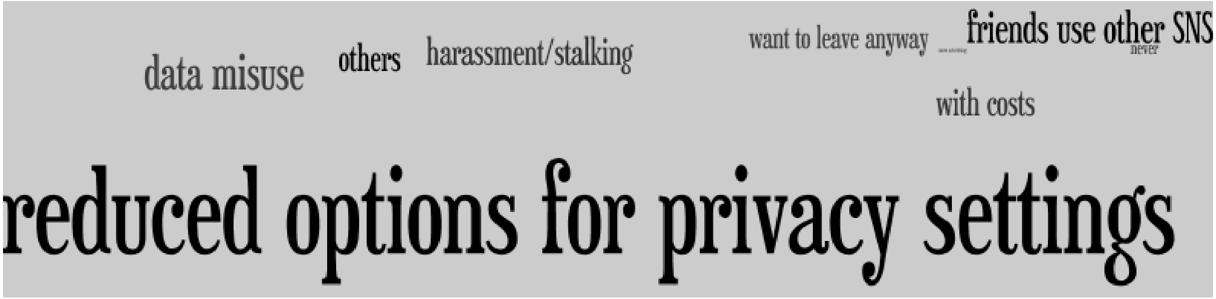

Fig. 2. Reasons to quit Facebook.

4. Discussion

The aim of the current study was to analyze privacy concerns of Facebook members in Germany. The study investigated three main aspects that had to be answered as a first part of a greater research process that yields to the development of technical support to enhance people's privacy.

First of all, analyses on general privacy concerns clearly showed that German SNS users are more afraid of a misuse of their personal data by the operator of the SNS than they are are of unwanted exposure of personal data to other users. A further multiple regression analysis revealed that feelings of control do not influence privacy concerns on any level. SNS users perceive the protection of their privacy as out of their personal control, which is accompanied by the greater fear of data misuse by the operator. The way an operator handles stored data, sells them to other companies, or uses it for customized advertising is something users cannot control with the individual privacy settings of their profile. Thus, policymakers are required to take action in a first step. It is the duty of a government to enact laws establishing guidelines for handling data and information collected and stored on SNS. In a further step, there is also a need for action on the operators' level. As the results of the third research question showed, users are aware and critical of the privacy policy. A reduction of options for privacy settings is the most important reason to leave a SNS, as is a probable misuse of data by the operator. In January 2015, Facebook rolled out a new, simpler privacy guideline that might enable users to better understand who can see their posts and other personal information. This can be seen as a first step into the right direction. On a higher level, namely the handling of stored data by the operators, there is still need for improvement.

Older participants are less concerned than younger participant. They experience a higher usability and a lack of usability, in turn, is the strongest predictor for the fear of data misuse which is more pronounced in younger participants. This age effect goes in line with results from Boyd and Hargittai in the US [9], which revealed, against the widespread assumptions that youths do not care much about their online privacy, young people are indeed concerned about their data protection. Furthermore, results indicate the need for enhancement of perceived control and knowledge of privacy settings, especially for older users.

The first part of our research emphasized the importance of privacy and opens the picture of privacy concerns of users in Germany in a way that we now know on which level users need more support. Most essential are changes on a policy level, but also on the user interface level, improvement is still needed. Taking privacy as a dynamic concept, as introduced at the beginning of this paper, offers a great space for future research. In a further step, it seems to be important to understand how personal data are valued on the peer group level and on the operator level. For example, which kind of data is perceived as sensitive and might a differentiated profile setting that allows to control publishing diverse kinds of information to a well-defined peer group provide enhancement of the perceived privacy. Valuation of sensitivity of personal data could also provide useful guidelines for policy changes on the operator level. It might be possible that de-personalization of profile data when stored or used for commercial activities decreases the feeling of loss of control of the own privacy on the users' side. Therefore, it has to be analyzed to which extent personal data have to be de-personalized. It might be sufficient, e.g., to decouple preferences and attitudes of a person from age and place of living. A comprehensive explanation of how this algorithm works and what happens with the data when processed in commercial ways might increase the users' trust in the operators' data policy. This concept of differential privacy offers various technical solutions to meet privacy interests on the user side and commercial interests on the side of the operator [20].

One limitation of this study is that the subjects had been recruited in an ad-hoc manner instead of a random sampling. Furthermore, the relatively small sample size has an impact on the accurate measuring of age and gender effects.

Acknowledgements

This research has been funded by the Excellence Initiative of German state and federal governments (Project 'NEPTUN, no. OPSF316). The authors express their thanks to Chantal Lydinia for excellent research support.

References

[1] Gross, R., Acquisti, A. Information Revelation and Privacy in Online Social Networks, in: Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, WPES ’05. ACM, New York, NY, USA (2005) pp. 71–80.

[2] Phelps, J.E., D’Souza, G., Nowak, G.J., Antecedents and consequences of consumer privacy concerns: An empirical investigation. J. Interactive Mark. 15 (2001) 2–17.

[3] Syed H. Akhter. Privacy concern and online transactions: the impact of internet self-efficacy and internet involvement. Journal of Consumer Marketing 31 (2014) 118–125.

[4] Litt, E., Hargittai, E. Smile, snap, and share? A nuanced approach to privacy and online photo-sharing. Poetics 42 (2014) 1–21.

[5] Jeong, Y., Coyle, E. What Are You Worrying About on Facebook and Twitter? An Empirical Investigation of Young Social Network Site Users’ Privacy Perceptions and Behaviors. Journal of Interactive Advertising 14 (2014) 51–59.

[6] Young, A.L., Quan-Haase, A. Privacy Protection Strategies on Facebook. Information, Communication & Society 16 (2013) 479–500.

[7] Krasnova, H., Veltri, N.F. Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA, in: 2010 43rd Hawaii International Conference on System Sciences (HICSS). Presented at the 2010 43rd Hawaii International Conference on System Sciences (HICSS), pp. 1–10, 2010.

[8] Krishnamurthy, B., Wills, C.E. Characterizing Privacy in Online Social Networks, in: Proceedings of the First Workshop on Online Social Networks, WOSN ’08. ACM, New York, NY, USA (2008) 37–42.

[9] Fogel, J., Nehmad, E. Internet social network communities: Risk taking, trust, and privacy concerns. Computers in Human Behavior 25 (2009) 153–160.

[10] Boyd, D., Hargittai, E. Facebook privacy settings: Who cares? First Monday 15, 2010.

[11] Boyd, D.M., Ellison, N.B. Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication 13 (2007) 210–230.

[12] http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (04/08/14).

[13] Dwyer, C. Digital Relationships in the “MySpace” Generation: Results From a Qualitative Study, in: 40th Annual Hawaii International Conference on System Sciences, 2007. HICSS 2007. Presented at the 40th Annual Hawaii International Conference on System Sciences, 2007. HICSS 2007, pp. 19–19.

[14] Nissenbaum, H. A Contextual Approach to Privacy Online. Daedalus 140 (2011) 32–48.

[15] Norberg, P.A., Horne, D.R., Horne, D.A. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. Journal of Consumer Affairs 41 (2007) 100–126.

[16] Nemec, L., Holbl, M., Burkeljca, J. & Welzer, T. Facebook as a Teaching Tool. Eaeeie Annual Conference
(Eaeeie), 2011 Proceedings of the 22nd, 13-15 June 2011. 1-4.

[17] Acquisti, A., Gross, R. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook, in: Danezis, G., Golle, P. (Eds.), Privacy Enhancing Technologies, Lecture Notes in Computer Science. Springer Berlin Heidelberg (2006) pp. 36–58.

[18] Casaló, L.V., Flavián, C., Guinalíu, M. The role of security, privacy, usability and reputation in the development of online banking. Online Information Review 31 (2007) 583–603.

[19] Stieger, S., Burger, C., Bohn, M., Voracek, M. Who Commits Virtual Identity Suicide? Differences in Privacy Concerns, Internet Addiction, and Personality Between Facebook Users and Quitters. Cyberpsychology, Behavior, and Social Networking 16 (2013) 629–634.

[20] Ziegeldorf, J.H., Morchon, O.G., Wehrle, K. Privacy in the Internet of Things: threats and challenges. Security Comm. Networks 7 (2014) 2728–2742.