Pros and Cons of Privacy by Default: Investigating the Impact on Users and Providers of Social Network Sites

Markus Tschersich
Goethe University Frankfurt
mailto:markus.tschersich@m-chair.de

Michael Niekamp
Goethe University Frankfurt
niekamp@econ.uni-frankfurt.de

Abstract

Based on actual experimental findings, we present a new line of argumentation about the chances, risks and effects of a Privacy by Default regulation for users and providers of Social Network Sites (SNS). We describe three important factors that have an impact on the utility provided by SNS and measure their change through opposing status quo. On empirical grounds, the results challenge the widely accepted assumption that restrictive default privacy settings cause overly negative consequences for providers.

1. Introduction

It is easy to see that any regulation regarding the privacy defaults on Social Network Sites (SNS) has large impact on welfare of users and providers. Users' welfare partially depends on their behavior on SNS and we assume that it is driven by two major concerns, the demand to share personal information to fulfill certain needs (e.g. gaining social capital, relations maintenance, lower feelings of loneliness) [2] and demand to stay secure against misuse and misinterpretation [5].

Accordingly, some users (or their representatives, e.g. the European Commission) value privacy and data protection as important assets. Earlier findings show that users underestimate potential risks [7]. Privacy-friendly services are often perceived as too complex and need more work than users expected. Therefore users welcome concepts for more user-friendly privacy concepts, but still do not see the need to protect their personal information [26]. Due to that, regulators and privacy professionals see the need to support users in protecting their privacy and assume that their welfare will be maximized when default settings are regulated by a Privacy by Default rule and not free to the providers' choice. Therefore, they propose Privacy by Default as powerful concept to reduce the risk of privacy violations [18]. Privacy by Default requires platform providers to preselect the most restrictive option as default for all privacy settings that manage the revelation of personal information [3]. Without a purposeful decision by the user no personal information is shared within the network. Due to the potentials to protect citizens' rights, the European Commission (EC) shares the opinion of privacy professionals and plans to oblige platform providers to implement Privacy by Default to their systems [9]. As part of the European Union legislation process the draft law also passed the European Parliament end of 2013 and is currently discussed in the Council of Ministers [10].

Contrary to that, the concrete and very basic conflict of interest we shall emphasize here is constituted by platform providers who assume that their welfare will be maximized when defaults of privacy settings are unregulated and free to decide by providers [8]. They argue that their business success is highly depending on users' participation, especially by sharing personal information. By regulating the default of privacy settings on SNS, providers expect that the status quo bias will lead to less shared personal information and as a consequence to less user participation [15]. Therefore, SNS providers fear threats for the functionality of the platform and their business models.

The legal debate often refers to this potential conflict of interest as a trade-off relation between the citizen rights to be protected against any privacy threats and the providers' rights to access any market within legal constraints. However, we address this conflict as a simple welfare maximization problem over two agents (users and providers). This raises several questions whether and how to regulate the SNS market to provide optimal results by default settings for users and providers at the same time. In general debates about social engineering it is often assumed that one effective tool to regulate markets optimally is given by regulating default settings [21].

In order to shed some light on all of the above empirical assumptions, we tested whether subjects are prone to a status-quo-bias [11, 27] or an anchoring effect [17] in their configuration of privacy settings. The goal of this paper is twofold. Firstly we provide empirical insights that confirm that people are affected by these effects that cause a conflict of interest between users and provider, but secondly and surprising-

1530-1605/15 $31.00 © 2015 IEEE
DOI 10.1109/HICSS.2015.211

ly that the reasonable net effects on providers are much smaller than they assume. We would rather emphasize that a suggested Privacy by Default regulation improves different long-term interests of users and providers. A Privacy by Default regulation prevents potential damage for the citizens, but will neither hamper citizens from sharing data on SNS to fulfill their needs nor have much impact on the supply side. Our experimental results substantiate this through a clarification, whether and how users are prone to the default settings. Simultaneously, they indicate the expected impact on long-term chances and risks for providers of SNS.

The paper is organized as follows: In Section 2 we suggest three major factors that have an impact on providers' utility and should be taken into account. We designed two experiments, presented in Section 3 that measure the influence of privacy by default on two of the previous suggested factors. Here we present the effect and the estimated direction of a change in the default privacy settings. In Section 4 we discuss the implications on the question for legal regulation. Section 5 draws one important conclusion.

2. Factors of information exchange

SNS providers (e.g. Facebook) mainly create revenue out of targeted advertisement and successful marketing campaigns [4]. Those activities require the provision of personal information and high communication among the users. The objective of SNS providers is to increase their revenue and to build sustainable platforms. Therefore, SNS providers are encouraged to boost network expansion, activity and connectivity between users to increase their utility. Consequently, business success of SNS is crucially depending on a high exchange of personal information and messages within the network [15]. We assume that the overall exchange of personal information between users on SNS is based upon three relevant factors: Numbers of addressees, quantity of shared personal information, and total number of SNS members.

The first factor (a) comprises the *number of addressees* that are reached by a user with her/his shared personal information. In most SNS nowadays, providers try to maximize the number of addressees by implementing default settings that allow a higher number of users in the network to access the uploaded personal information. Hence, due to more restrictive privacy settings users can limit the access to their personal information to the number of connected peers in the network or even less.

The second factor (q) concerns the *quantity* of shared personal information. This takes into account how often a user decides to share personal information within the SNS. Shared personal information includes all information published by users (e.g. profile).

The third factor (u) refers to the *total number of users* actively participating on the platform by receiving and sending information. This number is not only depending on the popularity of the platform but also on users' satisfaction [15]. Assuming that all users are similar in their number of addressees and the quantity of shared personal information, we take the average of those two factors as basis for the multiplication with the total number of users to calculate the overall exchange of personal information.

To assess the overall effect of Privacy by Default on the utility of SNS providers in form of the exchange of personal information, the effect on each factor needs to be analyzed individually. The next section describes the operationalization of the factors and shows the results of empirical test measuring the impact of Privacy by Default.

3. Main results

Two experiments were conducted to collect empirical data about the effect of Privacy by Default on the number of addressees [22, 23] and quantity [25] of personal information on SNS. The process of the data collection as well as the main results are described in the following in more detail.

3.1 Addressees

On the common SNS (e.g. Facebook) users are able to decide who is allowed to access their personal information, to see their status updates, etc. The options range between granting access to the whole community or nobody. Based on the selected option the number of addressees varies.

Thus, to identify whether Privacy by Default makes a difference in the number of addressees we run a study to figure out whether users with restrictive default privacy settings configure their privacy settings differently considering the access rights from users with permissive privacy settings [23]. The 391 participants (students with the average age of 24) were randomly assigned to one out of two groups based on the two experimental conditions. The first group had restrictive default privacy settings (*Only me*) and the second had permissive default privacy settings (*Everyone*). For the data-collection a privacy interface prototype for SNS was developed and used comprising 14 different default privacy settings with preselected default options based on the experimental conditions.

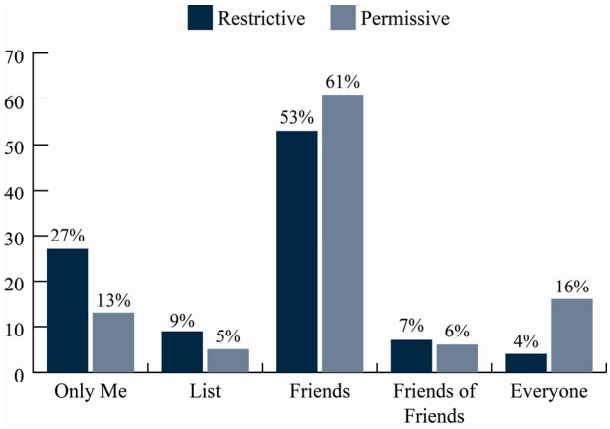

Figure 1. Aggregated distribution on selected privacy options

Results show that the two experimental groups significantly differ in their configuration behavior [23]. The restrictiveness of the preselected privacy options has an influence on the configuration of all 14 analyzed privacy settings. Figure 1 displays the aggregated distribution of the selected privacy options based on all analyzed privacy settings. This highlights that participants of the group having restrictive privacy settings were nearly two times more often keeping the default settings. However, this might be explained by the status quo bias. Further, the anchoring effect is higher in the case of restrictive default privacy settings, because the size of the deviation from the default was smaller in the group with restrictive default privacy settings than its permissive control group.

Literature shows that the style of the interface could also influence the configuration of settings [12, 19, 20]. Therefore, we run an extended treatment to analyze the influence of interface styles besides the influence of different default settings to identify potential bias by the interface. In this extended treatment we tested the two conditions of the default settings with two different types of interfaces. The first interface style displays all privacy settings in a list one below the other. The second style comprises out of multiple pages where the privacy settings are grouped by topic. Results show that in the case of the interface with multiple pages, privacy settings on other pages than the page displayed first, have much less been changed from the default option. Participants with this interface style are more biased by the status quo. Figure 2 shows this based on the average value of the selected privacy options. Privacy settings of section Profile Information had been displayed first. Here the lines of groups with the same default options (same color) are very close to each other. For sections Status Updates and Media in the case of the menu interface style (dotted lines), the selected options are closer to the default option compared to the list interface style (solid line).

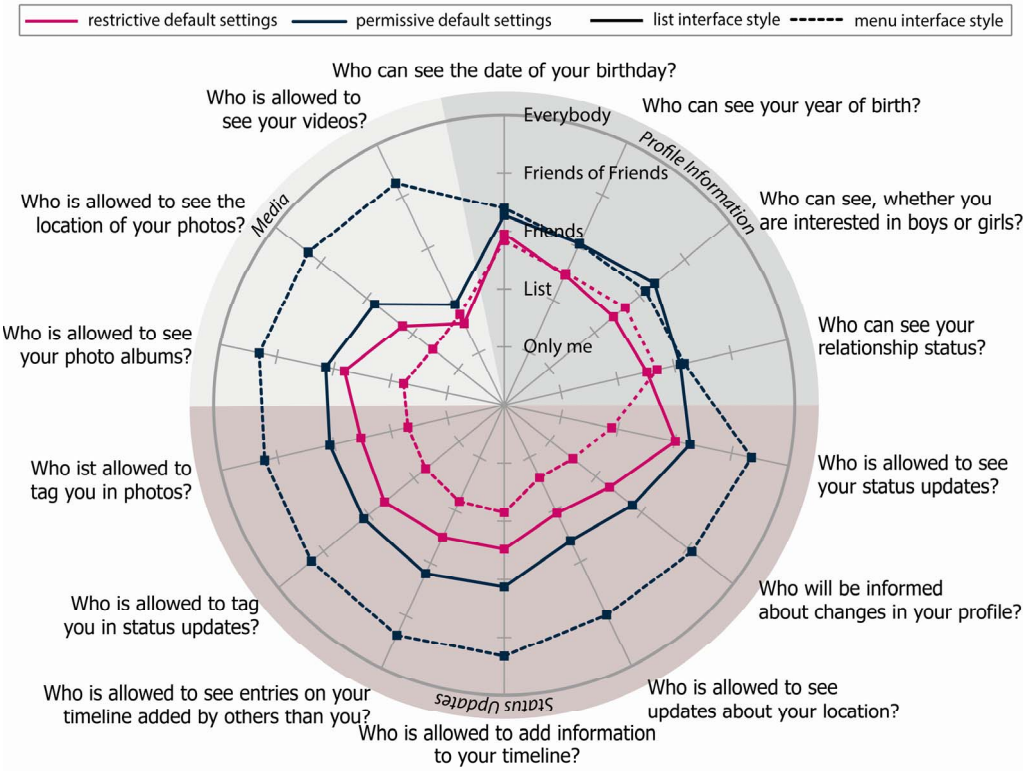

Figure 2. Selected privacy options based on the default settings and the interface style

Concluding, results show that restrictive default privacy settings lead users of SNS to share their personal information with a smaller number of peers compared to users with permissive default privacy settings. Consequently, Privacy by Default decreases the number of addressees of personal information on SNS and depending on the interface style this effect can be strengthened.

3.2 Quantity

In the next step we measured the quantity of shared private information (q) [25]. A better understanding of the quantity is also important to answer the question whether there is the presupposed impact on providers. We assumed that the decision-making process whether to reveal personal information or not can be captured by a privacy calculus that contains several factors [6]. This calculus describes a wide reflective equilibrium of benefits and costs of the revelation by the deciding user. Several factors have a significant impact on this calculus in the case of SNS [13, 14, 16]. We were especially interested in the task, if the need to purposefully decide, whether to reveal private information or not, causes a change in the quantity of information exchange on SNS. We tested their influence whether restrictive privacy settings encourages a positive decision to self-disclose or not and we analyzed the cost-benefits-ratio of restrictive default privacy settings on the privacy calculus [25] (cf. Figure 3). In the case of SNS the benefits of a revelation contain enjoyment, self-presentation and relationship maintenance [13, 24, 25]. Potential costs are determined by privacy concerns and its predecessors perceived likelihood and perceived damage of a potential misuse and misinterpretation of personal information.

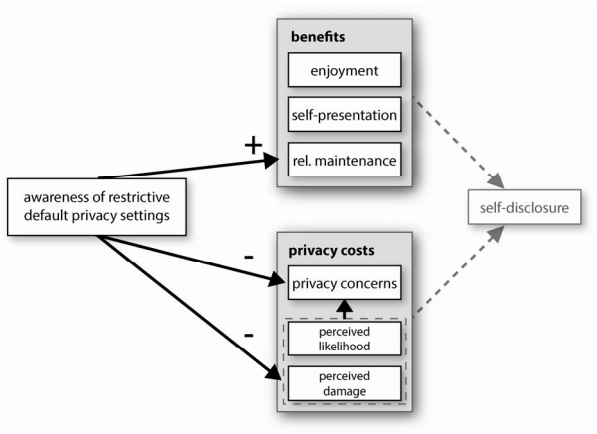

Figure 3. Impact on the privacy calculus of SNS by Privacy by Default

The study allows analyzing a change in users' perception of the benefits and costs of self-disclosure on SNS by making them aware of restrictive default privacy settings. Based on repeated measurement in a pretest-posttest experimental design, the perceived benefits and costs had been measured before and after a period of four weeks using the SNS Facebook by being aware of having restrictive default privacy settings.

Interestingly and opposed to the standard assumptions mentioned in the introduction, the results show (cf. Figure 3) that privacy by default settings have no significant impact on enjoyment and self-presentation, but do have a significant positive impact on the relationship maintenance, so that users perceive a higher possibility to better maintain their relationship even though in general less personal information is available by default. Additionally, there is a significant negative impact on privacy concerns and perceived damage, so that participants have less privacy concerns and perceive less damage of a potential privacy violation.

Consequently, restrictive default privacy settings decrease the privacy costs and increase the benefits of revealing personal information on SNS. Even though restrictive privacy will cause a positive shift to the benefits it is not necessarily given that the quantity of shared personal information is increased. Depending on the sensitivity of personal information the increased benefits might not be enough to compensate the existing privacy concerns even though they are decreasing. Hence, one can conclude that restrictive default privacy settings will not decrease the quantity of shared personal information on SNS and depending on the type of personal information it might increase the quantity.

3.3 Total number of participants

The success of an SNS is also depending on the total number of active users [15]. How Privacy by Default can influences the total number of participants has not been empirical investigated, yet.

In the case of non-restrictive default privacy settings, this non privacy-respecting behavior of the SNS can lead users to abandon the platform due to perceived higher risk of privacy violations and ultimately might decrease the total number of users. This in turn causes a reduced exchange of shared personal information. On the other hand, a high(er) effort to configure personal information settings could be a reason for participants to leave the platform or even do no register at all. Therefore, in the following the total number of participants is seen as a constant variable.

4. Implications

In contrast to expectations mentioned in the lobbying publications of Facebook [8] or the description of the planned regulation of European policy makers [10], the results of the previously described empirical studies allow a more profound argumentation about the chances, risks and effects of a Privacy by Default regulation. The gained insight about the influences of Privacy by Default on the exchange of information on SNS helps to build an instrument for decision-makers to support their evaluation whether Privacy by Default should be enforced or not.

Our results provide striking confirmation that Privacy by Default regulation will serve as an effective mean to user protection in the first place. Interestingly, this goal does not necessary lower the level of shared personal information, because due to the positive shift of the Privacy Calculus and on condition that personal information is not to sensitive a proportion of users might reveal more personal information, when they have more control of privacy, due to the required purposeful decision of self-disclosure. This might lead to the consequence that provider do not suffer at all from a regulation, because the possible increase of the quantity of shared personal information might compensate the decrease of the number of addressees, whereby the exact transmission remains open to future research.

The possible increase of shared personal information could have a positive side effect for providers of SNS because this increases the exchange of personal information. Based on that, data analytics can better deduce implicit data for improved personal profiles. This reduces stray light losses [1] and helps platform providers to increase revenue by offering their advertising customers higher quality of customer targeting.

Nevertheless, Privacy by Default is decreasing the number of addresses and thus this has a negative impact on the overall exchange of personal information. This raises the question how to evaluate this consequence from the perspective of legitimacy. We assume that it is unlikely that the right to keep revenues will override user protection. Especially when one takes into consideration that the number of users having restrictive default privacy settings that select option *Only me* consists of two different types. First, those users decide to share personal information with no one on purpose and second, those users that kept the default setting due to the status quo bias. As displayed in Figure 4, 13% of users with permissive default privacy settings decided explicitly to not share their personal information with anybody. Based on the random allocation to the experimental group we can assume that both groups are homogeneous. Thus, we assume that also 13% of the group with restrictive default privacy settings decided to keep the default setting on purpose and not due to the status quo bias. Therefore, 14% of users with restrictive default privacy settings do not share personal information due to the status quo bias. So, to estimate and value the damage of the regulation to the platform provider, one can only take into account those 14%.

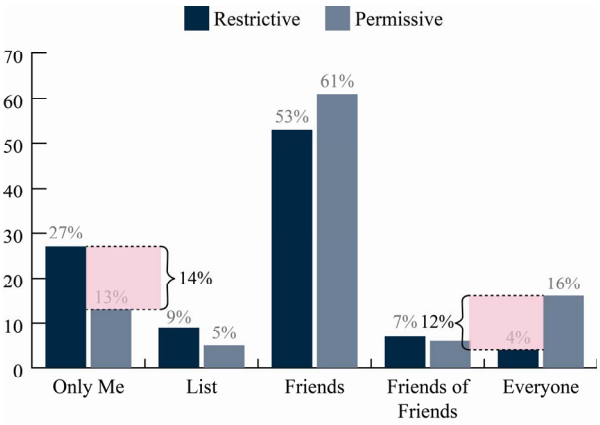

Figure 4. Identification of users biased by the status quo

Based on the same argumentation, we assume that 12% of the users with permissive default privacy settings share their personal information based on the status quo bias and not without a purposeful decision (cf. Figure 4). For a general assessment of the consequences of the regulation plans, deciders need to weight up the damage caused by 14% more users do not share any personal information with 12% of the users accidentally share personal information that might be protected or limited to a smaller number of addressees.

This undermines the basic assumption that Privacy by Default regulation has disastrous consequences on providers' business models. And we doubt that provider should argue on these grounds. We suggest that providers should reassess the potential improvements on enhanced profiles to be used for targeted advertising.

5. Limitations and further research

In terms of generalization there are some limiting factors to our study and its experimental findings. The studies for both factors *addresses* and *quantity* were carried out only with students. Even though the main group of SNS users are younger people, but the number of users with a higher age is increasing due to the expansion of SNS. Users with a higher age might behave differently in the case of Privacy by Default, but we assume that they are even more concerned about

privacy and thus give even more weight to the protection of privacy within their privacy calculus.

In the study 2, we analyzed the impact on the quantity of shared personal information based on users' decision-making to disclose personal information. This study does not cover the quality of the information shared after a positive decision of the privacy calculus. Further research should also analyze whether Privacy by Default has also an impact in the quality of shared personal information.

Further, we conducted the studies in the context of SNS used for private purposes (e.g. Facebook). SNS used for business purpose (e.g. LinkedIn) most probably provide different benefits of using them and users might also behave differently compared to a leisure time context and having Privacy by Default. This raises the general question whether the chosen factors are good proxies to estimate the driving forces of users' utility. Due to a statistical robustness check we can argue that it is unlikely that they are unreliable. Nevertheless, there might be others that we have not discovered, yet. Instead of emphasizing its limitation, we rather highlight that the given experimental test might provide a first scientific benchmark that we are otherwise still lacking. To fully evaluate a Privacy by Default regulation from a neutral scientific perspective more quantification of the factors is needed that neither providers nor the EC provide sufficiently.

The previous discussion provides only a first step into a better understanding of the impact of regulation of SNS. Future research should focus on a quantified measure in general and the impact on total number of users affected by Privacy by Default regulation and control for private users and business customers.

6. Conclusion

As it might be a little too early to draw outreaching conclusions on the use of Privacy by Defaults in SNS, and we do not want to repeat all the results here, we shall return towards the basic conflict of interest mentioned in the introduction. We conclude that the empirical evidence does not support all the necessary assumptions of a potential threat towards the business model of Facebook and other SNS provider. To the contrary, introducing Privacy by Default regulation makes users better off and possibly increases the quantity of shared private information. It remains open whether this possible increase can compensate potential losses from the number of addressees. As much as these revenues of the latter are built upon the dubious source of exploiting users' cognitive biases, it is hardly reasonable how to use such an argument for legal complaints.

7. References

[1] Bauer, H.H. and Bryant, M.D. Neue Trends im Behavioral Targeting. *Absatzwirtschaft 51*, 4 (2008), 42–44.

[2] Burke, M., Marlow, C., and Lento, T. Feed me: motivating newcomer contribution in social network sites. (2009), 945–954.

[3] Cavoukian, A. Privacy by Design. *privacybydesign.ca*, 2008. http://privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf.

[4] Constine, J. Facebook Beats In Q1 With $2.5B In Revenue, 59% Of Ad Revenue From Mobile, 1.28B Users. *techcrunch.comfacebook-q--earnings*, 2014. http://techcrunch.com/2014/04/23/facebook-q1-2014-earnings/.

[5] Deuker, A. and Rosenkranz, C. The usage of the individual privacy settings on social networking sites? Drawing desired digital images of oneself. (2012).

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

[7] Dinev, T. and Hu, Q. The centrality of awareness in the formation of user behavioral intention toward preventive technologies in the context of voluntary use. (2005).

[8] Europe versus Facebook. Facebook's views on the proposed data protection regulation. *europe-v-facebook.org*, 2012. http://www.europe-v-facebook.org/FOI_Facebook_Lobbying.pdf.

[9] European Parliament. *REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. (2012).

[10] European Parliament. *Report on the proposel for a regulation of the European Parliament and of the Concil on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. 2014.

[11] Gilovich, T., Griffin, D., and Kahneman, D. The Psychology of Intuitive Judgment. (2002).

[12] Hargittai, E. Facebook privacy settings: Who cares? *First Monday 15*, 8 (2010).

[13] Krasnova, H. and Veltri, N.F. Privacy calculus on social networking sites: Explorative evidence from Germany and USA. *Proceedings of the 43rd Hawaii International Conference on System Science*, (2010), 1–10.

[14] Krasnova, H. and Veltri, N.F. Behind the curtains of

privacy calculus on social networking sites: the study of Germany and the USA. *Wirtschaftinformatik Proceedings 2011*, (2011).

[15] Krasnova, H., Hildebrand, T., Guenther, O., Kovrigin, A., and Nowobilska, A. Why Participate in an Online Social Network? An Empirical Analysis. (2008).

[16] Krasnova, H., Veltri, N.F., and Günther, O. Self-disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture. *Business & Information Systems Engineering*, (2012), 1–9.

[17] Samuelson, W. and Zeckhauser, R. Status quo bias in decision making. *Journal of risk and uncertainty 1*, 1 (1988), 7–59.

[18] Schaar, P. Privacy by Default: Airbag für die Informationsgesellschaft. *bfdi.bund.de*, 2009. https://www.bfdi.bund.de/bfdi_forum/showthread.php?t=3365.

[19] Shah, R.C. and Kesan, J.P. Policy through software defaults. *Proceedings of the 2006 international conference on Digital government research*, (2006), 265–272.

[20] Stern, T. and Kumar, N. Improving privacy settings control in online social networks with a wheel interface. *Journal of the Association for Information Science and Technology 65*, 3 (2014), 524–538.

[21] Thaler, R.H. and Sunstein, C.R. *Nudge: Improving decisions about health, wealth, and happiness*. Penguin Books Ltd., London, 2008.

[22] Tschersich, M. Configuration Behavior of Restrictive Default Privacy Settings on Social Network Sites. (2014).

[23] Tschersich, M. Comparing the Configuration of Privacy Settings on Social Network Sites Based on Different Default Options. (2015).

[24] Tschersich, M. and Botha, R.A. Understanding the impact of default privacy settings on self-disclosure in social networking services: Building a conceptual model and measurement instrument. (2013).

[25] Tschersich, M. and Botha, R.A. Exploring the Impact of Restrictive Default Privacy Settings on the Privacy Calculus on Social Networking Sites. (2014).

[26] Tschersich, M., Kahl, C., Heim, S., et al. Towards privacy-enhanced mobile communities—Architecture, concepts and user trials. *Journal of Systems and Software 84*, 11 (2011), 1947–1960.

[27] Tversky, A. and Kahneman, D. Judgment under Uncertainty: Heuristics and Biases. *Science 185*, 4157 (1974), 1124–1131.