An Exploratory Qualitative Study on People's Attitudes towards Offline and Online Social Networks

A Case Study at a Brazilian University

Maria L. B. Villela[1], Simone I. R. Xavier[1,] Raquel O. Prates[1],
Marcos O. Prates[2], Antônio A. P. Prates[3], Alexandre A. Cardoso[3]

[1]Department of Computer Science– ICEx – UFMG - Belo Horizonte – MG, Brazil
Emails: {simone.xavier, mvillela, rprates}@dcc.ufmg.br

[2]Department of Statistics – ICEX – UFMG - Belo Horizonte – MG, Brazil
Email: marcosop@est.ufmg.br

[3]Department of Sociology – FAFICH – UFMG - Belo Horizonte – MG, Brazil
Emails: aaprates@oi.com.br, alexcard@fafich.ufmg.br

***Abstract*— Social networks have emerged as a new medium for sharing and exchanging information. As such, it brings new possibilities and challenges to people's interaction. In this work, we have investigated through a qualitative study one of these challenges: how people perceive and deal with privacy in online networks, as opposed to the physical world. Our findings from interviewing Facebook users show that although they perceive the online and offline worlds as connected, there is a significant discrepancy between their attitudes towards privacy in online and offline social networks, as well as strategies developed to deal with some of the experienced issues. Based on these findings, we discuss how design decisions are related to privacy issues identified through the interviews and considerations for the design and evaluation of online social networks.**

Keywords*— Social networks; privacy; qualitative study; online x offline; physical x virtual; contrast; GranDIHC; Facebook; Brazil.

I. Introduction

Ever since the first social network system (SNS) was launched in 1997 by Sixdgrees, many others have followed and their use has increased around the world [1]. However, along with all the benefits to users associated to their high popularity, information sharing in these systems has also brought privacy to the forefront of the research agenda for information technology [2]. In this same direction, the Brazilian HCI scientific community has identified privacy as being among the great HCI research challenges of this decade (2012-2022) [3].

Recent works have pointed out how fragile privacy can be in SNSs and the risks involved when it is not adequately managed [4]–[6]. Other works show that users' privacy is even more vulnerable when users accept and use default settings, which tend to be very permissive [5]–[7]. Thus, many researchers have tried to understand how people have used resources offered in SNSs, how vulnerable their personal information is and how they share their information online [6], [8]–[10]. Other studies have broadened this understanding by contrasting people's relationships online and offline, or even tried to understand how offline behavior may impact or determine online behavior [11]–[13].

In this paper, our goal is to investigate values, attitudes and perceptions of SNSs users in relation to privacy in the virtual and physical worlds. In other words, explore how people deal with privacy online and offline and their reasons for it. By doing so, we contribute to the large body of research work in privacy by providing a broad analysis on the contrasts between online and offline privacy in the users' perspective.

In order to achieve our goal we conducted in-depth semi-structured interviews using the Underlying Discourse Unveiling Method [14] . The interviews were conducted in face-to-face settings with 20 participants from the academic community (students and faculty) of the Federal University of Minas Gerais (UFMG) in Brazil in March 2013. All participants were Facebook users, since Facebook was selected as the social network for the study due to its high popularity in Brazil.

Our findings from the interviews indicate that users believe that the online and offline worlds are interconnected, but they perceive them as different spaces with distinct characteristics. While in the physical world they classify relationships in different levels of sharing and trust, in the virtual world these levels are commonly reduced to two. As a result they tend to adopt different strategies: the information they do not consider to be personal they share more broadly; whereas the information they consider personal they tend to share less (or not at all). Although sharing structures in online world are simplified in relation to the offline world, they believe that managing privacy online is more difficult. Most of the participants reported having had negative experiences regarding privacy and, they also believe that in general people are overexposed on SNSs. Based on these findings we discuss considerations regarding Facebook interface and aspects to be considered in the (re)design and evaluation of interactions in SNSs and their interfaces.

In the next section we present privacy related works that are closest to ours. Then, in Section III, we describe the

ISSN: 2236-3297

methodology adopted for our study and how it was conducted. The following section presents the results that emerged from the analysis of the interviews. Then, in Section V we discuss how these findings relate to interface design decisions for SNSs. Finally, we present our final remarks regarding the paper's contribution and the next steps in our research.

II. Related Work

The evolution of the concept of privacy follows the evolution of information technology itself [15]. In the offline world, privacy related to self-disclosure is easy to achieve because people usually share their personal information to a restricted and trusted audience. The rise of the Internet and Web 2.0 dramatically changed the landscape of information exchange, given the vast amount of personal information that is collected, processed, distributed and used through it. Thus, privacy concerns related to the online world rose to new highs. Addressing online privacy specifically in SNSs is a complex issue, which involves factors ranging from users' behavior to features of the system and it has been broadly studied by researchers. In this section, we focus on prior works that are more closely related to our goal: (*A*) works that address the interconnection between online and offline worlds; and (*B*) works that focus on SNSs users' behavior in SNSs, and (*C*) privacy handling within these systems.

A. Interconnection between offline and online worlds

The idea of privacy is as old as mankind. Privacy concerns started in relation with the protection of one's body and home, and soon evolved into the control of one's personal information. The development and use of technology in an information society brought a novel set of challenges and issues in regards to privacy, as it continuously increases the possibility for personal data to be collected and stored [16]. Since then, many discussions about online privacy emerged. This topic becomes even more complex with the advent of social networks.

Several studies have explored how online and offline contexts are intertwined. Cranshaw et al. [17] provided a model for predicting friendship between two users in SNSs by analyzing their location trails, based on the investigation of relationships between the users' mobility patterns and structural properties of their underlying online social network. Grieve et al. [18], in the opposite direction, investigated offline social connectedness derived from the use of Facebook and concluded that it may act as a separate social medium in which to develop and maintain relationships, providing an alternative social outlet associated with a range of positive psychological outcomes. Subrahmanyam et al. [13], on the other hand, shows how young adults use SNSs to strengthen different aspects of their offline connections.

Gross and Acquisti [19] claim that trust in and within online social networks may be assigned differently and have different meanings than in their offline counterparts. This is a consequence of the fact that offline social networks are extremely diverse in terms of how close and intimate a subject perceives a relation to be, while online social networks, on the other hand, often reduce these nuanced connections to simplistic binary relations: "Friend or not".

Rosen et al [11] addressed the impact of offline social network characteristics on online behavior of people from different cultural backgrounds. Their results suggest that SNS users who maintain larger offline strong-tie networks have larger online networks, indicating that their face-to-face networking behavior is indicative of their use of SNS. Results also show that participants who identify with more individualistic cultural backgrounds have a greater proportion of online friends who they have not actually met face-to-face, and share more photos online as opposed to participants who identify with less individualistic cultural backgrounds.

Specifically on self-disclosure, a review of 24 recent studies, each of which has examined the level of self-disclosure in online compared to offline contexts focusing on dyadic interactions was performed [20]. Contrary to expectations, the authors of this study found that disclosure was not consistently found to be greater in online contexts. Factors such as the relationship between the communicators, the specific mode of communication, and the context of the interaction appear to moderate the degree of disclosure. Finally, a survey with 148 participants was used to examine and compare how self-disclosure may differ in three distinct spaces: offline, general online and specific contextual online environments [21]. The results suggested that participants were willing to disclose more of their private information in face-to-face settings than within an online space.

B. User behavior in SNSs

Before understanding how people behave in SNSs, it may be important to understand the reasons why people use these systems, in order to identify the relationship they establish between their offline and online social networks. Studies have shown that one of the main reasons why people use these systems is to maintain and strengthen existing relationships [22], [23]. In this direction, previous researches suggest that people use SNSs more often to meet friends with whom they have an offline connection than to ''browse'' for complete strangers to meet [24], [25].

Another study has also identified relationships between the reasons people use SNSs and how they behave in these environments. Actually, the differing goals for using Facebook are reflected not only in behaviors that lead to usage patterns, but also in users' privacy settings. For instance, it was found that people whose privacy settings are more permissive are more likely to want to meet new people [26].

The understanding of how people behave in SNSs, specifically considering the disclosure of personal information to others, can be used as a starting point to understand the relationship between the online and offline worlds. Disclosure on SNSs may have significant consequences in relationship management and psychological well-being, as well as usual behavior, as shown in [22] by examining the perceived motivations and consequences of voluntary information disclosure of Facebook active users. These authors' findings indicate that the reasons why people disclose information on SNSs are: information sharing, information storage and entertainment, keeping up with trends, and showing off.

A factor related to users' behavior that causes privacy-related issues in SNSs is that, although they often willingly, share personal identifying information about themselves in these environments, usually many of them do not have a clear idea of who accesses their private information or what portion of it is really available to be accessed [27]–[30]. Rauber and Almeida [6] investigated privacy awareness of Facebook users in Brazil and India, using real-world data collected from an app installed in their computers. Their results show that only a small part of the users seem to be really aware of the consequences of permissive settings and their pervasive consequences, and, therefore, do not reveal any of their personal identifiable information. They also show that the majority of the users reveal publicly their gender on Facebook and that users exercise more control over content with more potential to endanger their reputation, such as videos and photo albums.

Vitak and Kim [8] explored the self-disclosure practices of 26 American graduate students on Facebook through in-depth interviews. Their findings reveal that users employed a wide spectrum of strategies to help them achieve their disclosure goals while decreasing perceived risks associated with making disclosures in a public forum. These strategies generally sought to recreate the offline boundaries blurred or removed by the technical structure of the site and allow users to engage in a more strategic disclosure process with their network. In a different direction, a questionnaire was applied to over 400 Internet users, focusing specifically on Facebook and those users who have left the service [31]. Results of the qualitative analysis reveal numerous complex and interrelated motivations and justifications for leaving Facebook. Privacy emerged as a resounding theme, with over a quarter of respondents citing privacy concerns as a reason for leaving, limiting, resisting, or considering leaving this system. Besides privacy, other motivations cited by participants for non-use include data misuse, productivity, banality, addiction, and external pressures.

C. *How people deal with their privacy in SNSs*

Several studies have sought to understand what factors impact the way people deal with privacy on SNSs. In this direction, individual experiences, such as user's network or frequency of use [32], [33], as well as having already been exposed to or been victim of personal information abuses [34], lead to stronger concerns regarding information privacy.

Studies also have shown that users' personal characteristics, like gender or culture, also impact their attitudes and behaviors related to privacy in SNSs [6], [33], [35]–[40]. Fogel and Nehmad, for example, identified that the level of privacy concern in these environments is higher among females when compared with males [36]. Concerning culture, an in-depth analysis of results from an online survey, which indicates significant differences between Hong Kong and French SNS users, in respect to their privacy settings and their usage patterns in general was presented [39].

In the opposite direction, studies have shown the effects of privacy concerns in attitudes and behaviors of users in SNSs [35], [41]. Stutzman and Kramer-Duffield [35] found that increasing levels of interpersonal privacy management are positively associated with the fact that people have a profile visible only to friends on Facebook. Staddon et al. [41] conducted a survey with 1,075 U.S. Facebook users and their results show a strong association between low engagement and privacy concern. Specifically, users who reported concerns around comprehension of sharing practices or general Facebook privacy concerns, also reported consistently less posting, commenting and "Like"ing of content.

* * *

As shown in this section there is a large body of work that investigates aspects related to understanding users' behaviors and attitudes towards privacy in SNSs. In analyzing online and offline worlds, prior work has investigated connections between people's online and offline networks, trust levels associated to them and differences in self-disclosure in each of these environments. Analyses of user behavior have explored how motivation for using SNSs is related to information disclosure, the reasons associated to information disclosure, what pieces of information they tend to protect more or less, as well as identified how privacy concerns have led users to develop different strategies to deal with information disclosure on Facebook, or even to stop using it. Finally, other works have identified how factors such as gender, culture or previous experiences impact how people deal with their privacy settings. Our work contributes to the current state of the art by investigating users' attitudes towards the online and offline worlds and how it shapes their decision on what or how to share information in each of them, aiming to understand how SNSs have changed the way people deal with the privacy of their information.

III. Methodology

An exploratory study was conducted aiming to probe people's attitudes towards online and offline privacy, through semi-structured interviews, applying the Underlying Discourse Unveiling Method (UDUM) [14][1]. UDUM is an exploratory research method that allows for a systematic analysis of discourse material, especially one collected through semi-structured interviews [14]. Thus, such method does not start from a pre-defined hypothesis, but rather from an open question one aims to investigate. As a qualitative method, UDUM focuses on in-depth and detailed results achieved from the analysis of small samples, seeking to make the latent meanings present in the users' discourse explicit. It unveils hidden or implicit fears, desires, motivations, conflicts, and other deep feelings experienced by individuals. The method was particularly well suited for this work, given the highly subjective values and attitudes underlying how people deal with privacy.

A. *Preparation*

In order to collect data for our research, we followed UDUM recommendations to perform face-to-face interviews.

[1] Currently there are no references about UDUM in English, but the reader may be interested in other works published in English that present and apply the method, such as that [43], [44]. Note that Nicolaci-da-Costa, one of the authors of UDUM, is also a co-author of both these papers.

In order to investigate people's attitudes towards online and offline privacy, it was necessary for the participants to have experience in using SNSs. UDUM suggests that the more homogeneous is the group in the study, the more precise the study will be, thus we decided to focus on users of one specific SNS. Since at the time of this research Facebook already was the most popular SNS in Brazil and the world[2], our decision was to interview Facebook users. We also decided to select participants who were students or professors at the Federal University of Minas Gerais (UFMG) in Brazil as an attempt to minimize the differences between the participants and the external factors that may bias their responses.

Previous works have shown that some factors may impact people's attitudes towards privacy, such as understanding how technology works [33], age [42] and gender [6], [36]. Thus, in order to avoid a bias resulting from one of these factors, we decided to include participants who varied according to these factors. To vary participants' understanding of technology, we chose people from IT and non IT fields. With respect to age range, people of each background group were divided into two groups – from 18 to 35 years old and over 35. Also, we selected an equal number of male and female participants. Based on these criteria, 20 participants were selected from the researchers' network of contacts and 4 groups were formed, each one with 5 participants. Table 1 shows participants distribution according to the criteria.

TABLE 1 –PARTICIPANTS' CHARACTERISTICS.

Age range Field	18 a 35	Over 35	Total Number
Non IT	Participants[1] E1 - E5	Participants[2] E16 - E20	10
IT	Participants[2] E6 - E10	Participants[1] E11 - E15	10
Total Number	10	10	20

1Three males and two females
2Two males and three females

The interview was comprised of 23 open-ended questions, divided into four thematic sections, which addressed several issues related to privacy. The first section featured questions about the understanding of privacy, how much the participant is concerned with privacy and how he/she shares his/her personal information in the physical world. In the second section there were questions exploring the differences between online and offline privacy. The third section focused on information about participants' experiences on Facebook and how they dealt with privacy in this environment. Thus, this section featured questions on the use of privacy settings on Facebook and with whom participants share their information in this system. Finally, the last part had questions related to privacy in the society at large, such as participants' opinions about privacy as an essential right and about people's overexposure on SNSs.

B. *Conducting the interviews*

Before the actual interviews, a pilot interview was conducted with the participation of two members of the research team who would be conducting the interviews. The pilot aimed at testing the interview guide, as well as allowing the interviewers to develop a joint style for conducting the interviews. Face-to-face interviews were conducted in March 2013 in Portuguese, in private places chosen by participants, and lasted on average 39 minutes (interviews varied from 20 minutes to 1:03). Some interviews were conducted jointly by the two interviewers, while others were conducted by either one of them separately. Participation was voluntary and all participants read and signed the consent form before the interviews. The audio of each interview was recorded and later transcribed for the analysis step.

C. *Analysis step*

In UDUM the analysis step is comprised of two sub-steps: inter-participant analysis and intra-participant analysis [14], [43], [44]. In the inter-participant analysis the answers given by all participants to each individual question are closely examined in search of recurring categories, metaphors, positions, behaviors, feelings, beliefs, etc. that would allow access to group culture. Recurrences that have a higher frequency are assigned a higher priority. The intra-participant step involves analyzing all answers given by each participant. The analyst looks for occasional contradictions and inconsistencies in participants' statements. If any are found they could be a good pathway to invisible aspects that underlie human behavior, such as desires, motivations and/or fears. With the insight generated by the intra-participant step the analyst goes back to the answers and performs a second analysis of the inter-participant step. The iteration takes place as many times as needed. As a result of the analysis, the researcher identifies a set of categories that have emerged from participants discourse and that is then used to present the results. In this research the analysis was performed by the two researchers who conducted the interview.

IV. RESULTS

Before presenting the resulting categories, it is interesting to note that, as in the scientific literature [45], there does not seem to be a consensus on the definition of privacy among the participants. Our analysis shows that people understand privacy differently. For many participants, the concept of privacy is understood as them not having to report on their actions to others. For example, participant E2 (M, 28, nIT)[3] defined privacy as: *"[privacy] is the set of attitudes, actions and behaviors that takes place in a private space, at home or related to a life in which one doesn´t have to report to others"*[4]. In this regard, privacy was also associated to having freedom of actions and control over who can have knowledge of these actions, as defined by E7 (F, 25, IT): *"[...] I think that privacy is people being able to do what they want, without*

[2] Data accessed on: http://www.alexa.com (Last visit May, 2015).

[3] In parenthesis, the respondent's gender, age and background in Information Technology (IT stands for Information Technology and "nIT" stands for "non IT").

[4] As mentioned, all the interviews were conducted in Portuguese (participants' first language). The quotes presented in this work have been translated to English by the authors.

having to tell the rest of society."

For many of the other participants, on the other hand, the concept of privacy was more associated with the selective control of what should be shared according to their trust of or their degree of intimacy with the audience that will have access to the information, as illustrated by E17's (M, 43, nIT) speech: *"[...] in general terms, it would be something that I would not share with other people, unless they were very close and, even with people as close as relatives, some topics would not be shared"*. E13's (M, 41, IT) definition of privacy directly referred to trust: *"[...] whatever you want to keep just to people of your complete trust"*.

Participants' definition of privacy seems to be influenced by their age. The definition "*of not having to report on one's actions*" was mostly mentioned by participants in the 18 to 35 age group. Whereas, participants over 35 seemed to associate privacy to "*being able to select what to share and with whom*" more often.

A. *The most personal information is related to safety, relationships and feelings*

We sought to know what information participants consider the most personal, i.e., those pieces of information they retain more or choose not to share with a broad audience. We identified that the two types of information participants considered the most personal were related to safety and to emotions.

Participants' main concern was associated to sharing information related to safety, such as identification cards, phone number and address. Respondents were afraid what may happen if there was improper disclosure of such data. E8 (F, 23, IT), for example, voiced her concerns in this direction when asked about what types of information she considers to be personal: *"For me, private personal information is telephone number, CPF*[5]*, ID, anything that could be used and somehow could harm us"*. E12 (M, 42, IT) also showed the same opinion: *"Well, mainly identification documents, right? All types of identification documents, right? I don't like to inform some types of identification documents at just any place. Anything that might allow someone to take my place [...]"*.

Still regarding information related to safety, several participants also considered information about their routine, such as the place where they were, as private information which people should be careful about, as stated by E10 (F, 26, IT): *"[...] and where I am, for example, I am totally against that Foursquare. I think that is too much privacy invasion. People are always posting ´I´m here´, 'I´m here'. I even think that type of thing is dangerous. This is the type of information I think is necessary to keep confidential"*.

In addition to safety, information about close relationships, feelings and behaviors were also considered highly personal. E2 (M, 28, nIT) expressed this view when talking about what kind of information he keeps private: *"[...] the information that I tend to keep private is related to my closest relationships, right? So the relationships with friends, relationships with family, relationships with my intimate life, right? There are dimensions in life that I don´t usually share in social networks in the internet, nor with people in public places..."*. E5 (M, 23, nIT) also makes this same point clear: *"[...] Maybe in a work environment it's a project, or information about a project, or it may be data…, in the private life it may be feelings, emotions, ways of acting, this would be information that should not be shared…"*.

On the other hand, sharing academic and professional information was not of much concern to participants, as can be seen in E14's (M, 37, IT) speech: "*[ ] this topic about where I work or study, I think there is no problem in sharing"*. The majority of participants reported disclosing this type of information publicly or with friends on Facebook. For example, when asked if he shares such information on SNSs, E17 (M, 43, nIT) answered: *"Yes, these things 'school', 'where I´ve studied', this I think is interesting to be able to bring together people we haven´t seen in a long time and were friends with before. So, it is a way to recover those memories"*.

B. *Information considered very private may not be on SNSs*

There are different degrees of how personal a piece of information might be [46], [47]. During the interviews, we noticed that participants adopt different strategies to decide what personal information they will (or not) disclose on SNSs, depending on how private they think the information is. Therefore, the more private a piece of information is, the smaller the chance of it being shared on Facebook.

Even those participants whose information is visible only to friends rarely post on SNSs information they consider very private. For example, E3 (M, 25, nIT) said that he shares his photos on Facebook and restricts the visibility of all the information he posts to his friends. However, he stated he would not post information that he considers to be very personal: *"Oh, I tend to post more a song, a piece of international news, national news, some joke I find funny, but my stuff, things that I am saying, I don´t post"*. E2 (M, 28, nIT) also demonstrated this caution: *"[...] I´ve already forgotten my Facebook open and a colleague had access to it. It was, is something unexpected, but it was not embarrassing because, exactly, I do not feel that my Facebook is a place filled with secrets, I don´t feel like I share my privacy there"*.

Participants reported disclosing on SNS personal information such as tastes, links, photos and other's posts, besides likes or comments on the posts of others. On the other hand, participants avoid sharing information considered more personal, like problems or details of their relationships. This distinction is made clear by E5 (M, 23, nIT), when he talks about what he discloses on Facebook: *"So, the information that I currently post is more related to principles, religious issues and... mainly that, no personal information, nor feelings, nor emotion, nor anything, only things of spiritual nature"*.

It is noteworthy that the concepts of what would be personal information and which information would be too

[5] CPF is the Brazilian identification document equivalent to the Social Security number in the US.

private to be disclosed on SNSs are subjective. For example, in this passage E4 (F, 21, nIT) says that sometimes she uses Facebook as an outlet because she does not consider her outpours something so personal that she cannot share in her timeline: *"But thinking of social networks and things of the sort, I protect myself up to a point, but, at the same time, it is a place I use as outlet at some moments"*.

On the other hand, E5 (M, 23, nIT) reported not disclosing feelings on Facebook because he considers this kind of information too private. Some participants talked about it explicitly, showing that they understand that the concept of what is personal or not is quite subjective. When E7 (F, 25, IT) is asked about what kind of information she considers to be personal or private, she says: *"That, each person decides what it is, I imagine that each one decides what is personal or not, what is public or private, I don't think there is a general label, it is up to the person to define it"*.

Nineteen out of the twenty participants adopt a strategy which basically consists in evaluating how private they consider the information to be, to determine if it will be posted or not on Facebook. The one participant who did not adopt this strategy claimed to have all the information about himself set to private and to never post anything about himself, only relevant Government campaigns or information (e.g. missing person).

Participants might classify how personal the information is based on the risks they perceive could result from its disclosure. Thus, the greater such risk, the lower is the chance of disclosing it in these systems. For example, E16 (F, 44, nIT), in addition to sharing many photos only with her friends on Facebook, discloses other information she thinks have a low risk of being criticized: *"I share those [comic] strips, post information about some plans, some achievements, but nothing actually that can generate envy or mocking"*.

Participants also pointed to reasons that led them not to share some information. One of the reasons that participants mentioned for not disclosing more personal information on SNS is the cost associated with properly restricting access to that information. For example, the E11 (F, 42, IT), when asked if she uses "lists"[6] on Facebook, indicates she does not think the cost to use it is worth the benefits: *"I know that they exist, once I tried, more or less, classifying, but then I noticed that I had too many friends to waste my time classifying [...]. The time I spend in Facebook is not enough to classify my friends in that (laugh)"*. E10 (F, 26, IT) also demonstrated a similar view regarding the list resource: *"I end up separating [with the automatic list], well, a little bit, just family and friends, I have not gotten to separating [manually], nope, never had the patience to separate it.*"

Based on our interviews we noticed that the list resource, provided by Facebook designers, is, in general, declined by users as a resource to manage their privacy. Participants prefer alternative ways to manage it, including the strategy of not disclosing certain pieces of information on the system.

Another reason that people indicated for not disclosing their information on Facebook is the general lack of trust that their data will be kept private, even by companies responsible for the sites. An example of this concern is voiced by E5 (M, 23, nIT): *"[...] what happens nowadays is: you register in a site and your information ends up in ten different sites…"*. E11 (F, 42, IT) also expressed the same concern: *"Facebook I understand as a public thing [...] if I posted it there, it is not mine anymore, I am not the owner of that space, I can even delete it, but I know very well that I delete it, it won't show up in my timeline but it has not been erased from the database…"*.

C. Offline and online sharing levels are not the same

During the interviews, participants were asked to list with whom they share more personal information in the physical world, in descending order. Based on their responses we identified offline sharing levels, i.e., who are the people to whom they entrust their personal information, grouped into levels, from the highest trust level to the lowest. Each participant could report as many levels as considered necessary. Thus, it was observed that the levels differed among participants, but all of them reported having at least three sharing levels. E7 (F, 25, IT), for example, has four sharing levels: *"Look, with my mother, usually, I come home and tell her everything that happened during the day, I tell her everything. To my best friends, like, I tell, sometimes my worries or interesting stuff, [...]. To my cousins, like, I meet them, talk about general things of life, to my colleagues, everyday things, but it decreases, right, how much we talk about..."*.

Besides the change in the amount of information that is shared in each level, we also identified situations where the type of information shared might also change within the same level or between different levels. When asked whether there would be differences in the type of information he shares at each level, E2 (M, 28, nIT) says: *"Yes, there is. For instance, information related to my sexuality, I don't usually share with my family [...]. With my friends, on the other hand, I don't usually share financial challenges in life, for example, I feel a little embarrassed"*.

By contrasting the sharing levels that participants have in the physical world and their criteria for accepting friendship requests on SNSs, we found that almost all of them do not reflect in these systems the way they share information in the physical world. For example, E6 (M, 23, IT) shares publicly all his Facebook posts, while in real life he has the following sharing levels: family, girlfriend and close friends, friends not so close and colleagues. Thus, in most cases, in their daily lives, participants consider they have several levels of trust. However, on SNSs they treat all of these levels the same way, i.e., all of them are classified as friends and have access to the same information (or all users, if the information is public). E9 (M, 26, IT) seemed to realize such situation, when asked if he had sharing differences within the same level: *"You have a different level of trust with each person. However, sometimes, in social networks, you may end up generalizing"*.

[6] List is a resource that allows users to group friends and might be used for privacy management. See https://www.facebook.com/help/325807937506242/ (Last visited in May 2015)

From the interviews, we concluded that users adopt two main strategies to deal with the privacy of their information on Facebook, switching between them according to how personal they consider the information to be: a) they do not post the information and treat everyone as being in the lower level of trust; b) they share the information, treating everyone within the level where there is enough confidence to give access to that information.

In strategy “a”, information filtering is done outside of the SNS and the person chooses to expose less on this system than he/she would offline. Thus, users decide if that information can or cannot be accessed by all users who are on their friends list, or even if it can be accessed by anyone, if their posts are shared publicly. E6 (M, 23, IT) illustrates this point in his interview: *“So, when I post, I already post thinking that everything is public, see, I don’t try to protect myself in that way, I don’t try to trust that ‘hey, this will only be seen by this guy’. No. I already think about the worst case. Everything I post is accessible to everybody, so I have to take precautions against everything”.*

In contrast, in strategy “b”, users choose to expose more on SNS than they would offline. Thus, in order not to have to worry about privacy settings, and still share with some participants things they consider interesting, they give access to that information to their whole contact list (or to the whole network, if their posts audience is set as public). E10 (F, 26, IT) illustrates this point when talking about her trip photos, which she had already mentioned posting on Facebook. When asked if SNSs have changed her concerns about privacy she says: *“I guess a little [...], because you wouldn’t walk around, for example, with a photo album of your trip saying: ‘Hey, you that I met in the hall, take a look at my trip’. You end up exposing yourself more…”.*

Regarding the adoption of these strategies by participants, we observed that they often use both, choosing which one of them to apply in a context according to how personal they consider a piece of information to be. They adopt strategy “a” (sharing with no one) when they consider the information to be of a more personal nature, and adopt strategy “b” (sharing with everyone) when the information, although personal, is perceived as less critical. Even though they are aware that in adopting strategy “b” they are sharing the information more broadly, the possibility of restricting is usually perceived as not being worth the cost to do it.

D. The physical and virtual worlds are interconnected

The broad use of SNSs, and even of the internet has changed how most participants deal with their privacy. For many of them, privacy concerns have increased since they are aware that in SNSs their information is accessible to more people than in the offline world. E8 (F, 23, IT) talks about it when asked if SNSs have changed the way she cares about privacy: *“[...] it changed a little. Because, like, I think that when you are away from someone, that information is hard to reach that person, but with the social network, it is much easier for this information to reach that person. [...] and I think that in the real world, this is not as easy to spread”.*

For some participants, SNSs have increased their privacy concerns even in the physical world, as they consider that their attitudes could be recorded and published online, even without their consent, as explained by E12 (M, 42, IT): *“[...] without the networks, we had the usual concerns about privacy. Now you have to worry about this issue, like I was telling you, if you are going to show up in a friend’s picture [...] in Facebook...”.*

Few respondents said that SNSs have not changed anything in their privacy concerns, since they rarely post information on these systems or even because SNSs were already part of their lives from the moment that privacy began to be of concern to them. For example, E1 (F, 22, nIT), explaining why her concern about privacy had not changed, said: *“Worrying with privacy... does not change, because ever since I know the internet, there have been social networks. Ever since I know privacy there have been social networks...”.*

Most participants think that online and offline worlds are connected, either because information disclosed online becomes conversation topics in the offline world, or because people reflect in the online world their thoughts, attitudes and behaviors from the offline world. E5 (M, 23, nIT) and E10 (F, 26, IT) illustrate in their discourses these points of view, respectively: E5: *“[...] the information that is available online is brought up, all the time, offline. For example, I’m talking to you here and ‘Oh, did you see what that guy posted’, if it is a common friend, then, online privacy is related to offline privacy, yes, in that sense, it is”.* E10: *“[...] everything is already linked, you are in real life doing something, ‘I’m eating my desert’, at the same time, you take out your phone, take a picture and show everyone in your online life what you’re eating. I think that nowadays, things are very intertwined”.*

When comparing online and offline privacy, participants commented on the audience, the spreading and the impact of information shared on SNSs, which are much higher than in the physical world. For example, E1 (F, 22, nIT), comparing the online and offline worlds, said: *“[...] if you have a social network, that already is some level of exposure, you post your pictures there, you comment on things you’re doing [...]. Offline that happens too... but I think that online it happens much more, because anyone can be there looking at your life...”.*

Some participants demonstrated concern with this fact and highlighted the importance of restricting the information shared in the virtual world when compared with the physical world. In that direction, E17 (M, 43, nIT) says that: *“If there is anything that happens in the family level or with friends, and you register that moment and keep it, just those people and you have it. From the moment you post it in the social networks... it gains a dimension that you, sometimes, may lose control of. And, sometimes, it’s not good to disclose some moments that are more intimate, that is something very private”.*

Therefore, the perception of most participants is that SNSs have brought changes to their privacy concerns. These changes could be either the need to adopt a more cautious attitude online than offline, or even to be more mindful in the physical world in order to avoid being taken by surprise by their information being disclosed inappropriately online. Thus, participants understand online and offline privacy as connected, i.e., one can be reflected upon the other, and they are concerned about their behaviors and their consequences, especially in the virtual world.

E. *Management of online privacy is more difficult than offline privacy*

The vast majority of participants explicitly said or indicated that they consider online privacy to be more difficult to manage than offline privacy. The main reason for this, mentioned by participants, is because in online environments their information has a broader and sometimes unknown reach. For example, E1 (F, 22, nIT), when explaining why she thinks that online privacy is more difficult to manage, said: *"[...] In the offline [world] not many people have access to you, you are surrounded by many people, but it's less than online. In the online [world], any person can find me and have access to my data..."*. E13 (M, 41, IT) presented a similar explanation: *"[...] because it's more open, there are more paths, [online privacy] is more difficult to control. Thinking of my house: I lock the front door, in principle no one can get in and, if anyone does get in, I know that someone has forced their entrance to my house and found some document or something they were not supposed to. Not online. Suddenly the person is accessing my account ... without me knowing it, because there are mechanisms for that. Then, like, I think offline privacy is easier for you to control, manage and all"*.

Some participants attributed the reason they believe online privacy is more difficult to manage than offline privacy to the fact that privacy control in the virtual world does not only depend on them, but also on others. For example, E9 (M, 26, IT) justified this difficulty by not being able to have full control over the disclosure of his information: *"[...] online is harder... you go to a party, let's suppose, and someone takes a picture of you, and posts it in Facebook. That photo is not in your control, but you're there, on display, so it's a little out of your control"*. E11 (F, 42, IT) also illustrates her perception of the challenges in managing her online privacy related to being a professor: *"[...] Sometimes I would say something in the classroom without any worries about the consequences of what I said, because I knew that I said it there, and then it was over. Now, I said something here, but it's not over, I said it here, and tomorrow it may be in Facebook, it could be in Facebook within five minutes, because it's real time, it's recording here and already posting..."*.

The vast majority of respondents indicated several differences between online and offline privacy showing that, in their perception of privacy, one is required to be more cautious when managing privacy in online environments. One of the perceived risks is a higher chance of losing control over the information being shared.

F. *Negative experiences - Exposure out of control*

Most participants reported having already had negative experiences regarding privacy on SNSs. We classified participants' negative experiences into three main types of issues in these environments: a) lack of control of disclosure of users' information in SNSs by others; b) undesired system discourse on users' behalf; and, finally, c) problems caused by the misuse of these systems by other users.

The first type of issue – lack of control of disclosure of users' information on SNSs by others – consists of the inconveniences caused by the actions of others and involves the lack of control users have over the actions that third parties can take with their information. One example, cited by several participants, is the posting of photos or videos that include them without their consent. E15 (F, 38, IT) reported her negative experience: "*So, an experience I had on a birthday [...] you select some people, because the apartment, the space available... Then, a friend posted on Facebook some pictures that I had not wanted to be put on Facebook, because there was one specific person that I had not invited"*.

Still regarding problems caused by third parties, another negative experience often cited by participants was inappropriate comments. E16 (F, 44, nIT), talking about her negative experience related to privacy on Facebook, said: *"[...] people make rude comments, make jokes that are not funny, trespassing the limits of your privacy"*.

The second type of issue is related to Facebook's initiative in some contexts to "speak" on behalf of the users. Related to this issue, we have identified two situations, one in which Facebook highlights users' activities to (some of) their friends, and the other in which it offers new information about users' actions in the system to another user.

Regarding Facebook highlights, participants mentioned several experiences in which they felt exposed or monitored on SNS, often not knowing what to do to avoid such a situation. E7 (F, 25, IT) expressed that she felt exposed by the Facebook resource that shows her friends' actions in real time, and that she could not disable it in order to avoid others from being informed of what she was doing: *"One of the things that happened in Facebook was, not that happened, happen, but yesterday they took it down, I think there might have been so much complaining, that yesterday disappeared the small window on the right side that everyone sees everything that you do, comment, like. And I, at least, had not found a way to prevent people from seeing it, because it's within my circle of friends, but it does not mean that I want them to see that I'm liking that specific photo, or making a comment to a third person that does not make sense to the first, right? So, for example, I'm talking to someone and giving an excuse: 'Oh, I can't talk to you now, because I'm busy' then I go in Facebook and make a comment and that person complains: 'Oh, but I noticed that at that time, that day, you were making a comment on a photo'"*.

The resource to which E7 referred was not removed from Facebook, but it has been redesigned and for some users it does not appear, but can be displayed if the user wants it to[7]. Thus, the problem goes on, but now this user and others, who may have had the same impression that the function was taken

[7] See Facebook team's answer on this matter: https://www.facebook.com/help/community/question/?id=607629589247866 (Last visited in May 2015).

down, are not aware of its existence, even though their friends might continue to be able to monitor their actions in real time.

Also in the same direction, E1 (F, 22, nIT) commented on a Facebook feature that allows users to include people in their Close Friends list and then see more of them in her News Feed and get a notification each time they post[8]: *"I found that this exists because my boyfriend included me as his best friend. Everything that I do, he knows, it's outraging! Like, that is very obsessive, isn't it? What do you mean? (laugh) [...] There is a list that he goes into and that contains only the things that I do"*.

Regarding Facebook's discourse about users' activities, E12 (M, 42, IT) reported how it put him in an awkward social situation: *"So, one nice day [...] I open Facebook this way I told you about, quickly, and simultaneously I opened another site, and went to check this other site that was more important to me. Then this guy [...] talked to me in the chat, then when I noticed that Facebook was open, I changed to the Facebook tab and immediately closed it. Then later, this guy, a friend from..., old, sent me this rude message saying that I had been rude with him not having answered the question he had sent to me…"*.

Possibly what happened to E12 was that when he changed to the Facebook tab to close it, Facebook considered that the message was seen, informing the sender that it had been seen by E12. In this case, the notification can be perceived as the system speaking to the sender of the message in behalf of the user who received the message. The sender being informed that his message had been seen, and realizing that it was not answered, felt ignored by the recipient.

Finally, the last type of issue is the misuse of SNSs by their users. Some participants cited as an example of this kind of experience the creation of fake profiles using their name or photo. E2 (M, 28, nIT) shared the following experience: *"[...] I have had fake profiles created with my name, in Facebook and in Twitter. These are two social networks I use very often. I noticed that there was one, there were profiles with the same name as mine. I tried to click and report it, saying that they were trying to pass off as me, but still I don't know if it had the expected result"*. E13 (M, 41, IT) also went through similar experience: *"[...] one person created a profile in Facebook with my picture... another name, etc., but my picture... so [...] someone warned me: 'That guy is using your picture in Facebook with another non-related name,'. So, I sent an e-mail to the 'report'[...] fake profile and I don't know what came of it"*.

Although in this case, people are violating SNSs "terms and conditions" by creating false profiles, users still associate the negative experience to the SNS and to the lack of feedback regarding their report of the abuses.

G. *Common sense is that there is overexposure on SNSs, even though people sometimes do not realize it*

We noticed that the perception that participants have of themselves regarding personal information disclosure is opposed to their perception of other users' information disclosure. Most respondents think that there is an overexposure of people on SNSs, and that it is the consequence of people's lack of concern regarding their privacy in these environments.

The fact that people excessively post the most diverse types of private information in these systems, often without worrying whether such information can be shared with an unexpected or unknown audience, was appointed by the participants as the main evidence of this lack of concern. An example can be seen in E5 (M, 23, nIT) views on the subject: *"[...] they [the people] have lost the limits of things. Social networks have become so important, indispensable to people, that they don't even preserve their feelings, don't preserve their emotions, if now I am feeling bad about something, I go there and disclose it, the person is somewhat racist, he goes there and discloses it, is angry with some politician, goes there and discloses it... Or if they want to meet someone, they post their phone number on the wall, they don't stop to think, it has become very confusing for them to manage their private life and their online life, they understand that it can be disclosed to more people..."*. Another example is when E8 (F, 23, IT) justifies why she thinks that people do not care about privacy on SNSs: *"[...] for example, a lot of people post without even worrying, like, they are invading their own privacy. For example, I have a friend that posted that she had surgery. She posted her picture while at the hospital, many pictures of her baby. So, I think she's losing some of her privacy, right? It's something, like, very personal"*.

In general, participants believe that there is also an involuntary overexposure on SNSs, i.e., people do not expose themselves purposely or are not aware that they are over-exposing their personal information in these environments. One of the main causes of such unintended overexposure, according to half of the participants, is how simple it is to quickly disseminate information in these systems. For example, E1 (F, 22, nIT), talking about overexposure, reflected on her own behavior on Facebook: *"As much as we know that it's for anyone, that anyone can see, sometimes we don't attribute any malevolence to it"*.

However, most of the participants believe that, combined with the individual's nature to act on impulse when exposing information related to his/her personal life on SNSs, these systems have led to a change of people's frames of mind and attitudes towards privacy, leading them to be less concerned about the preservation of their intimacy or privacy of their personal information. E5 (M, 23, nIT), for example, explains why he believes there is an involuntary overexposure of people on SNSs: *"I think that people have lost their senses [...] They don't know anymore, they want a lot of people to like it [...]. It's a notion to reach the world, a sense that you belong to the world, a sense that you are part of a world, when you would only need to share some pieces of information with a smaller group..."*. In this regard, participants also

[8] See more about Close Friends list on: https://www.facebook.com/help/598069963644156 (Last visited in May 2015).

believe that there is an involuntary overexposure, since people are using SNSs to assert themselves socially or outpour their views or concerns. About this topic, E15 (F, 38, IT) said: *"[...] let's consider the teenagers' profile, so, there is already that need for social acceptance, and defining groups or "tribes" they belong to. Given that context, the tendency, I think, is that, due to their psycho-affective development stage, I think the tendency is to an even larger exposure, it's even involuntary"*.

Several participants also cited as causes of this involuntary overexposure people's lack of understanding about privacy settings and how broadly the information they disclose can be disseminated. For example, E8 (F, 23, IT) pointed to Facebook's default settings as a cause of such involuntary overexposure of users: *"[...] if we compare the late Orkut and today's Facebook, its [Facebook's] default settings are much more open than Orkut's. [...] I think that we have become more, like, exposed, especially with Facebook"*. E12 (M, 42, IT) also expressed a similar viewpoint: *"[...] the person does not read the privacy terms, does not know how to change the settings, just wants to create an account, goes in, creates the account, don't know they are exposing themselves that much, right? Often they want to disclose to their group there, but they don't know how to restrict, and end up disclosing without meaning to..."*.

For some participants, the involuntary overexposure of SNSs users could still be due to actions of other users. For instance when they reference or post content that involves other users without their proper consent. E11 (F, 42, IT), highlighted that possibility: *"[...] I may be teaching a class, I said something dumb in the classroom, without meaning to, and in the next second my foolishness is already on Facebook..."*. E12 (M, 42, IT) in the same direction commented: *"[...] This issue... of a person taking a picture, you in that picture, someone else goes there and tags you..."*.

V. DISCUSSION

The resulting categories yielded from the interviews generate information on users' perception about online and offline privacy and information disclosure, strategies adopted, and their experiences in sharing information in SNS. In this section we discuss the relation of these experiences with design decisions and considerations to be taken into account in the (re)design and evaluation of interactions in SNSs and their interfaces.

Our results show that offline sharing levels are reduced to only two levels when transposed to SNSs. Depending on how personal users perceive a piece of information to be, they choose one out of two strategies. In the first, all other users' relations (friends, or even all users) are treated as non-reliable people and the information is not shared in the system. In the second strategy, people at different levels of trust are treated as if they were part of the higher level of trust and the information is posted and everyone, without distinction, has access to it.

In both strategies, users' behavior online is different from how they would behave offline. In each strategy users have to choose what they are willing to give up. In the first one, there could be a loss of interaction opportunities, since users choose not to interact instead of trying to restrict the access to the information to the intended people. The second strategy leads to a greater exposure in the virtual world than users would experience in the physical world, since they share it with a broader group of people than they normally would. A factor to be considered regarding the second strategy is that the audience of the information often is excessively broad, considering that most of the participants accept as friends people they only know by sight, or people they do not even know. In the interviews, one of the reasons participants gave for taking these strategies was because they thought the cost of configuring the privacy settings was not worth the benefits.

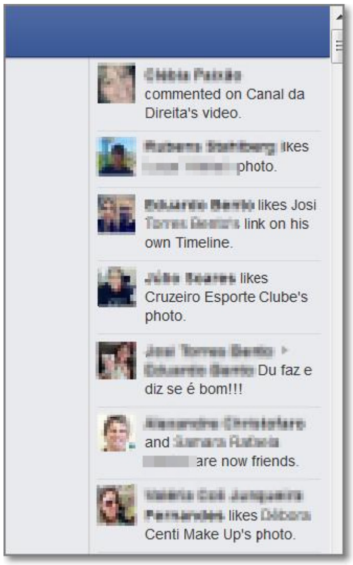
The first strategy in which the user self-censors the content to be sent and decides not to share it, is in line with findings from other researches [8], [10]. However, in these researches other strategies identified were different from the second strategy that emerged in our research. It is worth noting that although both studies were also conducted in academic environments, they both interviewed students from US universities.

The strategies adopted by the users indicate how the high cost to properly configure the privacy settings on Facebook, which represents designers' decisions, may influence their behavior online. In fact, the refusal to use privacy settings, which was reported by participants, leads users to act differently from how they would normally choose to share information or even wish to. This points to the need to consider changes in the privacy settings resources currently offered to users, which is a complex and challenging issue.

However, one could argue that current Facebook design decisions aim at fostering information sharing among its users, since one of the relevant goals of an SNS is information dissemination. On the other hand, reviewing the available models for privacy settings configuration could be of interest, since one of the strategies adopted has been not to post the more personal information at all, which goes against the goals of SNSs.

Furthermore, some negative experiences with privacy in Facebook were directly related to interface design decisions. The prominent feature pointed out by users was Facebook's discourse on behalf of the users. Two instances of this discourse were pointed out as causes to socially awkward situations, resulting in negative experiences for the users. The first one is Facebook´s ticker (see Fig. 1) that shows to users, in real time, their friends' activities. As explained in the help page about ticker[9], users can only see information they would already have access to. Nonetheless, the information is now promptly presented in real time, as opposed to the user having to go look for it. Furthermore, users may choose to hide ticker from their own interface, but they do not have the choice to ask Facebook not to broadcast their activities to others. In other words, they may choose not to "see", but do not have the option to choose "not to be seen".

[9] See: https://www.facebook.com/help/255898821192992/ (Last visited in May 2015).



[redacted] commented on Canal da Direita's video.

[redacted] likes [redacted] photo.

[redacted] likes [redacted] link on his own Timeline.

[redacted] likes Cruzeiro Esporte Clube's photo.

[redacted] ▸ [redacted] Du faz e diz se é bom!!!

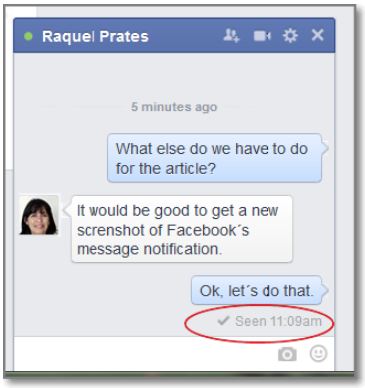
[redacted] and [redacted] are now friends.

[redacted] likes [redacted] Centi Make Up's photo.

Fig. 1. Facebook ticker interface.

The second instance of Facebook's discourse mentioned was the chat or message function. In this function, whenever users send a message to someone else they are informed as soon as the message is seen by the recipient[10], as shown in Fig 2. Once again the recipient of the message has no control whether he/she wants the sender to be notified about him/her having received the message or not.

If on the one hand, the notification provides awareness [48] to the sender, on the other, it may create awkward social situations. It has been argued [49] that mediated communication systems should allow users to engage in situations that may require face-work – that is, managing impressions that other people have of one's behavior, which in some situations may require the user to tell a "white-lie". In this case, Facebook informs user when their message has been received, generating an expectation of a response.



Raquel Prates

5 minutes ago

What else do we have to do for the article?

It would be good to get a new screnshot of Facebook´s message notification.

Ok, let´s do that.

✓ Seen 11:09am

Fig. 2. Facebook chat/message interface notifies user that his/her message has been seen by the recipient.

The problems associated to Facebook's discourse on behalf of the user may suggest that on the users' perspective it might be interesting to provide them with control settings to indicate which of their activities they authorize Facebook to tell other users about. One could ask if adding even more settings would be useful, when many participants mentioned that they thought configuring settings was not worth its cost. However, at least one participant in our research (E7) thought settings to deactivate Facebook's discourse about her activities would be worth the cost and reported looking for a way to do it. Another possible issue could be that such settings would potentially decrease the exchange of information among users, and might not be line with Facebook current strategies to engage users.

The other negative experiences reported by participants are mainly related to actions of other users within the system. Some of these actions are legitimate actions in Facebook, such as posting a picture that includes other people besides the user or tagging[11] other users on photos or posts. The possibility of being able to perform such actions without needing the other's person consent is what sometimes causes the negative experience to someone involved. Posting a picture that includes someone or a comment that mentions another user cannot (currently) be prevented in the technological protocol. Nonetheless, if the user is explicitly referenced (e.g. tagged) then Facebook notifies that person. Users have the option (in the privacy settings) to define that any content that reference them must be reviewed and accepted by them before being posted on their timelines[12]. However, choosing not to post content on their timeline is not the same as not allowing it to be posted. The content may be available to other people, even the user's friends, in the timeline of who has originally posted the content. If users would not want a content to be posted at all, they must negotiate it with the poster(s) of that content. This negotiation must be done through social protocol and is not supported by Facebook's interface. There have been proposals on how to include an interface in Facebook, that could support users' negotiation regarding a photo [50], but such solutions have not yet been adopted by SNSs.

The other problem caused by other users reported in the interviews refers to unauthorized use of Facebook, such as creating fake profiles using users' information. These actions are explicitly prohibited in Facebook terms of use and Facebook offers mechanisms for users to report this kind of abuse[13]. However, once the report is sent to Facebook, the user does not receive any notification regarding any decisions

[10] See: https://www.facebook.com/help/316575021742112 (Last visited in May 2015)

[11] Facebook has the "tag" feature which allows referencing a person's profile in photos or posts.

[12] Timeline review allows users to decide whether content (e.g. posts or pictures) in which they have been tagged will appear in their timelines. The default is that if a friend tags a user that post will automatically go to their timeline, if someone who is not a friend tags the user it will await for the user's review. See: https://www.facebook.com/help/168229546579373 (Last visited in May 2015).

[13] Terms of use available at https://www.facebook.com/legal/terms, and the help page explaining how to report abuse is available at: https://www.facebook.com/help/181495968648557/ (Last visited: May 2015).

or actions taken in response to his/her report[14]. As mentioned by some of the participants of the interview they can only wonder if their complaint resulted in any effects. If social networks provided feedback to users who filed reports about their results, it would possibly increase their feeling of security and even trust on the system.

Users understand that the physical and virtual worlds are interconnected, and for several of them the emergence of SNSs has also increased their offline privacy concerns, given that attitudes and behaviors in the physical world might be disclosed online by other users, without their consent. Thus, even people who choose not to have a profile on an SNS might change their privacy concerns or have their privacy invaded by other users in these systems. In that case, it might be even worse in the sense that it might be harder for the person to detect a problem. Facebook acknowledges the problem by allowing people who do not have an account to report abuse[15].

It is interesting to note that in the interview, participants expressed a different view between their own attitudes towards privacy and the attitudes of others. The majority of the participants said that they take actions to protect their privacy by controlling in some way the disclosure of their personal information. However, when talking about other users, participants believe that, in general, most people do not care about this issue and overexpose themselves on SNSs, by disclosing their intimate and personal information.

It could be that this difference is the result of people's distinct views on the concept of what is considered to be or not personal. However, this difference might be explained by attribution theory – an area in Social Psychology that indicates that the attribution related to themselves is different from that attributed to others, even when the behavior is exactly the same [51]. This theory states that people tend to give themselves credit for their successes and blame the environment for their failures. When it comes to others, they are more likely to attribute their success to the environment and their failures to themselves. In our interview, people seemed to attribute their own negative experiences with privacy to the results of the actions of third parties (Facebook or other users), whereas they believed that others were careless towards protecting their information online.

The results from our interview indicate that, in spite of the various privacy settings available to users, there are still many undesirable situations relating to privacy. Some of them are a consequence of SNS design choices, such as users declining to use the settings due to its perceived high cost, or problems caused by system discourse on behalf of users. On the other hand, others are beyond the control of users and the company responsible for the system, such as when information posted involves more than one user, or users who intentionally misuse SNSs by passing off as someone else. Even though, in some situations, design choices might not be enough to prevent the problems, they could be reviewed to help mitigate them.

Finally, it has been argued that a socio-technical gap [52] is inherent to collaborative systems, i.e. it is not technically possible to implement all nuances, rules and exceptions present in the physical world. As a result, it might never be possible to transpose interactions from offline environments to online environments without losing or changing some of their characteristics. This study has indicated that despite the socio-technical gap, or perhaps because of it, there is a "reflux" from the virtual to the physical world, in which decisions about privacy on SNSs changes and generates impacts in how people behave and interact in the physical world.

VI. FINAL REMARKS

In this study, we presented an exploratory qualitative study based on in-depth interviews aimed at contrasting users' attitudes towards online and offline privacy. Twenty members (between faculty and students) of the academic community of the Federal University of Minas Gerais in Brazil participated in the study. As a result we have identified seven categories that addressed their perception about personal information, their strategies for disclosing information online, the difference perceived in regards to disclosing information online and offline, how these two worlds are interconnected, challenges in managing online privacy and their negative experiences and finally their views on overexposure online. Based on these results we have argued that some of the problems experienced by users are related to interface design choices, such as the system's initiative to disclose information – mainly information about users' activities – on behalf of the users. Other problems might not be an effect of design decisions, such as experiences in which other users violate SNS terms and other users' privacy. Nonetheless, considerations on how the system could better support users in mitigating some of these problems are discussed.

Finally, privacy settings are perceived in general as not being worth their cost to users. Thus, users developed strategies in which depending on the piece of information they choose to share less information with closer relations or more information with distant relations, since these relations are flattened into two categories in Facebook (friends or not friends). Whereas sharing *more* could be in line with some of SNSs' designers intent (which may include broad information sharing), it seems that the information being shared is *less* relevant in terms of how personal they are to users, which might not be perceived as a positive effect by SNSs designers.

These results contribute to the HCI and Collaborative Systems fields, since the users' perceptions and experiences, problems identified, and design considerations can be useful in the (re)design and evaluation of SNSs. This work brings contributions to understanding and reflecting about privacy in SNSs which has been identified by the Brazilian scientific HCI community as being among the great research challenges for HCI from 2012 to 2022 [3][53]. Furthermore, contrasts and interconnections related to privacy online and offline identified in this study point to relevant values to the society

[14] Infographic with the treatment flow of a report: https://www.facebook.com/notes/432670926753695/ (Last visited: May 2015).

[15] See https://www.facebook.com/help/434138713297607/ (Last visited in May 2015).

and could be used as basis for future more in-depth research on the topic in the social sciences.

It is well known that culture influences how people perceive and deal with (online) privacy [6], [38]–[40]. Our study focused on members of an academic community in Minas Gerais in Brazil, and our findings may not be generalizable for users of other cultures, or even from different regions of Brazil. Nonetheless, this study adds to existing culturally bounded studies as important puzzle pieces that can integrate future comparative analysis of different contexts. As presented in the previous section some of our findings resonate results from privacy studies in other cultures, but there are also differences that might be interesting to explore and identify their causes.

In continuation of this research, a questionnaire based on the interview findings was prepared and deployed. Initial quantitative analysis of the data has been performed [47]. Our next steps involve a broader analysis of the data collected with the questionnaire, as well as an analysis of how qualitative and quantitative results complement each other. Finally, given the complexity around privacy settings on SNSs, which causes users decline to use them, we intend to investigate privacy models that can support designers in making design choices related to privacy in these systems. We expect that results from our analyses will inform considerations on such model.

Acknowledgments

Authors thank all the participants of the interview for their valuable collaboration to this research. They also thank FAPEMIG (grant #CEX 10044/11) and CNPq (grant #248441/2013-2) and INCT-Web (INWeb) (MCT/CNPq nº 57.3871/2008-6) for the partial support to this research.

References

[1] D. M. Boyd and N. B. Ellison, “Social Network Sites: Definition, History, and Scholarship,” *Journal of Computer-Mediated Communication*, vol. 13, no. 1, pp. 210–230, Oct. 2007.

[2] A. Acquisti, L. Brandimarte, and G. Loewenstein, “Privacy and human behavior in the age of information. Science,” *Science*, vol. 347, no. 6221, pp. 509–514, 2015.

[3] M. C. C. Baranauskas, C. S. de Souza, and R. Pereira, “I GranDIHC-BR — Grandes Desafios de Pesquisa em Interação Humano-Computador no Brasil,” 2014.

[4] D. Michalopoulos and I. Mavridis, “Surveying Privacy Leaks Through Online Social Network,” in *Informatics (PCI), 2010 14th Panhellenic Conference on*, 2010, pp. 184–187.

[5] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove, “Analyzing facebook privacy settings: user expectations vs. reality,” in *Proc. SIGCOMM 2011*, 2011, pp. 61–70.

[6] G. Rauber and V. A. F. Almeida, “Privacy albeit late,” *Networks*, vol. 13, p. 26, 2011.

[7] R. Gross and A. Acquisti, “Information revelation and privacy in online social networks,” *Proc. WPES 2005*, pp. 71–80, 2005.

[8] J. Vitak and J. Kim, “‘You Can’T Block People Offline’: Examining How Facebook’s Affordances Shape the Disclosure Process,” in *Proc. CSCW ’14*, 2014, pp. 461–474.

[9] E. P. S. S. Baumer, P. Adams, V. D. Khovanskaya, T. C. Liao, M. E. Smith, V. Schwanda Sosik, and K. Williams, “Limiting, Leaving, and (Re)Lapsing: An Exploration of Facebook Non-use Practices and Experiences,” in *Proc. CHI ’13*, 2013, p. 3257.

[10] L. Barkhuus, “The mismeasurement of privacy,” in *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems - CHI ’12*, 2012, p. 367.

[11] D. Rosen, M. A. Stefanone, and D. Lackaff, “Online and Offline Social Networks: Investigating Culturally-Specific Behavior and Satisfaction,” in *Proc. HICSS 2010*, 2010, pp. 1–10.

[12] R. Gross and A. Acquisti, “Information revelation and privacy in online social networks,” *Proc. WPES 2005*, pp. 71–80, 2005.

[13] K. Subrahmanyam, S. M. Reich, N. Waechter, and G. Espinoza, “Online and offline social networks: Use of social networking sites by emerging adults,” *Journal of Applied Developmental Psychology*, vol. 29, no. 6, pp. 420–433, 2008.

[14] A. M. Nicolaci-da-Costa, C. F. Leitão, and D. Romão-Dias, “Como conhecer usuários através do Método de Explicitação do Discurso Subjacente (MEDS),” in *Proceedings of VI Simpósio Brasileiro de Fatores Humanos em Sistemas Computacionais*, 2004, pp. 47–56.

[15] A. F. Westin, “Social and Political Dimensions of Privacy,” *Journal of Social Issues*, vol. 59, no. 2, pp. 431–453, 2003.

[16] J. Holvast, *History of privacy*. Springer, 2009.

[17] J. Cranshaw, E. Toch, J. Hong, A. Kittur, and N. Sadeh, “Bridging the gap between physical location and online social networks,” *Proceedings of the 12th ACM international conference on Ubiquitous computing - Ubicomp ’10*, p. 119, 2010.

[18] R. Grieve, M. Indian, K. Witteveen, G. Anne Tolan, and J. Marrington, “Face-to-face or Facebook: Can social connectedness be derived online?,” *Computers in Human Behavior*, vol. 29, no. 3, pp. 604–609, May 2013.

[19] R. Gross and A. Acquisti, “Information Revelation and Privacy in Online Social Networks,” in *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, 2005, pp. 71–80.

[20] M. Nguyen, Y. S. Bin, and A. Campbell, “Comparing online and offline self-disclosure: a systematic review.,” *Cyberpsychology, behavior and social networking*, vol. 15, no. 2, pp. 103–11, Feb. 2012.

[21] L. Emanuel, G. J. Neil, C. Bevan, D. S. Fraser, S. V. Stevenage, M. T. Whitty, and S. Jamison-Powell, “Who am I? Representing the self offline and in different online contexts,” *Computers in Human Behavior*, vol. 41, pp. 146–152, 2014.

[22] S. Waters and J. Ackerman, “Exploring Privacy Management on Facebook: Motivations and Perceived Consequences of Voluntary Disclosure,” *Journal of Computer-Mediated Communication*, vol. 17, no. 1, pp. 101–115, 2011.

[23] J. H. Choi, “Living in Cyworld: Contextualising Cy-Ties in South Korea,” *Uses of blogs*, pp. 173–186, 2006.

[24] A. Lenhart and M. Madden, *Teens, privacy & online social networks: How teens manage their online identities and personal information in the age of MySpace*. Pew Internet & American Life Project, 2007.

[25] C. Lampe, N. Ellison, and C. Steinfield, “A Face(Book) in the Crowd: Social Searching vs. Social Browsing,” in *Proceedings of the 2006 20th Anniversary Conference on Computer Supported Cooperative Work*, 2006, pp. 167–170.

[26] A. N. Joinson, “Looking at, Looking Up or Keeping Up with People?: Motives and Use of Facebook,” in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2008, pp. 1027–1036.

[27] B. Krishnamurthy and C. E. Wills, “Characterizing Privacy in Online Social Networks,” in *Proceedings of the First Workshop on Online Social Networks*, 2008, pp. 37–42.

[28] M. Pereira Junior, S. Xavier, and R. O. Prates, “Antecipando Possíveis Implicações De Privacidade Na Postagem De Fotos No Facebook,” in *Proceedings of the 12th Brazilian Symposium on Human Factors in Computing Systems*, 2013, pp. 62–71.

[29] F. Bergmann and M. Silveira, “Eu vi o que você fez... e eu sei quem você é!: uma análise sobre privacidade no facebook do ponto de vista dos usuários,” *Proc. IHC'12*, pp. 109–118, 2012.

[30] M. Pereira Junior, S. Xavier, and R. O. Prates, “Investigating the use of a Simulator to Support Users in Anticipating Impact of Privacy Settings in Facebook,” in *Proceedings of the 18th ACM International Conference on Supporting Group Work*, 2014.

[31] E. P. S. Baumer, P. Adams, V. D. Khovanskaya, T. C. Liao, M. E. Smith, V. Schwanda Sosik, and K. Williams, “Limiting, Leaving, and (Re)Lapsing: An Exploration of Facebook Non-use Practices and Experiences,” in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2013, pp. 3257–3266.

[32] K. Lewis, J. Kaufman, and N. Christakis, “The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network,” *Journal of Computer-Mediated Communication*, vol. 14, no. 1, pp. 79–100, Oct. 2008.

[33] D. Boyd and E. Hargittai, “Facebook privacy settings: Who cares?,” *First Monday*, vol. 15, no. 8, 2010.

[34] B. Debatin, J. P. Lovejoy, A.-K. Horn, and B. N. Hughes, “Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences,” *Journal of Computer-Mediated Communication*, vol. 15, no. 1, pp. 83–108, Oct. 2009.

[35] F. Stutzman and J. Kramer-Duffield, “Friends Only: Examining a Privacy-enhancing Behavior in Facebook,” in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2010, pp. 1553–1562.

[36] J. Fogel and E. Nehmad, “Internet social network communities: Risk taking, trust, and privacy concerns,” *Computers in Human Behavior*, vol. 25, no. 1, pp. 153–160, Jan. 2009.

[37] R. Dey, Z. Jelveh, and K. Ross, “Facebook users have become much more private: A large-scale study,” in *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on*, 2012, pp. 346–352.

[38] H. Krasnova and N. F. Veltri, “Privacy calculus on social networking sites: Explorative evidence from Germany and USA,” in *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*, 2010, pp. 1–10.

[39] H. K. Tsoi and L. Chen, “From Privacy Concern to Uses of Social Network Sites: A Cultural Comparison via User Survey,” in *2011 IEEE Third Int'l Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third Int'l Conference on Social Computing*, 2011, pp. 457–464.

[40] Y. Wang, G. Norice, and L. Cranor, “Who is concerned about what? A study of American, Chinese and Indian users' privacy concerns on social network sites,” *Trust and trustworthy computing*, pp. 146–153, 2011.

[41] J. Staddon, D. Huffaker, L. Brown, and A. Sedley, “Are privacy concerns a turn-off?: engagement and privacy in social networks,” *Proc. SOUPS '12*, pp. 10:1–10:13, 2012.

[42] S. Kisilevich, C. S. Ang, and M. Last, “Large-scale analysis of self-disclosure patterns among online social networks users: a Russian context,” *Knowledge and Information Systems*, vol. 32, no. 3, pp. 609–628, Sep. 2011.

[43] C. M. de A. Barbosa, R. O. Prates, C. S. de Souza, and A. M. Nicolaci-da-Costa, “Using the underlying discourse unveiling method to understand organizations of social volunteers,” in *Proceedings of IHC2002 - V Workshop de Fatores Humanos em Sistemas Computacionais*, 2002.

[44] C. S. de Souza, A. M. Nicolaci-da-Costa, E. J. da Silva, and R. O. Prates, “Compulsory institutionalization: investigating the paradox of computer-supported informal social processes,” *Interacting with Computers*, vol. 16, no. 4, pp. 635–656, Aug. 2004.

[45] H. J. Smith, T. Dinev, and H. Xu, “Information privacy research: an interdisciplinary review,” *MIS Quarterly*, vol. 35, no. 4, pp. 989–1016, Dec. 2011.

[46] R. Turn, “Classification of personal information for privacy protection purposes,” in *Proc. NSATC 1976*, 1976, pp. 301–307.

[47] M. L. B. Villela, S. Xavier, R. O. Prates, M. O. Prates, F. M. Shipman, and A. A. Prates, “Investigating Brazilian and American Users' Perceptions of Content ‘Personalness’ and the Impact on their Attitudes towards Information Sharing. Technical report: RT.DCC.001/2015 - DCC-UFMG.,” 2015.

[48] P. Dourish and V. Bellotti, “Awareness and Coordination in Shared Workspaces,” *Proc. Intl. Conf. on Computer-Supported Cooperative Work*, no. November, pp. 107–114, 1992.

[49] P. M. Aoki and A. Woodruff, “Making Space for Stories: Ambiguity in the Design of Personal Communication Systems,” in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2005, pp. 181–190.

[50] A. Besmer and H. R. Lipford, “Moving beyond untagging: photo privacy in a tagged world,” *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 1563–1572, 2010.

[51] E. E. Jones and K. E. Davis, “From acts to dispositions the attribution process in person perception,” *Advances in experimental social psychology*, vol. 2, pp. 219–266, 1965.

[52] M. Ackerman, “The Intellectual Challenge of CSCW: The Gap Between Social Requirements and Technical Feasibility,” *Human-Computer Interaction*, vol. 15, no. 2, pp. 179–203, Sep. 2000.

[53] M. C. C. Baranauskas, C. S. de Souza, and R. Pereira, “GranDIHC-BR: prospecção de grandes desafios de pesquisa em interação humano-computador no Brasil,” in *Companion Proceedings of the 11th Brazilian Symposium on Human Factors in Computing Systems*, 2012, pp. 63–64.