LIVING IN THE DIGITAL AGE

SELF-PRESENTATION, NETWORKING, PLAYING, AND PARTICIPATING IN POLITICS

**Pascaline Lorentz, David Smahel,
Monika Metykova, Michelle F. Wright (Eds.)**

Masarykova univerzita

Brno 2015

european social fund in the czech republic

EUROPEAN UNION

MINISTRY OF EDUCATION,
YOUTH AND SPORTS

OP Education
for Competitivness

UNIVERSITAS MASARYKIANA BRUNENSIS

INVESTMENTS IN EDUCATION DEVELOPMENT

This publication was supported by the project Assembling an Interdisciplinary Team for the Research of Internet and New Media (VITOVIN CZ.1.07/2.3.00/20.0184), which is co-financed by the European Social Fund and the state budget of the Czech Republic.

Reviewers:

Dr. Christopher Barlett

Dr. Zaheer Hussain

Dr. Pablo Vicente Sapag Muñoz de la Peña

Dr. Kaveri Subrahmanyam

ISBN 978-80-210-7810-9

ISBN 978-80-210-7811-6 (online : pdf)

Children’s Privacy Management on Social Network Sites

Hana Machackova, Martina Cernikova, David Smahel, Zuzana Ocadlikova

ABSTRACT

The chapter examines the management of online privacy on Social Network Sites (SNS) among children and adolescents. Petronio’s Communication Privacy Management Theory (CPM) was selected as the primary theoretical framework for capturing the process of privacy management and boyd’s features and dynamics of networked publics were used to depict the specific affordances of the SNS environment. Using qualitative cross-national data from European children aged 9–16 from the EU Kids Online III project, the chapter illustrates how current children manage their privacy on SNS and show in which aspects this process has become problematized. Using the CPM framework, several components of children’s privacy management on SNS are described: The perception of the ownership (and loss thereof) of private information; different types of control over the published information and the online audience; the rules which guide the control and overall online behavior, including the co-ownership of private information; and the boundary turbulences that lead to the co-construction of privacy rules and boundaries on SNS.

Keywords

online privacy, communication privacy management theory, social network sites, children and adolescents

INTRODUCTION

In last decade, Social Network Sites (SNS) have become important venues for our social lives. Their use is connected with a number of opportunities for forming and sustaining relationships (Livingstone & Brake, 2010), processes which inevitably involve some degree of disclosures (Derlega & Chaikin, 1977). But information disclosed on SNS is persistent, can be easily accessed, spread, and replicated (boyd, 2010). This is why disclosures on SNS may result in a negative experience and even harm if published information and materials are in some way misused. Therefore, many SNS users protect their privacy by balancing between disclosures and concealments, striving for the most positive outcomes but, at the same time, fearing potential risks.

In this chapter, we focus on children and adolescents, who enjoy SNS for their affordances but for whom they also pose a challenge in terms of privacy. Despite the fact that youth seem to be savvy media users, they still develop cognitive, social, and digital skills needed to sustain optimal levels of online privacy. Although a number of studies have focused on privacy online (i.e., Trepte & Reinecke, 2011), we still lack sufficient knowledge about the experiences of contemporary children and adolescents. We need to understand how they manage their privacy on SNS and how they perceive the specifics of the online environment in this context.

Our aim is, therefore, to capture how youth balance their disclosures and manage privacy boundaries on SNS. To achieve this goal, we will utilize existing knowledge about the specifics of SNS environment (boyd, 2010) and Petronio's Communication Privacy Management Theory (2002; 2010), which offers a useful framework to capture privacy management on SNS (Child & Petronio, 2011). Using data from interviews with European children aged 9–16 in the cross-national project EU Kids Online III (Smahel & Wright, 2014), we will illustrate how contemporary children manage their privacy on SNS and how they avoid possible risks connected to privacy violations.

SPECIFICS OF THE SNS ENVIRONMENT

In past years privacy management has become problematized. People have been lamenting the loss of privacy as well as the unregulated disclosures of private information and materials online (Solove, 2007). The task of keeping privacy online can be more difficult, considering how easily personal information can be published, accessed, and distributed. As privacy management differs across different online locations and platforms, we focus exclusively on the use of social network sites, which currently belong among youth's predominant online activity (Livingstone & Brake, 2010). SNS are designed to motivate users to publish and share information and materials which can have various forms: text, photos, videos, or links to other web sites.

The particularities of the SNS environment as "networked publics" have been described by boyd (2010). As she pointed out, SNS have structural affordances which "do not dictate participants' behavior, but they do configure the environment in a way that shapes participants' engagement" (p. 309). Four specific features typical for the SNS environment belong among these affordances. *Persistence* refers to the fact that, once published online, information can be stored for a very long time, especially when circulated among a wide audience. *Replicability* indicates that the information and materials posted online can be easily duplicated. This means that they can be very quickly and easily spread and/or stored by another party. Moreover, they can also be altered and, in the end, the true source (and original form) can be nearly unrecognizable. *Scalability* describes that the online information is potentially widely visible. It does not mean that the information is actually accessed and seen by a wide audience; it means that the potential exists. *Searchability* is closely connected to scalability. While online, the information can be reached using search engines (or other tools). Thus, even though the owner of the information (or even the whole profile) does not intend to make the information accessible for other parties, it still might be reachable. It is noteworthy that the extent to which these features are applicable differs across different SNS sites. For example, while some SNS might limit scalability via technical setting, others do not have such an option. But, since we focus on the whole spectrum of different SNS with a wide range of technical possibilities, we focus on all of these features.

These features introduce the three basic dynamics of networked publics. An *invisible audience* emphasizes that, although audience knowledge is crucial for assessing the context of communicating information, the audience on SNS can remain invisible. Further, *collapsed contexts* depicts how different social groups often merge into one audience. When posting on SNS, users can divide their audience into separate groups, or clearly target the information to a single group of people. But, despite these attempts and due to the invisibility of audience, the user is often unaware of all the people in the audience and the fact that information is gathered (and interpreted) by people from different contexts (e.g., classmates, a football team, and parents). In result, because of the audience's invisibility and context collapse, SNS users cannot always sufficiently assess the social context of their disclosures, foresee their consequences, and overall adequately manage privacy boundaries. The last dynamic describes the *blurring of private and public*. In this chapter, we take this last dynamic as the starting point for our examination.

COMMUNICATION PRIVACY MANAGEMENT THEORY

Concerns about privacy and disclosure online have been especially emphasized in relation to children's and teen's use of the internet, particularly the use of social network sites (Livingstone & Brake, 2010). But while the interest in privacy on the internet is something rather new, the interest in privacy per se has a long history. There are various conceptualizations of privacy. For example, Westin (1968) conceived privacy as the "claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (p. 7). Altman (1975) approached privacy as a temporal dynamic process for the regulation of interpersonal boundaries, "the selective control of access to the self" (p. 24).

Recently, a lot of attention was given to the work of Sandra Petronio (2002, 2010) and her Communication Privacy Management Theory (CPM). CPM has been successfully employed in the family context (Petronio, 2010), but it is also considered extremely valuable for understanding privacy in computer-mediated communication (Child & Petronio, 2011). Petronio views privacy and disclosure (i.e., sharing personal information and feelings which stimulate the development of relationships) as mutually and inevitably interconnected in dialectical tension. Throughout their lives, people keep balancing between disclosing and concealing, taking into account cultural, gendered and motivational factors, perceived risks and benefits, and the overall context. Altogether, these factors are situated within specific contexts and influence the process of privacy management. Central to this process is a metaphor of boundaries, which may range from complete openness to being completely closed-off (i.e., secrets), reflecting varying degrees of willingness to share private information.

CPM is based on five core principles:

1. People perceive the private information as something that belongs to them: they **own the information**. The ownership of private information is based on one's beliefs and feelings, and also includes the prerogative to manage the information according to their wishes.
2. Hand in hand with the first principle goes the second: when people perceive they own the information, they also assume their right to **control the privacy boundaries** (i.e., they control who has access to the information). The level of control varies with regard to the kind of information and/or context (e.g., high control would appear when one does not wish to share information with anyone or only with a very limited circle of their nearest friends or family and sometimes just one person).
3. When managing the private information, people depend on **rules to control the information flow**. Privacy rules and regulations guide the possibilities of spreading someone's private information to other people. These rules depend on many factors, from cultural values to specific situations and can be explicit as well as implicit.

4. When information is shared, it is in a sense also **co-owned** with the information recipient. The recipient of private information is expected to follow (preferably, negotiated) rules about privacy boundaries (and, therefore, the process of sharing disclosed information). *Linkage rules* determine who else can be included within one's privacy boundary (and know about the disclosed information), *permeability rules* define how much is actually shared with others, and *ownership rules* depict the extent to which recipients themselves control the information.
5. Privacy management is a dynamic, interpersonally dependent concept, and, as such, privacy rules are constantly negotiated and adapted. Each person can have a different definition of privacy rules and boundaries, and, therefore, when not effectively negotiated, each relationship has the potential for privacy boundary conflicts. **Privacy boundary turbulence** denote such misunderstandings, (un)intentional rules violations, or privacy intrusions, which happen more or less often in interpersonal relationships.

CPM operates not only with the privacy regulation on an individual level, but also with permitted access to the information of others. CPM, thus, allows for the investigation of the flow of private information between and among people in order to understand privacy management on multiple levels (i.e., individuals, dyads, and groups) that occur in many different contexts, including online social media (Child, Haridakis, & Petronio, 2012).

PRIVACY MANAGEMENT ON SNS AMONG EUROPEAN CHILDREN

The aim of this chapter is to describe the specifics of privacy management on SNS among children from their perspectives. To achieve this goal, we adapt the five core principles of CPM (i.e., ownership, control, rules, co-ownership, and turbulence), and we explain their specifics of SNS usage in light of the features and dynamics of networked publics: *persistence, replicability, scalability, searchability, invisible audiences*, and *collapsed contexts* (boyd, 2010). Structurally, this sub-chapter will individually address each of Petronio's five principles and illustrate the moments in which privacy management differs due to the character of the SNS environment. This depiction will be grounded in empirical evidence from the project EU Kids Online III. Details about the project and its methodology are described in an available online report (Smahel & Wright, 2014). In this project, children between the ages 9–16 in nine European countries[10] were asked about their online experiences. Within

[10] Belgium, the Czech Republic, Greece, Italy, Malta, Portugal, Romania, Spain, and the United Kingdom.

interviews and focus groups[11] primarily focused on problematic experiences with Information and Communication Technology (ICT) use, children depicted how they perceive, assess, and manage their privacy on SNS. With these data, we will illustrate the specifics of privacy management in the SNS environment as perceived by European children.

Private Information Ownership

The ownership of information – in other words, the declaration and perception of information as something that belongs to oneself – is an essential parameter of privacy (Petronio, 2002; 2010). But when the information is posted on SNS, due to the *replicability* and *scalability* of the information, the (sense of) ownership is challenged. The user can feel that the information is no longer just his or her because the posted information is persistent and "always online". Moreover, others can search and then also replicate the information. As an Italian boy (11–13 years old) said: "*…if someone posts a personal photo on his profile, someone can copy it and everyone can see it*". Such conditions can erode the perception of the ownership of information by individual users, who can ask themselves: Is information which I post on SNS still (only) mine? Some of the children in our research voiced such concerns and reflected perceived *persistence* and *scalability*. A Romanian girl (11–13) said: "*Well...everyone could access it and write something or just to see what you're up to, what pictures you're posting, where you are....*" For some children, this loss of ownership was accompanied by negative feelings; for others, it was a necessary trade-off between the loss of privacy and the social benefits provided by SNS. Still, despite these concerns, many children persisted in their right to be the owner of the information they disclosed. As they described, it is still they who own their information (also in the form of pictures and videos) and they who, therefore, have the right to control it.

Private Information Control

The perception of ownership is, therefore, closely related to the control of the information: while ownership underlies the control, a lack of control can disrupt that sense of ownership. The control over information published on SNS is a very complex task, and children often mentioned how the loss of control limits and shapes their use of SNS. They depicted how control can be problematized due to the *persistence* of posted information, which they often perceived as something irreversible: "*Girl1: As they say: once online, forever online… Girl4: It's almost like tattoos: we have to think if that's what we really*

[11] In focus groups, only age range (e.g. 9–11) was recorded; therefore, in some quotations specific age is not presented.

want… Girl3: Or else it will be there for life!" (Portugal, girls, 15). Sometimes, this was connected to the feelings of helplessness, as control was completely lost. "*…all the things you disclosed about yourself stay on Ask, even if you delete your profile.*"*(*Italy, girl, 11–13). Of course, this did not apply for all children – many debated possible ways to make (at least some) information disappear. The negative consequences of losing control were also articulated with regard to *scalability* and *replicability*, which represented the potential for the misuse of information. In the words of a 14-year-old Greek girl: "*…it's just that you don't know what anyone can do with your photos … cause you hear many things, that they take [other people's] photos and edit them and stuff … Once, a friend of mine told me that she had a photo and they made her look naked, poor girl!*" Finally, the *searchability* of information can also become an issue. Some children discussed how public profiles allow others to find their posts, and some even feared that people could find them and track them. " *… also the school can track your Twitter and Facebook accounts … Because if they wanted to search me they just type in my name, because my name's on Twitter it will come up with me and they could look through what I'm saying and stuff because they've done it before in other schools.*" (UK, boy, 14–16). It is important to say that all these features are not seen only negatively. For example, *scalability* was also seen as an advantage, such as the possibility to quickly and rather effortlessly reach beyond the nearest social circles and share experiences with a larger crowd of friends and acquaintances. All these features and specifics of the online environment influence how children perceive the possibilities and limits of control over privacy boundaries and disclosed information, which in turn influences how they behave online.

But despite these specifics of the online environment, SNS users can exert different types of control upon their privacy and upon our data. We distinguished the following three levels of control.

1) The first level is the basic decision for a child to use SNS. Some children refuse to even create a SNS account because they perceive it as an environment where others can search, see, and reach their (persistent) information, and where they lose all control over their information. As an Italian girl (9–10) said: "*I don't want to trust Facebook because I don't like it very much …my brother has it, but my mum always tells him not to use his own picture because you can never know who it may reach... so I don't want it...*"
2) On the second level of control, children agree to have an SNS account, but they do not post any (or hardly any) information. As mentioned

by a Spanish boy (14–16): *"On the only social networking site that I use, which is Twitter, I have never tweeted anything."* In this case, children use SNS in a rather passive way, enjoying some of the benefits, but at the same time significantly constraining their own activities. Such extreme control seemed to be most prevalent among younger children, who had not yet developed sufficient skills to master the third level of control.

3) On the third level, the SNS users make more complex decisions about publishing their personal information and the management of online boundaries. Specifically, they consider the character of information, the audience, and the overall context. They ask: What kind of information would I like to post? Under which condition would I like to post the information? And with whom would I like to share it? Thus, on this third level, SNS users also think about whether to publish information, but they also make more subtle decisions. "*I am careful, because I am aware that what you post on the internet stays there forever. So I try to be as careful as I can, with pictures I post, with people I add, with people I let see my posts!*" (Portugal, girl, 14–16).

These kinds of decisions on the third level can also include technical control over information on SNS, with the help of "privacy settings" – some children create groups of users (i.e., family, school, best friends) and then decide which piece of information they share with specific groups. In this way, children manage their online audience and, with regard to the possible *scalability* and *replicability*, children delineate clear boundaries for who can access (and potentially co-own) their information. But the possibility for such technical control over information also depends on digital literacy, and not all children are aware that there are such options on SNS.

According to our research, children differ substantially in their need to keep control of their privacy. Some children reported that they "open" their boundaries when they decide to open their whole SNS profile by sharing their passwords with other children, in most cases with significant and trustworthy others. These children usually emphasized the benefits of such a decision. For example, younger children who shared passwords with parents, appreciated that the parents helped them maintain their profiles and, in the end, increased their control over their privacy. For older children, disclosing passwords to peers was seen as part of trustable relationships, as well as an easy way to mutually "keep tabs" on what is going on in their private lives. "*I actually gave her my password and she gave hers to me.… I will call her, hey look at my chat with someone…*" (Czech Republic, girl, 14–16). But in many cases, sharing a profile was seen as "too much", and children kept them secret even from their closest relations and friends in order to keep control of their private spaces. As Spanish girl (14–16) said: *"My passwords are mine. I've never talked to a boyfriend about that."*

Besides sharing whole profiles, children also often make more nuanced decisions related to the different types of disclosed information, differentiating among distinct types of audiences. "*For example when there is something that only your friend may know, I think that the people who are not friends with you on FB don't have any business with that.*" (Belgium, girl, 11–13). Many children limited their audience, relying on mutual trust, and sharing personal information with just a narrow circle of friends, modifying *scalability* according to their individual needs. *"For example you post one thing for 'public' and another thing for 'only friends'. But on my profile I only post things for my friends, those I know really well. Those people I trust, so the others I put them in the list of 'acquaintances'"* (Belgium, boy, 15). Still, some children did not make such nuanced distinctions and relied on the fact that their posts are not actually too personal and not connected to any risk.

But despite these strategies, children still voiced fears over the loss of control due to others who can access the information on SNS. For example, children perceived danger linked with "hackers", who can hack their profiles and get their personal information, such as mobile number or email address. They even reflected that they can use this information to replicate a profile, as described by a Romanian girl (9–10): *"Let's say that when you go on Facebook, there are cases, it's happened a lot of times, when hackers, that's what they're called, look at your Facebook account and access your page if...you don't really figure out what's going on. It's a page, where you post your pictures, status updates in which you write what you've been up to. So hackers take your email and phone number and they have a special software, like that, which they access and create a Facebook account, with exactly the same name and pictures and the exact same phone number and stuff like that."* Some children also decided to control their privacy by staying anonymous on SNS, such as by using false name.

We can see that although children are aware of the principles of *persistence*, *replicability*, *scalability*, and *searchability*, they control their privacy on SNS by various creative ways.

Private Information Rules

Children in our research differed largely in their individual perceptions about what is appropriate and comfortable to publish on SNS. Children have developed rules guiding their individual online behavior, which were based on general privacy management rules but also on the awareness of the specifics of this online environment. These rules guide the management of the audience and the decisions about disclosing the content.

Regarding the audience, we can distinguish the two basic aspects of the rules: (1) the management of the audience and its access to information; and (2) rules for the audience and how it should behave with respect to children's privacy.

Ad (1) The first aspect describes the rules in relation to *scalability* (as a visibility), *searchability*, and *replicability*. Children created rules about others to decide who their "friends" are on SNS, who can see their profiles, who can see their statuses, who has access to their private information, and who is trusted not to misuse (e.g., replicate) it. These rules were related to their offline environment and the control over boundaries on SNS was usually interconnected with the control over offline boundaries.

For example, while offline friends were cordially invited within their private online spaces, with increasing age, parents were less and less welcome. This is analogous to the adolescents' growing need to guard boundaries against parental intrusions in the offline environment. In the words of an English girl (14–16): *"First rule of Facebook, I got told by everyone, was, never add your parents as your friends, because then they'll see everything you're up to."* Besides their offline experiences, children also base these rules on the general awareness of potential risks, such as "online stranger danger". As a Belgian boy (11–13) said: *"When people ask me where I live and how old I am, then I know enough, and I won't add them anyway. Then I call my dad, and if they would continue like that, my dad would call the police."*

Ad (2) The second set of rules defines what is (in)appropriate in the behavior of others. Children develop specific perceptions of what is right and wrong as they ask: Who should add photos with me? Who should share my photos and/or tag me? These questions are reflected in the co-ownership rules described below.

The rules do no concern audience management only, but they are also related to the contents of the disclosures. There is information which is perceived as "benign", for which the perceived *replicability* or *scalability,* and now also *persistence,* is not an issue. Such benign information is seen as harmless, even if it is shared with the wider public or stored for many years into the future.

But a lot of information, most notably one's photos, are assessed as sensitive. Their publication by users or others is seen as inappropriate, because they are widely reachable and can be stored for a long time and, therefore, possibly misused. As pointed out by a Belgian boy (14–16):*"Especially sending such (sexy) pictures on the internet that is just stupid. Eventually people will find out about it…especially when it's sent to a boy."* Such information is often subjected to rules which state whether they can even be published, and, if yes, who can get access to them.

In the end, rules about these two aspects – audience management and publishing different contents – are interconnected and function together. For example, some children allow their best friends to post photos with them as pointed out by an Italian girl (9–10): *"This friend of mine who one day on Facebook posted a picture of the two of us together when we were skiing, but I was fine with it because he had also written 'my best friend and I'."* But if such photos would have been published by someone else, for example, a more distant acquaintance, it could be perceived as breaking the implicit privacy rule.

Private Information Co-Ownership

As mentioned, there are specific rules connected to the behavior of those to whom children disclose – the co-owners of the information. Children reported the development of specific expectations for how others should treat their disclosed and shared information. Children often expected that their information be understood as more or less private and not permeable to other users or even the wider public. But children also know that these rules can easily be broken, and due to *replicability*, even very complex information (e.g., a whole chat conversation or an SNS profile) could potentially be shared with a wider audience. Specifically, the co-ownership of an SNS profile is a very sensitive issue and is tightly connected to the child's offline relationships – and, conversely, trust in the offline world is closely connected to trust in the online environment. *"No…I wouldn't exchange [a password] with just anyone I mean only with my best friend, whom I've known for seven years and I trust her. I mean I don't just give out my password to anyone." (Romania, girl, 16)*. Although children sometimes share access to their profile on SNS, it is usually with the belief that others will not misuse this trust, and sometimes even with the implicit expectations that others will not actually do anything within their profile.

But co-ownership rules are not only related to the private space demarcated by the whole SNS profile. These rules are expected to also apply to the general behavior of others within the online social network(s). A lot of information is actually co-owned in offline spaces, or via explicitly private channels: children take group pictures with their friends, they share rumors or experiences in class, they email each other videos, etc. The treatment of this information by others in the SNS environment is also subjected to the rules of co-ownership. Some children have very strict preferences that they explicitly articulate to others. "*Sometimes, there were people who uploaded pictures of me that I didn't like and I asked to remove them or something. If they didn't, I could report the situation. I sent the person a message, because there was that option, and she removed it…For instance, when I take pictures with my friends, we have a deal: no one uploads anything before we all decide what we are going to upload." (Portugal, girl, 14–16)*. In their social circles, children develop common rules for what is right and wrong in terms of co-ownership. These rules vary, but usually they reflect the possibilities of misuse of information due to their *scalability* and *replicability*.

Private Information Boundary Turbulence

Turbulence grounded in negative experiences on SNS serve as powerful incentives which influence changes in children's management of privacy. Considering that SNS profiles are strongly connected to offline life, the misuse of information can result in severe harm. For example, the cases of stolen online identity, in which children's profiles were hacked and abused, were described as very harmful.

Children described many incidents in which the disclosed information or even a whole private space (i.e., profile) were misused. Some of them talked about their own experiences, which increased their need for control. In a rather extreme case described by a Czech girl (12), the negative experience led her to abandon SNS usage: *"I don't have Facebook anymore, because I was cyberbullied there. I definitely learned something from what happened with Facebook. And I don't really want to make an account now."* Other children mentioned the experiences of others, be it their friends, acquaintances, or unknown people, whose negative experiences circulate as stories depicting the misuses of information published on SNS. After hearing such stories, some children changed their own rules and behavior on SNS to prevent such misconduct from happening to them.

Turbulence emerges upon complications in co-ownership, when a co-owner fails to act upon expected rules which can be expressed explicitly, but sometimes only on an implicit level. But the agreement upon a set of rules can be complicated on SNS, where the *audience* is often *invisible* and consists of different groups (i.e., *context collapses*). The invisible audience is connected to the fears of possible misuse, mainly by unknown others, "online strangers", or hackers. The assessment of what is still private also differs across different social groups in the audience. While in one social group the publishing (and the replicating) of a more sensitive photo might be seen as acceptable; in another, this is perceived as highly inappropriate.

These differences might be in the perception of ownership. Some children understood *scalable* and *replicable* information not as private and owned by the user, but as public and, therefore, as information which might be misused. In some cases, children blamed the victim because he or she "should have realized" that misuse happens on the public SNS. Similarly, victims of privacy violations were blamed if they were not efficient in the control of information. But it should be noted that although there is a variety of choices enabling different levels of control over the access to information, most notably the SNS's explicit privacy settings, these require certain digital skills, which are still developing, especially among children (Sonck, Livingstone, Kuiper, & De Haan, 2011).

Thus, the differences of assessment differ across contexts. But considering the *persistence* of information, the context is changing with children's development, as well as their perception of privacy and attitudes to disclosed materials, which may as well result in turbulence. What users perceive as benign at a younger age might be seen as less appropriate later – yet the same information is still available. Moreover, as the information stays published, it can be reached after some time, in another place, and in a different context. "*She sent a naked picture to her boyfriend. And she told us her Facebook password at the party that was going on at the moment in my house. And some of my friends went to her Facebook profile a few months later, and there they found out about this picture. And then the girl was bullied*" (Belgium, girl, 14–16).

CONCLUSION

The aim of this chapter was to depict how children's privacy management is shaped by the "networked public" environment on SNS. Based on the opinions and experiences of European children, we pointed out how the specific aspects (*persistence, replicability, scalability, searchability, invisible audiences*, and *collapsed contexts;* boyd, 2010) intervene in the process of privacy management on SNS.

Our findings challenge the still-prevailing notion that children do not know or care about their privacy and disclosures on SNS. The awareness of the potentially risky features of the SNS environment was embedded in children's online praxes. The simplicity of publishing information and materials online and the ease by which they can potentially be misused by a wide audience created many situations where children had to think about what they wanted to disclose.

In the SNS environment, children often perceived the possible loss of the ownership of (otherwise private) information. Considering the features and dynamics typical for the SNS environment, they managed their privacy by applying different types of control over the published information and the online audience. The control ranged from the complete refusal to post any private information to the development of nuanced strategies of audience and information management. The control exerted over their own privacy boundaries was grounded in specific sets of rules. Since SNS are a platform through which children sustain existing relationships and which copies their offline circles (Livingstone & Brake, 2010), online privacy management also copied this offline process. For example, those who are trusted offline (e.g., best friends) were also trusted with private information online. On the other hand, it is the potential of SNS to reach beyond normal offline circles and, in a sense, to be very close and open also with "mere" acquaintances and more or less unknown people, which problematizes this process. Moreover, the rules set for the audience and published content differ dramatically among children, depending on their individual preferences and experiences, developmental stage, and digital skills. Inter-individual differences underlie privacy boundary turbulence. When their borders were crossed, children had to change their behavior and/or set different privacy settings. In this way, the privacy rules and boundaries are co-constructed in a continuous process of decision making about children's privacy.

Our chapter offered a deeper insight into the everyday experiences of contemporary youth and the strategies by which they manage their online privacy and prevent the negative outcomes of privacy violations. But it is necessary to stress that there is a huge variety of approaches toward online privacy among children. We saw that, despite the fact that children often know about the specifics of the online environment, they react very differently. Our research helped to get a closer look at this variety of perspectives and behaviors. But, we also recommend to further pursue this topic and examine how all these variables moderate children's privacy rules and boundary management.

What is also important to mention is the fact that, for most children, SNS represent a "natural" environment through and on which they interact. It is understandable that they were prone to open privacy boundaries and, at least to some extent, to profit from the affordances of SNS. What is inevitably inherent to SNS use are the benefits of all the features and dynamics. These were not specifically articulated in our study, which was mostly focused on the problematic aspect of ICT use. To better understand the benefits of opening one's privacy boundaries would help us to better understand the whole process and the outcomes of privacy management on SNS.

ACKNOWLEDGMENT

The authors acknowledge the support of the VITOVIN project (CZ.1.07/2.3.00/20.0184), which is co-financed by the European Social Fund and the state budget of Czech Republic.

REFERENCES

Altman, I. (1975). *The environment and social behavior.* Monterey, CA: Brooks/Cole.

boyd, d. (2010). Social network sites as networked publics: Affordances, dynamics, and implications. In Z. Papacharissi (Ed.), *Networked self: Identity, community, and culture on social network sites* (pp. 39–58). Routledge.

Child, J. T., & Haridakis, P. M., & Petronio, S. (2012). Blogging privacy rule orientations, privacy management, and content deletion practices: The variability of online privacy management activity at different stages of social media use. *Computers in Human Behavior, 28*, 1859–1872.

Child, J.T., & Petronio, S. (2011). Unpacking the paradoxes of privacy in CMC relationships: The challenges of blogging and relational communication on the internet. In K. B. Wright & L. M. Webb (Eds.), *Computer-mediated communication in personal relationships* (pp. 21–40). New York: Peter Lang.

Derlega, V. J., & Chaikin, A. L. (1977). Privacy and self-disclosure in social relationships. *Journal of Social Issues, 33*(3), 102–115.

Livingstone, S., & Brake, D. R. (2010). On the rapid rise of social networking sites: New findings and policy implications. *Children & Society, 24*, 75–83.

Petronio S. (2002). *Boundaries of privacy: Dialectics of disclosure.* Albany: University of New York.

Petronio, S. (2010). Communication privacy management theory: What do we know about family privacy regulation? *Journal of Family Theory & Review, 2,* 175–196.

Smahel, D., & Wright, M. F. (Eds). (2014). *Meaning of online problematic situations for children. Results of qualitative cross-cultural investigation in nine European countries.* London: EU Kids Online, London School of Economics and Political Science.

Solove, D. J. (2007). *The future of reputation: Gossip, rumor, and privacy on the internet.* New Haven: Yale University Press,

Sonck, N., Livingstone, S., Kuiper, E., & De Haan, J. (2011). *Digital literacy and safety skills.* LSE, London: EU Kids Online.

Trepte, S., & Reinecke, L. (2011). *Privacy online*. Springer.

Westin, A. (1968). *Privacy and freedom* (5 ed.). New York, U.S.A.: Atheneum.