Societies **2014**, *4*, 770–784; doi:10.3390/soc4040770

OPEN ACCESS

societies

ISSN 2075-4698

www.mdpi.com/journal/societies

Article

Trust into Collective Privacy? The Role of Subjective Theories for Self-Disclosure in Online Communication

Ricarda Moll *, Stephanie Pieschl † and Rainer Bromme †

Institute of Psychology, Westfälische Wilhelms-Universität Münster, Fliednerstr. 21, 48149 Münster, Germany; E-Mails: pieschl@uni-muenster.de (S.P.); bromme@uni-muenster.de (R.B.)

† These authors contributed equally to this work.

***** Author to whom correspondence should be addressed; E-Mail: ricarda.moll@uni-muenster.de; Tel.: +49-251-83-39497; Fax: +49-251-83-39105.

External Editor: Sonja Utz

Received: 3 July 2014; in revised form: 1 December 2014 / Accepted: 4 December 2014 / Published: 15 December 2014

Abstract: In order to build and maintain social capital in their Online Social Networks, users need to disclose personal information, a behavior that at the same time leads to a lower level of privacy. In this conceptual paper, we offer a new theoretical perspective on the question of why people might regulate their privacy boundaries inadequately when communicating in Online Social Networks. We argue that people have developed a subjective theory about online privacy putting them into a processing mode of default trust. In this trusting mode people would (a) discount the risk of a self-disclosure directly; and (b) infer the risk from invalid cues which would then reinforce their trusting mode. As a consequence people might be more willing to self-disclose information than their actual privacy preferences would otherwise indicate. We exemplify the biasing potential of a trusting mode for memory and metacognitive accuracy and discuss the role of a default trust mode for the development of social capital.

Keywords: Online Social Networks; self-disclosure; privacy; subjective theory; memory; metacognitive accuracy

1. Introduction

Research on interpersonal relationships suggests that people have two opposing needs: On the one hand they need to withhold information about themselves to prevent costs of a privacy loss, and on the other hand they need to reveal personal information in order to get more involved in personally relevant social networks [1]. In online environments, this tension between self-disclosure and privacy [1] has become more salient than ever: On the one hand digital technologies endanger the preservation of privacy through facilitated information transference and storage. Thus, as digital data are persistent, searchable, scalable and replicable [2], the risks of self-disclosure relate to data access by unauthorized people, identity theft, unwanted solicitations, cyberbullying, or the mere storage of personal information that enables individually-tailored advertisements or even the development of digital dossiers by intelligence services. On the other hand, digital technologies make it very easy to establish and improve one's involvement in different social networks and to thereby create interpersonal closeness [3], and to enlarge one's social capital [4–6].

Social capital is closely related to the issue of self-disclosure and privacy boundary regulation in online environments. First, on an individual level the concept of social capital encompasses norms of reciprocity that not only exist regarding beneficial outcomes such as access to information, help, or social support, but also regarding self-disclosing behaviors (see [7]). Thus, personal information may be conceptualized as a further commodity of social exchange within personal relationships [8]. This exchange which takes place on a micro-level, namely between familiar people, may in a second step create a "climate of trust" [9] on a macro-level in which "trustworthiness is taken for granted and trade can occur with ease" [10] (p. 99)—even between strangers. Therefore, it seems likely that especially people who actively interact with other users [11–13] and reciprocate their self-disclosures within Online Social Networks (OSNs) such as Facebook, Twitter, or Google Plus, contribute to and benefit from such a climate of trust. Passive usage alone such as the observation of a network cannot be associated with beneficial outcomes neither on a micro-level in terms of direct socio-emotional outcomes [14], nor on a macro-level in terms of a climate of trust. Therefore, the building and maintaining of social capital is inherently tied to the regulation of one's privacy.

Given the potential conflict between self-disclosure and privacy, it is important to see how people adjust to these unique properties of online communication, how they solve the conflict, and what kind of behavior they show as a result. On a phenomenological level, scholars and lay people have shown great concern about people's willingness to disclose personal information in different online settings. For example, Grossklags and Acquisti have demonstrated that people rather reveal personal information to gain a very small amount of money while at the same time being surprisingly unwilling to pay for the protection of their privacy [15]. However, it would be an oversimplification to conclude that users simply do not care about their privacy, for after all, the same people who so willingly disclose personal information online, experience a sort of tension produced by the co-existence of conflicting social spheres [16,17] and furthermore report to be severely concerned about their privacy [18]. This "privacy paradox" mirrors the conflict between self-disclosure and privacy users potentially find themselves in whenever they communicate online.

In this context, building on Altman's theory of privacy regulation [19] Sandra Petronio [1] argues that people have individual privacy boundaries which they shift in accordance with context, personal needs and preferences. However, especially in online communication the functioning of boundary regulation is likely to depend on a variety of cognitive processes relevant for the assessment of risks and benefits. Whereas some scholars depict the weighing of risks and benefits regarding self-disclosures as a rational process in the sense of a privacy calculus [20], other authors reject this idea. For example, Alessandro Acquisti [21] argues that users cannot be expected to manage their privacy in a rational way because they have incomplete information about risks and furthermore would not be able to stochastically analyze this information if it was available. Instead, people would be prone to psychological distortions when it comes to the weighing of risks and benefits of self-disclosing behavior. As a result, users would display self-control problems in that they prefer the immediate gratifications of a self-disclosure over the distal benefits of having avoided a loss of privacy.

In this conceptual paper we contribute to the debate about the role of cognitive factors when facing the tension between self-disclosure and privacy. Thereby, we offer a new perspective on the question of why people might engage in privacy boundary regulation in online environments that seems inadequate with regard to their actual privacy needs (but which ensures a climate of trust and the collective maintenance of social capital). More specifically, we propose that users have developed a *subjective theory* about online privacy which puts them into a processing mode of default trust with direct consequences for the processing of self-disclosing events. Due to their importance for behavioral regulation we take *memory* and *metacognitive accuracy* as exemplary processes to clarify how cognitive processing might be influenced by a default trust mode.

2. Subjective Theories: Trust into Collective Privacy

A starting assumption underlying our conceptual paper is that users' self-disclosing behavior is impacted by their *subjective* theories about the behavior of their potential audiences. The review of *scientific* conceptualizations of privacy is beyond the scope of this paper, but can be studied elsewhere (e.g., [22–24]).

Research about subjective theories [1] stems from different psychological subfields such as cognitive, educational or developmental psychology. It is based on the depiction of human beings as everyday scientists [25] who—in a somewhat parallel manner to formal scientists—develop understandings of their surroundings from their *everyday experiences* [26] and build up relatively stable theories on issues that are not directly observable. Such theories then constitute frameworks or mindsets on whose basis all further perceptions and judgments may be grounded [27]. In comparison to *scientific* theories however, *subjective* theories are rarely formal or coherent, and emphasize causal relationships which are rarely systematically tested in everyday life [28]. In the following, we will first discuss on which kinds of experiences subjective theories about online privacy may be built. We will then discuss the case of the *subjective collective-privacy theory* (*cp-theory*) and its implications for people's online behavior.

[1] Similar concepts are addressed as implicit, intuitive, lay, naïve, or folk theories.

2.1. The Everyday Experiences of Online Users

In a digitized society we assume that people make at least three important experiences when being online. We propose that these experiences pertain to *helplessness*, *information overload,* and *diffuse audience reactions*:

First, for a while now people receive mass media reports on intelligence services' and governmental practices pertaining to the surveillance of common citizens' digital data [29]. From these reports, people might build the discrete knowledge that once being online, there is almost no possibility to control the storage of their data, leaving them with an experience of latent *helplessness*.

Second, when being online, people are likely to experience *information overload* [30] to some degree, namely the state of receiving more information than one can process. As a consequence, people learn that they need to invest their reading capacities economically [31] and that they have to be selective in their reading behavior as they cannot read and understand every piece of information they are confronted with.

Third, in contrast to face-to-face interactions where people usually know who listens to what they say, in OSN users can never be sure who is really going to be at the receiving end. Moreover, people experience that not everyone who has access to their uploaded contents ultimately responds to it (*diffuse audience reactions*). It is then likely that users build hypotheses on why not everyone receives and responds to their information, eventually contributing to the consolidation of the subjective theory.

We propose that based on the experiences of helplessness, information overload, and diffuse audience reactions, users develop an intuitive understanding of online privacy. Depending on the extent to which these experiences are made, there naturally are a variety of possible subjective theories about online privacy. In the following we will discuss the *collective-privacy theory* (*cp-theory*) as a commonly observable subjective theory.

2.2. The Subjective Collective-Privacy Theory

The linking of research about subjective theories to the realm of online privacy-related behavior was inspired by a discussion put forward by the legal practioner Niklas Lundblad, who elaborated what he called a "noise society" [32]. A noise society is characterized by the fact that its members produce a constant flow of information (noise) from which one can only attend to a few pieces due to limited perceptual and processing capacities. Members of the noise society understand these conditions and thus *expect collective privacy* because they know that it is too costly for others to attend all available information. Expecting collective privacy would therefore imply that although other people *potentially* have access to one's information, it is unlikely that they would make a time-costly effort to actually retrieve it. Within this mindset, information would indeed be private in public, unless 'the public' actually accesses the information.

There are some psychological arguments in favor of Lundblad's thesis, and by extension for the existence of a *cp-theory*. For example, there is good evidence that people in general take their own experiences and behaviors as a default model to infer other people's motivations and behaviors [33] in the sense of social metacognitions [34,35] or theory of mind [36]. Thus, people might project their experience of an information overload into different subgroups of their potential audience. This might be especially true with regard to those subgroups of the potential audience that are *not* expected to read one's self-disclosed contents, while the so-called imagined audience, namely the "mental conceptualization of the people with whom we are communicating" [37] (p. 331), is expected to eventually read the information.

Within the *cp-theory* people might expect that people who are not part of their context-dependent imagined audience

a) must also experience information overload.
b) must have similarly limited time and/or motivation to read everything.
c) must therefore also select which posts to really read.
d) infer that other users have similar reading criteria (for example that they only read things they find interesting).
e) estimate *which* or *whose* information potential readers might find interesting.

Eventually, the consequence of the *cp-theory* is the phenomenon that although the "audience is potentially limitless, [users] often act as if it were bounded [38] (p. 2). Thereby, users might regulate their privacy boundaries according to what they *believe others* will do with it. As this belief does not always reflect other people's *actual* behavior, users might self-disclose more willingly then their actual privacy needs would otherwise allow them to.

2.3. Anecdotal Evidence for the CP-Theory

Until now, there is only anecdotal evidence to support the assumption of a subjective theory about online privacy and its potential impact on users' willingness to self-disclose personal information in online environments. For example, when Facebook (the currently largest OSN) introduced its Newsfeed function users regarded it to be an invasion of their privacy. They did so although these functions did not make *more* information accessible, but merely facilitated their perception by their Facebook contacts. Hoadley, Xu, Lee, and Rosson argue in this context that "NewsFeed and MiniFeed induce lower levels of perceived control over personal information due to the easier access of information, which in turn leads to a subjectively higher probability of privacy intrusion" [39] (p. 57). Interestingly, the authors implicitly describe "privacy intrusion" as the moment when other people actively receive information that has been publicly accessible anyway. This reveals that although users might be aware of the public nature of their information, they still did not expect it to be received by everyone who potentially has access—they relied on "security through obscurity" [40] (p. 15). Users' subjective conceptualizations of online privacy might hence not consider *actual control* over their personal information, but rather their estimated probability that other people will *transform* their stored raw data into knowledge, that is, information that has been understood and internalized by an intelligent agent [41]. Therefore, within the *cp-theory*, self-disclosure is not equivalent with a privacy loss, because only few intended people are assumed to read one's posts, despite the (semi-)public nature of the information. Therefore, the Newsfeed introduction disrupted the expected self-regulative balance between the searching costs and benefits of reading other people's information.

Another anecdotal example is people's frequently stated explanation that they do not care about intelligence services' and governmental spying practices, for after all, they say, they have nothing to hide [42]. This widespread argument is in some way related to the collective privacy expectation, because it reveals how people think about the collection of their data. This data collection constitutes the *possibility* to retrieve sensitive information about every single citizen, but importantly, citizens think that intelligence services would not make a costly effort to actually pick them out of a noisy pool of information without having a good reason for it. Hence, the basis of this argument is the assumption that—due to the assumed limited resources to store, perceive and transform data into knowledge—it is "possible to chart the life of anyone, but not the lives of everyone" [32] (p. 4).

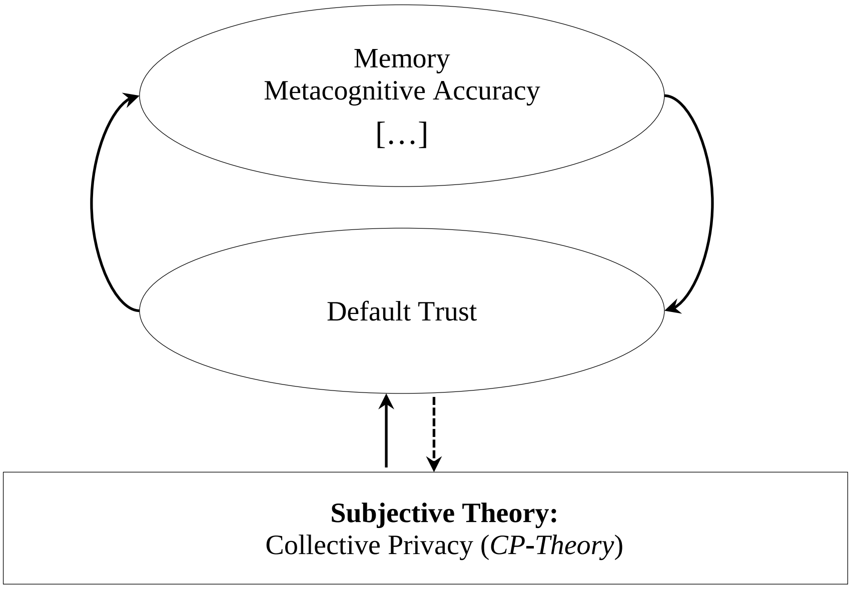
While the presented anecdotal evidence for the *cp-theory* is naturally insufficient to prove our hypotheses, there are several possibilities to approach this topic more systematically in future research. For example, apart from established research programs on subjective theories [43], the development of questionnaires asking for people's privacy expectations might be useful. Furthermore, research under controlled laboratory conditions could systematically investigate factors that influence the *cp-theory* such as the size of the potential audience or the cognitive load people experience through information density.

In summary, we argue that OSNs-users have built subjective theories about online privacy that often take the form of the *cp-theory*. We propose that the *cp-theory* might result in an overall discounted risk perception and put users in a mode of *default trust* which would enhance their willingness to self-disclose. This again can be seen as a double-edged sword: On the one hand this default trust mode is necessary for the collective action of social capital. On the other hand, the default trust mode may cause users to disclose more information than their actual privacy needs would actually indicate. This problem may be even more severe, as the *cp-theory* may be reinforced by the hence trusting mode of information processing.

3. Default Trust: Consequences for (Meta-) Cognitive Processes

Sperber *et al*. [44] argue that humans display trustful behaviors to start with, "and withdraw this basic trust only in circumstances where they have special reasons to be mistrustful" (p. 361). This *default trust* can be seen as the basis for online interactions, and in a further step for the establishment of social capital. We propose that in the context of self-disclosure in online communication, the fundament of such a default trust is the *cp-theory* described above. We argue that in a default trust mode, in which users may think that it does not matter what they self-disclose anyway, users might on the one hand directly infer that it is not risky to self-disclose, but might furthermore be put in a trusting mode of *information processing* in which they draw inferences about associated risks from cues that do not always reliably describe reality [45]. This rather superficial information processing might then reinforce the default trust mode, initially derived from the *cp-theory* (Figure 1). As a consequence, users might be overall more willing to self-disclose personal information than they would be if they engaged in a privacy boundary regulation according to their personal preferences and needs. This again would result in a lower level of actual privacy on the one hand, but in an enhanced level of social capital on an individual and a collective level.

Figure 1. Schematic portrayal of the role of a subjective theory for further stages of processing.



There are many aspects of cognition that might be influenced by a default trust mode. In this paper, we exemplify potential biases for *memory* and *metacognitive accuracy* because of their relevance for self-regulative behaviors [46] and discuss the meaning of related research findings for the realm of online communication.

3.1. Memory

The structural complexity of our environment in relation to our limited cognitive capacities makes it impossible (and often unnecessary) to remember everything about our lives. Therefore, research usually focuses on specific memory impediments and biases. For the context of privacy management in OSNs, especially one body of research is of particular interest: During the last decade, studies in face-to-face contexts have investigated how well people remember what information they disclosed (item memory) to which person (target memory). Study results show that people remember their communication partners and conversation topics quite well separately in the short run, but struggle to make correct associations between topics and targets [47–49]. This basic feature of human cognition might impede the *overall knowledge* users have about their online disclosures. In addition, interactions in OSNs are decontextualized in multiple ways [50] which might even further impede the memory of those interactions.

However, knowledge about one’s online self-disclosures may be crucial for privacy boundary regulation in several respects. For example, when users are unable to recall past disclosure events they might mistake this inability to indicate that they actually have not disclosed much information *at all*. In this context, research on heuristic processing has shown that people use the ease with which a memory comes to mind as a cue to draw inferences about reality [51]. However, concluding that one has not disclosed much information to large audiences in the past would make it impossible for users to grasp the real nature of the associated risk. Since OSN-users use their platform regularly and disclose personal information in a repetitive manner, it is rather the cumulative amount of information stored online creating an overall risk instead of the revelation of a single piece of information alone.

If the difficulty to remember self-disclosing events is leading to the inference that one has not disclosed that much information in the past, this could cause the false conclusion that disclosing just this once is not that risky. The actually *cumulative risk* [52] would hence be misperceived as being a situational one.

In our own work we have investigated the extent to which people remember what information they have disclosed to which online audience with different methodological approaches. Study 1 [53] was a standardized interview study with young Facebook-users. Participants had to indicate in which profile categories they had disclosed content and which privacy setting they had applied to the specific content. They furthermore rated their confidence into the correctness of their assumptions. Afterwards, they logged into their Facebook-accounts so we could check the correctness of their assumptions. Study 2 was an experimental study [54,55] in which participants repeatedly disclosed personal or impersonal information to a small or large audience in a sham social network group. Afterwards they took a memory test in which they had to remember which information they had disclosed and which one not, and furthermore had to indicate the correct corresponding audience. For each answer they furthermore indicated the confidence into the correctness of their answer. Our results consistently show that participants had good memory for the contents they had disclosed, but struggled to associate the correct privacy setting (Study 1) and audience (Study 2). Furthermore, results from Study 2 revealed that users remembered the associations between disclosed content and audience significantly better in the presence of risk cues, namely when disclosing personal information or disclosing content to a large audience.

Although we have no direct empirical evidence for the proposed relationship between a trusting mode of processing and memory processes, specific aspects of this relationship seem plausible in the light of our findings. We argued that the *cp-theory* puts users into a generally trusting mode when communicating online. As a consequence, they might not only be more willing to disclose personal information, but they might furthermore forget even more easily what information they have disclosed to which audience. This forgetting might in turn reinforce the feeling of overall security initially derived from the collective privacy expectation (see Figure 1): Not only does the user believe that her/his information is “protected” by the noise it is surrounded by, but additionally s/he believes to not have disclosed that much information anyway to the public. This theoretically assumed relationship between users’ subjective theories regarding online privacy, their trusting mode of information processing, and their memory for self-disclosures and privacy settings needs to be investigated empirically by future research.

3.2. Metacognitive Accuracy

People do not only process information retrieved from their outer environment, but also experience and interpret variables of the acts of perceiving, processing, learning, and remembering [56]. These cognitions about one’s own cognitions are generally called “metacognitions”, a term encompassing a variety of different sub-concepts [57]. In the following, we will discuss the role of one of these sub-concepts, *metacognitive accuracy*, and its relationship to a trusting mode derived from the collective privacy expectation and to subsequent privacy boundary regulation.

Metacognitive accuracy can be described as the extent to which a person has an adequate model of the state of her/his own cognitions [57]. For example, people demonstrate high metacognitive accuracy if their answer to a question (the criterion) is correct and their corresponding confidence judgment is high; on the other hand they demonstrate low metacognitive accuracy if their answer is incorrect and their corresponding confidence is high [58]. Metacognitive accuracy is crucial because it influences if and how people regulate their subsequent behavior. Research in this area has shown however that people are rarely perfectly aware of the status of their own knowledge, learning, or comprehension, while often being overconfident in their judgments [59]. These judgments and their resulting behavior can be influenced by different kinds of (internal) cues like the familiarity or the fluency of the event or action. For example, Alter and Oppenheimer found that the experience of disfluency in the form of hard-to-read fonts of written texts decreased participants' willingness to disclose personal information [60].

A prerequisite for applying these findings to the realm of self-disclosure in OSNs is to understand that many people use OSNs in such a continuous and routinized manner that their usage certainly constitutes a familiar and in a wider sense fluent behavior. We propose that in a default trust mode, possibly caused by the *cp-theory,* people use internal cues such as the familiarity and fluency of an event to infer not only the trustworthiness of the environment, but also the *confidence into their own knowledge*. In this case, feelings of familiarity or fluency would reduce OSN-users' chances to detect their own memory problems: OSN-users, who do not remember what they have disclosed to which audiences (see previous section) could correct for this problem if they became aware of it, namely if they would monitor the state of their disclosure-related knowledge accurately (metacognitive accuracy). However, if the routine of an action or else the familiarity of its environment spills over to an impression of competence (*i.e.*, regarding one's knowledge of past disclosures or regarding one's knowledge of the applied privacy settings), the accuracy of these judgments is likely to be biased. While the relationship between familiarity and overconfidence in one's own competence is well established [61], little research has been done investigating the extent to which users of OSNs have an accurate impression about their own disclosure-related knowledge. In our own research (see previous section) participants also indicated how confident they were that they had given the correct answer. Across studies our results consistently show that participants indeed struggled to accurately judge the extent of their disclosure-related knowledge, as the relationship between their performances on the one hand and their correctness on the other hand was negligible [53–55].

In summary, we argue that in a trusting mode, potentially caused by the *cp-theory,* users might rather consider cues like the familiarity of an action to not only invalidly infer the trustworthiness of the environment but draw conclusions about also their own competence regarding their privacy boundary regulation. In that way, the *cp-theory* (lying at the core of the trust mode) might bias the way people perceive situational risks. Furthermore, if OSN-users have neither a comprehensive memory of past disclosures, nor are aware of this problem, the trust mode of these mechanisms may be reinforced by the failures it has produced (see Figure 1). Future research needs to empirically investigate this theoretically assumed relationship between users' subjective theories, a trusting mode of processing, and metacognitive accuracy.

4. General Discussion

In a world, in which privacy (as it has been known before the rise of digital technologies) seems somewhat unrealistic, people have to reconcile their basic need to keep things private with their knowledge that the possibility to actually control access to their online information is very limited. We proposed that this reconciliation might take place through the building of a subjective theory about online privacy, often in the form of the *cp-theory*. We thereby built on a discussion put forward by Niklas Lundblad [32] and linked it with a large body of research from different psychological disciplines. When people trust that their personal contents are protected by the noise of the information it is surrounded by, the number of people who are actually thought to receive (in the sense of understand and remember) the information is limited by the potential audience's attentional and processing capacities, or else by the storage capacities of institutions and their number of intelligent agents. We furthermore argued that in a default trust mode people might have problems to (a) remember which self-disclosed information is accessible to which audience; and (b) to be aware about their knowledge and literacy regarding their privacy boundary regulation. While on the one hand these issues constitute a problem on their own as they impede an adequate perception of the risk associated with self-disclosure, they might furthermore reinforce the user's trusting mode.

Naturally, the anecdotal evidence for the *cp-theory* in combination with our own research findings is insufficient to prove our points empirically, and other directions of causality are furthermore possible. For example, it might also be that a lack of memory and metacognitive accuracy puts the user into a mode of default trust which would then be the prerequisite for the building of the *cp-theory*. However, subjective theories are known to be powerful mindsets that determine how situations are interpreted [62]. Therefore, it seems plausible to presume the direction of causality put forward in the previous sections.

Nonetheless, further research is needed to investigate the role of subjective theories for privacy boundary regulation in our digitized society. Thus, future research could assess which subjective theories exist with regard to online privacy specifically, and with regard to digital technologies more generally. Given people actually have distinct subjective theories in these contexts, it could also be important to empirically study if and how they influence people's online behavior, for example their self-disclosing behaviors in OSNs. Moreover, as self-disclosure can be related to both, privacy loss and enhanced social capital, future research might assess how privacy perceptions and behaviors are related to the perceived and actual extent of users' social capital. For example, it could be interesting to systematically investigate how self-disclosure is related to privacy perceptions on the one hand, and to the extent of social capital on the other hand. For example, it might be that users, who neglect their privacy per se, simply have more online interactions and therefore more social capital. On the other hand, competent users might have optimized their self-disclosures in that they experience only minor privacy losses, but maximize benefits from the established social capital.

If the *cp-theory* determines how people handle the tension between self-disclosure and privacy, we need to ask ourselves how people can be influenced to become *vigilant* users instead of users who self-disclose information in a trusting mode by default. We see two major possibilities for change: In the short run, external risk cues could, if displayed saliently enough, disrupt the biasing influence of a trusting mode onto further cognitive processes. For example, technological or interface design changes, as well as privacy policies that are transparent and easy to understand [63] could support users in judging their environment more adequately. In the long run however, we believe that in order to enable users to actually regulate their privacy boundaries according to their personal needs, their subjective theory must be altered, for example in the sense that they do not *generally* expect their information to vanish in the noise of all available data. In this respect, we see a significant need for transparent reports and educational programs aiming to build up common knowledge about how meta-data is used by institutions and what the societal risks of these practices are.

At the same time, one might ask to which extent it is beneficial to enhance users' risk perception, as the general (collective) trust in OSNs is an important prerequisite for the establishment and maintenance of social capital. In this respect, it is crucial to understand that "vigilance (unlike distrust) is not the opposite of trust" [44] (p. 363) but rather indicates the overall *readiness* to perceive a risk. Thus, vigilant usage is not a normative concept and should not keep users from self-disclosing in OSNs altogether, since their usage is associated with a collective action of trusting behaviors that ensure the establishment of social capital, and by extension the functioning of communities in general. Rather, vigilant usage should enable users to adjust their privacy boundaries according to their actual needs instead of their biases.

Educating people to be vigilant users will be difficult for several reasons. First, research consistently shows that it is extremely difficult to change a powerful and seemingly coherent naïve theory [64]. In the context of a subjective theory about online privacy this could be even more difficult, because how users' information is handled by silent audiences on the one hand, and by data collecting institutions on the other hand, eludes their immediate experience [21]. Therefore, the *cp-theory* cannot be disproven empirically and could hence be extremely difficult to overcome.

Second, it is yet unclear by which variables the development of the *cp-theory* is influenced. Thus, the belief into the functioning of collective privacy seems to be prevalent in all kinds of educational and economical strata. For example, there are even *scholarly* recommendations to actually *not* encrypt one's emails as this action would imply that one has something to hide [32]. The reasoning behind this recommendation is highly seductive at first glance, because it resolves all tension created by the dialectical relationship between self-disclosure and privacy: People would be able to maximize the benefits by self-disclosing much information and minimize the associated risks through that same behavior because they add to the overall amount of noise (that seemingly secures the confidentiality of single pieces of information). At the same time however, the reasoning of the recommendation is characterized by a demonstrative *resignation* of all democratic ideas—for after all, within collective privacy there is no possibility for the individual to really control personal information whatsoever. Information is controlled by the processing and storage limits of other people and institutions, and, as Lundblad states, it is thus indeed possible to "chart the life of anyone" [32] (p. 4). The fact that at the same time it is not possible to "chart the lives of everyone" should normatively be of little consolation.

The actual accomplishment of conceptualizing characteristics of a noise society is to bring the role of subjective theories for privacy-related behavior into public discussions. If people were aware of the problematic nature of a collective privacy expectation, they could adjust to digital realities in much more sophisticated ways. As online communication offers new opportunities to get in touch with people, the rather broad concept of social capital [65] might also be re-interpreted in this context: If people would build social relationships within communities that vigilantly observe and discuss these matters, they could reap the true benefit of online social networking, as being a part of such a discursive process makes a functional adjustment to a digital society far more likely.

In the end, users need to be aware of the true nature of associated risks which do not always take place on an individual level, but have a transformative power in a societal, political, and democratic sense. Thus, "the value of privacy eventually (…) ends up relating to one's views on society and freedom" [21] (p. 27).

Acknowledgments

This research was funded by the Research Training Group 1712/1 "Trust and Communication in a Digitized World" of the German Research Foundation (DFG).

Author Contributions

This paper is the result of an iterative process, in which the main ideas were developed in joint discussions between the authors of this paper. The corresponding author wrote the article and the co-authors commented the resulting text, including concrete new text elements.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Petronio, S. *Boundaries of Privacy: Dialectics of Disclosure*; State University of New York Press: Albany, NY, USA, 2002.
2. Boyd, D. Taken out of context: American teen sociality in networked publics. Doctoral Dissertation, School of Information, University of California-Berkeley, 2008. Available online: http://www.danah.org/papers/TakenOutOfContext.pdf (accessed on 22 August 2012).
3. Laurenceau, J.P.; Barrett, L.F.; Pietromonaco, P.R. Intimacy as a process: The importance of self-disclosure and responsiveness in interpersonal exchanges. *J. Pers. Soc. Psychol.* **1998**, *74*, 1238–1251.
4. Ellison, N.; Steinfield, C.; Lampe, C. The benefits of Facebook 'friends': Exploring the relationship between college students' use of online social networks and social capital. *J. Comput. Mediat. Commun.* **2007**, *12*, 1143–1168.
5. Steinfield, C.; Ellison, N.; Lampe, C. Social capital, self-esteem, and use of online social network sites: A longitudinal analysis. *J. Appl. Dev. Psychol.* **2008**, *29*, 434–445.
6. Valenzuela, S.; Park, N.; Kee, K.F. Is there social capital in a Social Network Site? Facebook use and college students' life satisfaction, trust, and participation. *J. Comput. Mediat. Commun.* **2009**, *14*, 875–901.
7. Cozby, O.C. Self-disclosure: A literature review. *Psychol. Bull.* **1973**, *79*, 73–91.
8. Altman, I.; Taylor, D.A. *Social Penetration: The Development of Interpersonal Relationships*; Rinehart & Winston: New York, NY, USA, 1973.

9. Kunnel, A. Eine integrative Theorie der Vertrauenskommunikation in sozialen Onlinenetzwerken [An integretaive theory of trust communication in Online Social Networks]. Unpublished Dissertation Exposé, Westfälische Wilhelms-Universität Münster, Münster, Germany, 2014.
10. Coleman, J.S. Social capital in the creation of human capital. *Am. J. Sociol.* **1988**, *94*, 95–120.
11. Vitak, J. The impact of context collapse and privacy on Social Network Site disclosures. *J. Broadcast Electron. Media* **2012**, *56*, 451–470.
12. Vitak, J.; Ellison, N.B. 'There's a network out there you might as well tap': Exploring the benefits of and barriers to exchanging informational and support-based resources on Facebook. *New Media Soc.* **2013**, *15*, 243–259.
13. Vitak, J.; Kim, J. "You can't block people offline": Examining how Facebook's affordances shape the disclosure process. In Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing, Baltimore, MD, USA, 15–19 February 2014.
14. Burke, M.; Marlow, C.; Lento, T. Social network activity and social well-being. In Proceedings of the ACM conference of Computers in Human Interaction, Firenze, Italy, 10–14 April 2010; pp. 1909–1912.
15. Grossklags, J.; Acquisti, A. When 25 Cents is too much: An experiment on willingness-To-sell and willingness-to-protect personal pnformation. In Proceedings of the Sixth Workshop on the Economics of Information Security, Pittsburgh, PA, USA, 7–8 June 2007.
16. Binder, J.; Howes, A.; Sutcliffe, A. The Problem of Conflicting Social Spheres: Effects of Network Structure on Experienced Tension in Social Network Sites. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Boston, MA, USA, 7 April 2009; pp. 965–974.
17. Rui, J.R.; Stefanone, M. Strategic image management online. *Inform Comm. Soc.* **2013**, *16*, 1286–1305.
18. Norberg, P.A.; Horne, D.R.; Horne, D.A. The privacy paradox: Personal information disclosure intentions versus behaviors. *J. Consum. Aff.* **2007**, *41*, 100–126.
19. Altman, I. *The Environment and Social Behavior*; Wadsworth: Belmont, CA, USA, 1975.
20. Xu, H.; Teo, H.-H.; Tan, B.C.Y.; Agarwal, R. The role of push-pull technology in privacy calculus: The case of location-based services. *J. Manage Inform. Syst.* **2009**, *26*, 135–174.
21. Acquisti, A. Privacy in electronic commerce and the economics of immediate gratification. In Proceedings of the EC'04, New York, NY, USA, 17–20 May 2004; pp. 21–29.
22. Margulis, S.T. On the status and contribution of Westin's and Altman's theories of privacy. *J. Soc. Issues* **2003**, *59*, 411–429.
23. Trepte, S.; Dienlin, T. Privatsphäre im Internet [Privacy on the Internet]. In *Neue Medien und deren Schatten* [*New Media and Their Shadows*]; Porsch, T., Pieschl, S., Eds.; Hogrefe: Göttingen, Germany, 2014.
24. Solove, D.J. Conceptualizing privacy. *Calif. Law Rev.* **1997**, *90*, 1087–1156.
25. Groeben, N.; Scheele, B. Dialogue-hermeneutic method and the "research program subjective theories". Available online: http://www.qualitative-research.net/index.php/fqs/article/view/1079/2354 (accessed on 11 February 2014).
26. Keil, F.C. Folkscience: Coarse interpretations of a complex reality. *Trends Cogn. Sci.* **2003**, *7*, 368–373.

27. Dweck, C.S.; Chiu, C.; Hong, Y. Implicit theories elaboration and extension of the model. *Psychol. Inq.* **1995**, *6*, 322–333.
28. Gelman, S.A.; Noles, N.S. Domains and naïve theories. *Wiley Interdiscip. Rev. Cogn. Sci.* **2011**, *2*, 490–502.
29. Beckedahl, M., Meister, A., Eds. *Überwachtes Netz: Edward Snowden und der größte Überwachungsskandal der Geschichte* [*Surveillance of the Internet: Edward Snowden and the Largest Surveillance Scandal in History*]; epubli GmbH: Berlin, Germany, 2013.
30. Toffler, A. *Future Shock*; Random House: New York, NY, USA, 1970.
31. Franck, G. *Ökonomie der Aufmerksamkeit—Ein Entwurf [Economy of Attention—A Blueprint]*; Hanser: München, Germany, 1998.
32. Lundblad, N. Privacy in the noise society. *Scand. Stud. Law* **2004**, *47*, 349–371.
33. Nickerson, R.S.; Baddeley, A.; Freeman, B. Are people's estimates of what other people know influenced by what they themselves know? *Acta Psychol.* **1987**, *64*, 245–259.
34. Michaelian, K. (Social) Metacognition and (Self-)Trust. *Rev. Philos. Psychol.* **2012**, *3*, 481–514.
35. Jost, J.T.; Kruglansky, A.W.; Nelson, T.O. Social metacognition: An Expansionist's view. *Pers. Soc. Psychol. Rev.* **1998**, *2*, 137–154.
36. Premack, D.; Woodruff, G. Does the chimpanzee have a theory of mind? *Behav. Brain Sci.* **1978**, *1*, 515–526.
37. Litt, E. Knock knock. Who's there? The imagined audience. *J. Broadcast Electron. Media* **2012**, *56*, 330–345.
38. Marwick, A.E.; Boyd, D. I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media Soc.* **2011**, *13*, 114–133.
39. Hoadley, C.M.; Xu, H.; Lee, J.J.; Rosson, M.B. Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry. *Electron. Commer. Res. Appl.* **2010**, *9*, 50–60.
40. Boyd, D. Facebook's privacy trainwreck: Exposure, invasion, and social convergence. *Convergence* **2008**, *14*, 13–20.
41. Ackoff, R.L. From Data to Wisdom. *J. Appl. Syst. Anal.* **1989**, *16*, 3–9.
42. Solove, D.J. 'I've got nothing to hide' and other misunderstandings of privacy. *San Diego Law Rev.* **2007**, *44*, 745–772.
43. Scheele, B.; Groeben, N. *Dialog-Konsens-Methoden Zur Rekonstruktion Subjektiver Theorien: Die Heidelberger Struktur-Lege-Technik (SLT), Konsensuale Ziel-Mittel-Argumentation Und Kommunikative Flußdiagramm-Beschreibung von Handlungen*; Francke: Tübingen, Germany, 1988.
44. Sperber, D.; Clément, F.; Heintz, C.; Mascaro, O.; Mercier, H.; Origgi, G.; Wilson, D. Epistemic vigilance. *Mind Lang.* **2010**, *25*, 359–393.
45. Koriat, A. Monitoring one's own knowledge during study: A cue-utilization approach to judgments of learning. *J. Exp. Psychol.* **1997**, *126*, 349–370.
46. Pintrich, P.R. A conceptual framework for assessing motivation and self-regulated learning in college students. *Educ. Psychol. Rev.* **2004**, *16*, 385–407.
47. Brown, A.; Hornstein, S.; Memon, A. Tracking conversational repetition: An evaluation of target monitoring ability. *Appl. Cogn. Psychol.* **2006**, *20*, 85–95.

48. Gopie, N.; MacLeod, C.M. Destination memory—Stop me if I told you this before. *Psychol. Sci.* **2009**, *20*, 1492–1499.
49. Marsh, R.L.; Hicks, J.L. Comparisons of target output monitoring and source input monitoring. *Appl. Cogn. Psychol.* **2002**, *16*, 845–862.
50. Grudin, J. Desituating action: Digital representation of context. *Hum.-Comput. Interact.* **2001**, *16*, 269–286.
51. Schwarz, N.; Bless, H.; Strack, F.; Klumpp, G.; Rittenauer-Schatka, H.; Simons, A. Ease of retrieval as information: Another look at the availability heuristic. *J. Pers. Soc. Psychol.* **1991**, *61*, 195–202.
52. McCloy, R.; Byrne, R.M.J.; Johnson-Laird, P.N. Understanding cumulative risk. *Q. J. Exp. Psychol.* **2010**, *63*, 499–515.
53. Moll, R.; Pieschl, S.; Bromme, R. Competent or clueless? Users' knowledge and misperceptions about their online privacy management. *Comput. Hum. Behav.* **2014**, *41*, 212–219.
54. Moll, R.; Pieschl, S.; Bromme, R. Sharing in the dark? Target memory and risk awareness in online communication. In Proceedings of the 35th Annual Conference of the Cognitive Science Society, Berlin, Germany, 31 July–3 August 2013; Knauff, M., Pauen, M., Sebanz, N., Wachsmuth, I., Eds.; Cognitive Science Society: Austin, TX, USA, 2013; pp. 3092–3097.
55. Pieschl, S.; Moll, R. For they know not what they do? Target memory and metacognitive monitoring of self-disclosures in Online Social Networks. Westfälische Wilhelms-Universität Münster, Münster, Germany. Unpublished work, 2014.
56. Flavell, J.H. Metacognition and cognitive monitoring: A new area of cognitive-developmental inquiry. *Am. Psychol.* **1979**, *34*, 906–911.
57. Nelson, T.O.; Narens, L. Metamemory: A theoretical framework and new findings. *Psychol. Learn. Motiv.* **1990**, *26*, 125–173.
58. Pieschl, S. Metacognitive calibration—An extended conceptualization and potential applications. *Metacogn. Learn* **2009**, *4*, 3–31.
59. Kruger, J.; Dunning, D. Unskilled and unaware of it: How difficulties in recognizing one's own incompetence lead to inflated self-assessments. *J. Pers. Soc. Psychol.* **1999**, *77*, 1121–1134.
60. Alter, A.L.; Oppenheimer, D.M. Suppressing secrecy through metacognitive ease—Cognitive fluency encourages self-disclosure. *Psychol. Sci.* **2009**, *20*, 1414–1419.
61. Metcalfe, J.; Schwartz, B.L.; Joaquim, S.G. The cue-familiarity heuristic in metacognition. *J. Exp. Psychol. Learn.* **1993**, *19*, 851–864.
62. Molden, D.C.; Dweck, C.S. Finding 'meaning' in psychology: A lay theories approach to self-regulation, social perception, and social development. *Am. Psychol.* **2006**, *61*, 192–203.
63. Stutzman, F.; Capra, R.; Thompson, J. Factors mediating disclosure in Social Network Sites. *Comput. Hum. Behav.* **2011**, *27*, 590–598.
64. Anderson, C.A.; Lindsay, J.J. The development, perseverance, and change of naive theories. *Soc. Cogn. Spec. Issue: Naive Theor. Soc. Judgm.* **1998**, *16*, 8–30.
65. Adler, P.S.; Kwon, S.-W. Social capital: Prospects for a new concept. *Acad. Manag. Rev.* **2002**, *27*, 17–40.