Collective Privacy Management Practices: A study of privacy strategies and risks in a private Facebook group

Ameera Mansour, University of Borås, Sweden
Helena Francke, University of Borås, Sweden

This paper qualitatively examines how members of a large private Facebook group view the risks of information disclosure to their privacy and the strategies they employ to navigate and manage those risks. The paper adds to an emerging interest in how privacy is managed collectively and within dynamic large groups, thus moving beyond established knowledge of privacy management on individual and small-scale levels. The work builds on semi-structured interviews with 20 members of a private Facebook group and draws on Communication Privacy Management theory. The study shows how privacy management practices are enacted at individual, intragroup, and group levels. Findings show that participants associate very high risks with sharing private information in the group, partly because it consists of a mix of known others and strangers, who are potentially geographically co-located. They adopt several strategies for managing and protecting their privacy at all three levels. The risks associated with context, time, and spatial collapse of the imagined audience are identified as important to how participants experience information disclosure in the group. The paper concludes by identifying some practical implications that serve as a call for developers to design privacy tools that support dynamic groups' privacy challenges and needs.

CCS Concepts: • **Human-centered computing → Empirical studies in collaborative and social computing;** • **Security and privacy** → Human and societal aspects of security and privacy → privacy protections

KEYWORDS: Information Disclosure; Communication Privacy Management Theory; Privacy protection; Social Networking Sites; Online Communities; Dynamic Groups; Facebook groups

ACM Reference format:

Ameera Mansour and Helena Francke. 2021. Collective Privacy Management Practices: A study of privacy strategies and risks in a private Facebook group. In *PACM on Human-Computer Interaction,* Vol. 5, CSCW2, Article 360, October 2021. ACM, NY, USA. 28 pages, https://doi.org/10.1145/3479504.

This work was funded by the Swedish Research Council (registration number: 349-2006-146).

Authors' addresses: Ameera Mansour, ameera.mansour@hb.se; Helena Francke, helena.francke@hb.se; The Swedish School of Library and Information Science, University of Borås, Sweden.

2573-0142/2021/October - 360 $15.00

https://doi.org/10.1145/3479504

1 INTRODUCTION

Facebook, one of the most popular social networking sites (SNSs), offers various opportunities to connect and interact with pre-established contacts (e.g., family, friends) and new networks through personal profiles and groups [1]. Facebook groups enable users to find and connect with local and global communities who share similar interests, experiences, or beliefs [2]. In these groups, users can exchange information, discuss mutual concerns, build solidarity, and mobilize around different causes [2-8]. As such, these groups can provide dynamic, collaborative, information-rich environments where users can extend their personal networks by joining wider, potentially heterogeneous communities of strangers [1, 5, 9, 10]. Several studies suggest that Facebook empowers various social groups (such as e.g., parents, college students, and people with chronic illnesses) by providing private spaces to seek and provide information and support on topics that are deemed to be inappropriate or stigmatizing to share with one's close networks [3, 4, 6-8, 10-17]. Members of Facebook groups can disclose and discuss information with people with whom they have no preexisting or long-term relationships, which may be considered less costly than doing so with their close social circles [7, 8, 12, 13]. Indeed, it has been argued that through Facebook groups, users can employ boundary management and 'privacy- protective' strategies to segregate different audiences and to avoid the risks of information disclosure with their Facebook friends (see [11]).

Besides highlighting the affordances and potential benefits of Facebook groups, previous studies have also provided insights into some of the challenges they may entail (relating to, for example, information credibility and trust [18, 19], and conflicts and disagreement [9]), and the ways users navigate and manage those challenges. However, few studies have so far examined information disclosure concerning privacy management practices *within* Facebook groups among group members. Rather, prior work has examined the groups function as a tool that helps users manage their privacy *across* various SNSs and Facebook privacy boundaries, rather than focusing on how users manage their privacy and information disclosure *within* the groups' boundaries. The recent few studies (e.g., [3, 5, 9]) that have addressed this perspective have studied privacy management as part of broader information practices and research questions, with the result that the findings are limited in depth and details. Further, although several studies of personal profiles on Facebook have focused on individual and collaborative privacy management among users, their findings can be limited in their applicability when it comes to collective and more dynamic sociotechnical environments, such as Facebook groups, where mutual information sharing and collaboration are the norms [4].

This suggests a knowledge gap regarding how information disclosure and privacy are managed collectively in Facebook groups, and how members handle the perceived risks of sharing private information with other members (i.e., unknown audiences). In particular, further research is required that focuses on the different levels – individual and group – on which privacy management strategies are employed in Facebook groups. It is important to address this knowledge gap because Facebook groups and similar SNSs have been shown to play a crucial role in information sharing and emotional support [3, 4, 6-8, 10, 12-16, 20], and thus group members need to have safe spaces where they have control over the information they disclose in these groups.

Based on in-depth interviews with one administrator and 19 members of a private Facebook group of international mothers living in Sweden, this paper qualitatively examines the privacy management practices of the group users by focusing on the privacy risks they associate with information disclosure in the group and the strategies they employ to navigate and manage those

risks. In the paper, we seek to answer the following research questions: RQ1) *What, if any, privacy concerns do members of a private Facebook group perceive in disclosing information in the group?* RQ2) *How is privacy co-managed by members within a private Facebook group?*

We found that unlike the safety of Facebook groups described in the cases outlined in the first paragraph, members in this Facebook group, who similarly gather around shared experiences, expressed risks associated with disclosing certain types of private information in the group. These risks arose partly from the fact that the group was too large for members to control if known others were in the group, and partly from the fact that members were potentially co-located and sometimes shared an offline presence, and so connections might be present that were unknown at the point of sharing information in the group. Overall, our findings highlight the complex nature of privacy management as a collective and multilayered information practice that requires constant consideration, coordination, negotiation, and collaboration by and among members.

In the paper, we aim to contribute to the growing CSCW and social computing literature on privacy management by developing in-depth insights into how privacy is managed in a large, networked, and collective environment that involve known, unknown, and co-located members. In doing so, we draw on and contribute to Communication Privacy Management theory (CPM). We also highlight how our findings may contribute to design opportunities, which allow people to have better control over their privacy in Facebook groups.

2 BACKGROUND WORK

In this section, we first provide a background of CPM theory and how it can be used to explain the processes involved in privacy management in groups. We then present and discuss some related work on information disclosure and privacy management in SNSs in general, and collective privacy management in particular.

2.1 Communication privacy management theory

Drawing on Altman's [21] work on privacy management, Petronio [22] has developed CPM theory to explain information disclosure processes on which people rely when deciding whether to disclose or conceal information. The theory is primarily concerned with the management of private information. Information disclosure can be defined as a communicative process that people engage in when deciding to reveal or conceal private information to others [22]. Information disclosure and self-disclosure are not synonymous, because information disclosures are not limited to the self, but they can also be about others (e.g., family, friends, groups, and organizations) [22]. Privacy can be defined as the right or freedom of individuals and groups to decide how their information flows by controlling what, when, how, and to whom information should be disclosed and made available [21]. What is considered private can vary between groups, cultures, genders, and contexts; as Petronio [22, p.67] writes "not all of our private information has the same level of significance, […] Private information changes in degrees of risk based on perceived repercussions for revealing or concealing information." The concepts of information disclosure and privacy are closely related, and CPM argues that decisions made about what information to reveal or conceal are not always straightforward, rather they represent a continuous balancing act that causes a "dialectical tension", where people have to weigh the benefits against the risks of revealing and concealing information from others [22, p.40, 23].

With CPM theory it is possible to conceptualize privacy management as a collective process that is performed at multiple levels of coordination. This process can be understood through five primary, co-dependent principles proposed in the theory: ownership, control, rules, co-ownership, and turbulence. The principle of ownership indicates that people and groups consider that they own their information and therefore develop boundaries to control and safeguard this information by deciding what, when, and with whom to disclose information. Co-ownership (guardianship) occurs when someone shares their information with others (e.g., family, organization, or group); information thus becomes co-owned by all parties involved, which expands the individual privacy boundary to a collective boundary. When others are co-owners of private information, privacy is often negotiated, coordinated, and regulated through establishing privacy rules, which may vary based on sociocultural norms, gender, motivation, context, or risk-benefit analysis [22]. These rules help draw privacy boundaries to control and safeguard private information and its flow by determining boundary linkages (i.e., who else can know the private information); permeability rules (i.e., how much others can know); and ownership rights (i.e., responsibilities of each information co-owner) [23, 24]. Thus, privacy boundary is a metaphorical concept used in CPM theory to highlight the lines or boundaries people draw around their private information [22]. Drawing such boundaries is what helps individuals and groups to control the flow and access to their information, hence what others get to know about them. When information is accidentally revealed or leaked outside the privacy boundary, because privacy rules are poorly defined, broken, or not followed through, it leads to privacy turbulence [23]. Hence, CPM can be used to move beyond an understanding of how privacy is managed individually, by emphasizing a more holistic approach of privacy management as an individual, cooperative, and collective process that is negotiated and coordinated with and on behalf of others. This theoretical approach has been useful in studies that examine privacy management practices among families, couples in face to face interactions and, more recently, in networked environments (for an overview see [24]). In this paper, we extend these conceptions by employing CPM theory to examine privacy management practices within a dynamic and collaborative Facebook group setting where privacy boundaries are collectively shared on a large scale among people who are in some cases co-located with both potential known (i.e., family, friends, and acquaintances) and unknown connections (i.e., strangers). This paper therefore contributes to the development of CPM and prior work by extending our knowledge of how privacy is co-managed and regulated in a large and dynamic group whose members do not necessarily personally know each other.

2.2 Information disclosure and privacy management on SNSs

Information disclosure on SNSs may involve both benefits and risks. On the one hand, previous research argues that disclosing information offers opportunities to connect to new people, to sustain and strengthen existing relationships, to validate and experiment with one's identity, to document important life milestones, and to access information-and-support resources from heterogeneous networks [4, 20, 25, 26]. In particular, recent research has claimed that talking about stigmatizing or traumatic experiences with others on SNSs may help people get proper information and support to adjust and better process their experiences and traumas [6-8, 12, 27-29]. On the other hand, disclosing information online may have negative consequences or risks, such as privacy loss, as information can be used and/or misused outside of one's control and the intended context. This may in turn lead to social rejection, embarrassment, and to damaged personal and professional relationships and reputations [15, 30-32].

To fully leverage the affordances of SNSs, users must disclose information to gain benefits from their connections [14]. These users may engage in (in)direct information disclosures about themselves or others by posting, liking, tagging, commenting, searching, or reading others' SNS posts. As previously discussed, balancing the benefits associated with openness and connectivity with the risks of negative repercussions from privacy loss may create tensions for users [15, 31, 33]. While such tensions can also commonly arise within traditional forms of communication (e.g., face-to-face, email), SNSs have served to heighten them, as information disclosed to/on SNSs is automatically recorded, can be viewed, shared, accessed, located, replicated and distributed to large audiences that can exist both in the present and in the future [31, 34, 35]. Consequently, SNSs often involve complex dynamics such as context collapse (i.e., the presence of people from multiple social circles and contexts) [36, 37] and invisible audiences [38] which blur the boundaries between private and public spheres [31]. Potential risks of privacy loss are further complicated on Facebook and other real-name sites where users are expected to adhere to the company's terms and conditions by providing personally identifiable information in order to access the site's features [39]. Vitak and Kim [40] have identified three main risks associated with sharing on these sites, which also summarize those identified above: interpersonal risks (stigma, social rejection, hurt feelings); impression management risks (reduction of integrity, loss of control); and affordances-based risks (visibility and persistence of information, associations with network members).

With the increasing popularity of Facebook over the past decade, considerable scholarly attention has been paid to users' privacy management practices on the site. Prior work has examined how the platform complicates information disclosure and privacy practices and how people cope with and navigate such complexities [20-21, 26, 31-32, 35-46]. These studies account for how users maintain their privacy by drawing distinct privacy boundaries between various social contexts on Facebook. This involves, for instance, employing both social and technical strategies to circumvent possible privacy turbulence when interacting with diverse audiences on one's personal profile [41]. The strategies include: changing Facebook profile privacy settings, employing lists to segment friends into various groups, selective friending, blocking, disclosing information through private messages, creating separate profiles, joining private or secret Facebook groups, disclosing content that is appropriate for all audiences or ambiguous information disclosure, self-censorship, and using different SNSs platforms to communicate with distinct audiences (e.g., Instagram, Twitter, WhatsApp, Snapchat, Reddit, Tumblr) (e.g., [20-21, 26, 31-32, 35-46]).

Previous studies have often focused primarily on how users manage their personal privacy boundaries on an individual level on Facebook and/or across different SNSs boundaries [14]. Such 'individualistic' approaches, where privacy management is considered an individual task, have increasingly been found wanting, though, as they limit their gaze to individual responsibility for controlling private information and managing privacy (for an overview see [42]). In line with this, from a CPM perspective, information shared through SNSs in general, and on Facebook in particular, is not and cannot be owned and controlled solely by an individual, as once information is disclosed, individual privacy boundaries expand into collective privacy boundaries, and thus information becomes co-owned with those sharing the boundaries. For instance, when a user discloses information by posting it to their Facebook profile, they expand their individual privacy boundary into a collective privacy boundary by including everyone, or a subset of their friends, who are allowed into this boundary [43]. Further, individual users cannot fully control disclosure of information they co-own with others or what information others share about them [44-47]. Moreover, content shared on SNSs can be viewed, accessed, leaked, harvested, and possibly used

by third parties in unintended or harmful ways (e.g., other people, the platform owners, advertisers, governments and institutions) [33, 48]. Hence, once information is disclosed on Facebook, it legally lies outside of the individual's control of how their information flows [37]. Drawing on such insights, CSCW scholarship (e.g., [47, 49-52]) has identified and emphasized the need for further empirical and theoretical conceptualization of privacy management within collaborative and dynamic group settings, to be able to better understand and support the privacy practices and needs of various groups.

2.3 Collective privacy management

Previously CPM has been applied in examinations within group contexts, such as families [23, 45] and in medical practices [49, 51]. For instance, privacy management in families has been found to be a collaborative effort where members of the family have explicit rules regulating the collective privacy boundaries around the private information co-owned by the family [22, 23, 25, 26, 45]. Within workplace settings, different medical staff teams collaborate in upholding explicit rules and policies around access, use, and dissemination of patients' medical records and sensitive information, where the protection of patients' confidentiality and privacy is a shared responsibility shared amongst all medical staff with legal repercussions for transgressing these regulations [49, 51].

A growing body of work on SNS environments proposes that as privacy boundaries are collectively shared and continue to expand across different levels, it is increasingly necessary to develop online and offline collaboration, coordination, and negotiation among users who own and co-own the information [37, 42, 44, 45, 47, 52-56]. These studies also argue that such management of information disclosure and privacy boundaries requires an understanding of the context, including audiences present and privacy norms and values [9, 34, 37]. Marwick and boyd [37] demonstrate this with the example of how young people develop creative tactics to regain control over the flow of their information by encoding shared messages, references, and symbols so they can only be understood by peers, and by negotiating with peers what content they can share about them. In this way, teens attempt to limit access to their private information from others (e.g., parents, institutions, and platforms). In addition to peers, young people also co-manage their interpersonal privacy boundaries by coordinating and negotiating what information is allowed to be shared about them on Facebook and across various SNSs with parents, siblings, and multiple generations of the family [45, 54].

From the parents' perspective, Kumar and Schoenebeck [26] illustrate the complex process of information disclosure when parents balance their needs for connection, self-validation, enactment of 'good' parenthood, and access to information and support against their needs to protect their children's privacy. In balancing the benefits and risks of sharing information about their children on Facebook, parents engage in "privacy stewardship" by coordinating and negotiating with spouses, children, and extended family members what content is (not) allowed to be shared about children on Facebook [8, 25, 26]. Along the same lines, albeit in a non-family context, De Wolf's [56] study of privacy management in a Flemish youth organization shows how the organization manages its content by discussing with youth and their parents what content is allowed (or not) to be disclosed on Facebook and other SNSs. This research particularly emphasizes the role of face-to-face and offline negotiations among members of the organization in this coordination.

As shown above, prior research provides interesting insights into collaborative privacy management practices, but we also identify some less investigated topics that motivate further research. Firstly, much of the research has focused on the ways in which personal or interpersonal

privacy boundaries are managed individually or collaboratively among small groups of people who know each other (e.g., couples, families, friends, and organizations). Our study sets out to complement previous research by focusing on an SNS environment where privacy and co-ownership of private information is negotiated with both known and unknown users. Secondly, collaborative privacy management is largely discussed in the literature when it takes place in negotiations with known users, who themselves (co-)own the information. In the context of our study, such negotiations also take place with unknown users around one party's private information. Third, earlier literature has focused primarily on dyadic, small-scale, offline group interactions, which can be difficult to apply to larger online groups, such as the Facebook group in this study [40, 47, 57].

3 THE STUDY

This section outlines the details of the Facebook group that provides the setting for the study, recruitment of the group, the participants in the study, and how the study was conducted.

3.1 Selection of research site and study participants

This study is part of a broader project focusing on the affordances of Facebook groups in enabling or constraining users' everyday life information practices. Mothers' Facebook groups were identified as interesting sites of information sharing and support, based on the lead author's personal experience of using and interacting with them. Furthermore, mothers' groups are one of the most popular and active types of groups on Facebook [19, 53-56], and the broad number of themes that may be discussed makes them an interesting site for studying users' privacy management practices on SNSs.

In the spring of 2014, the lead author approached four mothers' Facebook groups she was a member of to gain permission to recruit members to participate in the research. Two of the Facebook groups were based in Sweden and were targeted at mothers with a foreign connection who live in, or are planning to move to, Sweden, whereas the other two Facebook groups were based in the UK and had very exclusive membership criteria. All the groups were either secret or closed at the time. A secret Facebook group is only visible to group members, it is not visible to non-members and it cannot be located through search engines. A closed Facebook group is visible to non-members, which means that it can be located through Facebook's search feature, but a membership request must be sent and accepted in order for someone to gain permission to access the group and view its content. Based on the lead author's insider knowledge of implicit rules and norms in each group, permission was sought from all groups' administrators (n=8) before making a public announcement about the study in the groups. In the post, the lead author introduced herself and provided a description of the research project, inviting members to participate by answering a questionnaire. The questionnaire was designed to: 1) gauge the group members' reactions and responsiveness to the research; 2) gain the members' trust by making the goals of the study clear to potential participants; 3) evaluate the research questions and identify topics to prioritize; and 4) develop a nuanced understanding of members' general information practices in each of the Facebook groups. Thus, the questionnaire was not aimed primarily at producing data for analysis per se, but it was a useful way to negotiate access to potential research sites and to recruit members for an interview.

All group members were invited to participate, thus aiming to recruit through convenience sampling. In doing so, any member in the groups had equal opportunity to participate, and no specific criteria were used at this stage to guide the selection of the sample. While several reminders were posted in all groups inviting more members to participate, willingness to participate in an interview came almost exclusively from the Sweden-based Facebook groups. Further investigations revealed that of the two groups based in Sweden, the larger group was more active, with regular daily interactions among members. The frequency of posts led us to select that group as the research site.

Thirteen members initially agreed to participate, and the number was expanded via snowball sampling, with interviewees recruited based on recommendations by previous participants. A few members were contacted directly for a personal invitation based on their high activity or long-standing membership in the group. Recruitment ended when a point of saturation was reached, that is, when interviews added no new insights to the project [57]. At this point, 19 members had been interviewed. Initial analysis took place while interviews were carried out, which allowed (to some degree) for insights from the early interviews to guide which participants were recruited for subsequent interviews, as well as which topics were prioritized and how questions were formulated. The majority of the data collection was carried out with regular members between 2014 and 2015. These were later complemented by recruiting one member of the administrative group (the founder), as the importance of this role in managing the group emerged from our analysis of regular members' interviews. This interview was carried out in the fall of 2017.

3.2 The research site and participants

The members of the Facebook group we chose as a research site are international mothers situated in Sweden. The lead author has been a member of the Facebook group since early 2014, which as described above has facilitated her access to the research site and recruiting members from the group. Prior to the study, none of the study participants were friends of the author, although friendship with one participant developed after the interview took place. One member created the Facebook group in 2007, and she still administers it with the help of three other administrators. The main purpose of creating the Facebook group was to provide an information resource for the international mothers' community in Sweden to exchange local information, first-hand experiences, tips, and advice related to raising a family in Sweden. The group initially started as a small group of friends and acquaintances, but it has grown. When the group was first approached (spring 2014), it included 1,700 members, when the majority of the interviews were conducted (spring 2015) it had 3,000 members, and it reached 4,000+ members towards the end of data collection (fall 2017). While the privacy settings of the group were set as closed at the early stages of data collection, they were changed to secret in the later stages. Members of the group come from various backgrounds, nationalities and speak different languages. However, English is the official language of the group, as it is the common language shared among group members.

The participants ages range between 25 to 45 years old, and they had one to three children between the ages of a newborn up to 13 years old. Participants' time in Sweden ranged from eight months and up to 20 years. Their membership in the group ranged from five months and up to 10 years. We sought to recruit a demographically diverse sample, including specifically inviting participants from non-English speaking countries, but the majority of those who agreed to participate were highly educated, and primarily native English-speakers, even though they came from several different countries. While some participants described themselves as being very active, visiting and participating in the group's daily activities (e.g., by posting, commenting), some other

participants described themselves to be non-active in the group as they have seldom posted or commented. However, they actively followed and monitored the group's daily activities either through their Newsfeed or by visiting the group's page on the site. Two participants were not that active in the group, but visited or browsed through the group at least once a week.

3.3 Data collection

As participants resided at different locations and had busy work and childcare schedules, the interviews were organized around the participants' time and communication preferences. Participants were thus given the possibility to choose a time and communication medium that was most suitable for them. The interviews were conducted face to face, via Skype, FaceTime, Facebook messenger, or over the phone. Interviews lasted from 45 up to 90 minutes. In total, 20 members from the Facebook group, including the group's founder, were interviewed for the research project.

In this study we adopted a qualitative approach by employing in-depth, semi-structured interviews conducted by the lead author. The interviews covered what, why, and how the participants use the Facebook group to seek, share, and evaluate information and advice, as well as the risks and benefits they perceive when doing so. A concern about information disclosure and privacy in the group was a key theme that emerged as important for members we interviewed. One-on-one interviews were particularly useful in gaining insights into participants' views and concerns about topics and concerns that are not necessarily revealed when observing activities in the group. The interviews also allowed us to learn about information activities in which participants engaged outside the group or which were not visible to others in the group. Furthermore, this approach allowed the participants to both reflect on and share insights and views about other members' activities in the group. Further, interviewing members with wide-ranging experiences (e.g., administrative members, long-standing members, active and non-active members) who belonged to the same Facebook group allowed us to gain in-depth understanding and insights into interpersonal member dynamics and activities of importance for the group.

3.4 Ethical considerations

The Swedish Research Council's [58] advice and the AoIR Ethics working committee recommendations [59] informed the planning, collection, analysis, and dissemination of the research data. The participants gave their informed consent to participate and were advised not to disclose information about themselves or their children that they do not wish to be made public, for instance, in research publications and presentations. Further, all participants were offered the opportunity to review the interview transcript to identify potential concerns or sensitive information. None of the participants accepted the offer. To protect the participants' privacy we have excluded or replaced any demographics or identifying details that could lead to their being identifiable from within, or outside, the group with metadata (e.g., [nationality], [country of origin], [city], [occupation]). Pseudonyms (P1-P19; Administrator) are used throughout the study to further conceal the participants' identities. It should be noted that while a pseudonym (Administrator) is used to refer to the group's administrator, her identity is impossible to completely conceal as other group members can still easily identify her. The administrator was informed about this fact, and was aware of it during the interview. She was also offered the opportunity to review and approve the interview transcripts and quotations used in research manuscripts/reports; however, she rejected both offers.

3.5 Data analysis

The qualitative analysis software ATLAS.ti was used to facilitate the analysis process for this paper. Analysis was conducted through constant comparative technique [60] by the lead author and served to identify key themes in the empirical material, informed by, but not restricted to, themes identified through the literature review. We were particularly interested in identifying what privacy concerns and risks participants perceived and associated with disclosing private information in the group. The perceived privacy risks in the group were analyzed based on both the concerns of each individual member as well as for the group as a collective. We further examined the specific underlying group dynamics that have shaped how members protect their privacy. In our analysis of the data, we have drawn on the key principles of CPM theory (e.g., boundaries, co-ownership, turbulence, rules) to help interpret and contextualize our findings. Particularly, we used these principles to identify the various levels of privacy boundaries that members draw around their private information and how these boundaries may expand, decrease, and/or intersect as members recalibrate them to address various privacy challenges and needs in relation to disclosing information within the group. Using these principles allowed us to identify strategies on three main privacy management levels that members engage in to manage three main nesting privacy boundaries (see Table 1 below). Subsequently, we sought to identify the interrelationship between these boundaries by focusing on the privacy rules and strategies that regulate the links and permeability of each boundary. The analysis process was iterative; new codes were continuously compared to previous ones and were revised or merged, and additional codes and sub-codes were added. This resulted in the two main themes (perceived risks and collective privacy management) and several sub-themes presented below.

4 FINDINGS

In this section, we present findings related to our research questions, first describing how participants in the Facebook group perceived privacy risks of disclosing information (RQ1), followed by an analysis of the strategies employed by group members to minimize and circumvent these risks (RQ2).

4.1 Perceived risks of information disclosure within the Facebook group setting

The data show that the participants expressed several concerns about information disclosure in the group. These concerns also mirror findings from previous studies of information disclosure risks on SNSs (see [31, 34, 35, 40]). One of the main concerns voiced by the study participants pertained to the growing size of the audience in the group and the resulting lack of control over personal information shared within the group. It becomes an unattainable task to maintain awareness of who is in the group or to whom one is disclosing information. For example, P11, wrote in a chat interview: “This group has what 2000? 3000? Members? I do not know who they are. I feel I know many of them, as I have been following some of their life stories, but I do not know anyone in real life.” It can be challenging to delineate the potential audience as well as the context for one’s information disclosures, which also can have a negative impact on willingness to disclose information [36]. This involves the risk of context collapse [36, 37] as private information disclosed in the group may accidently be revealed or leaked to known others.

Perceived risks can also be related to Facebook’s policies and the group rules which both enforce the use of real names and participation through profiles with identifiable personal information (see also [39]). The administrator explained that in this group, members also had privacy concerns

because "many people generally use their real names and because they have got real-life friends, work colleagues, or acquaintances in the group that they may not want to know about whatever that is they are posting." Paradoxically, the use of real names is also a strategy used by the group administrators to control the legitimacy of prospective members (see below). This makes it difficult for members to use a fake or separate Facebook account [8, 13], or a temporary account [61], which would allow them more anonymity in the group. The possibility of linking information with a named person and profile poses further risks due to Facebook's affordances of visibility and persistence, since not only current but also future members can access older postings in the group [4]. This means that in this current iteration of Facebook's design, members' information disclosures can potentially be seen and used beyond the original context and the current audiences of these posts, creating not only the risk of context collapse but also of "time collapse" [62].

Other participants feared that their information disclosures could have much higher cost than causing embarrassment. While P5 felt safe and unconcerned about 'ranting' and/or reaching out for support, she also reflected that what she had disclosed previously in the group might have very serious negative repercussions on her potential future employability and networking opportunities, as she may encounter group members in other roles. P5 described "I was thinking maybe if somebody had said 'oh, I have a job', and if I want to get an employment advice, they might have seen things I have shared in the group. They might not want to employ me based on the opinions I have shared or something that is very personal I have shared in the group." Similarly, consistent with prior work (e.g., [8, 26]), many participants in our study expressed concerns about potential unforeseen or future consequences if information they had disclosed, particularly about their children, were to be accessed in the future. P4 expressed: "what concerns me the most, um, my daughter is only two and a half, but I have always worried of what's going to happen in a fifteen years' time."

The large membership base, and the persistence of the group's information, mean that extending the responsibility for private information by making group members co-owners of the information further increases the permeability of the information boundaries and the risks of leaking of information outside of the group. Unintended audiences or non-approved members (e.g., outsiders) may obtain unauthorized access to information disclosed in the group, for instance if they happen to gain access to information through an approved member's account. While P5 worried that what she posts to the group could be intentionally leaked by group members to others outside of the group if she unknowingly communicated the information to a member who had an (in)direct relationship with someone in her offline social network (e.g., family members), P10 shared similar concerns:

> "sometimes I have posted about my [partner's] family, but then I have thought 'oh, God what happens if somebody in the group knows somebody in the family in real life and, you know, have seen something I have wrote when I was bitching about something'. Like, you know, Sweden is a big country but there are not many people here and sometimes you meet people that know people, that know people, and this happens quite often." [P5]

> "I feel there is often a risk that their partners might get hold of that conversation, or maybe get access to the forum and then they can use part of that online discussion against them. Because most often abusive men do, and can, have access to their wife's device. So, if they have happened to have access to it somehow they could use that against them like 'this is how she talks about me or my kids." [P10]

Both context collapse and unauthorised access can lead to privacy turbulence, or various types of violation of privacy. This was an important concern for the study participants; whereas less serious disruptions could include stigma or embarrassment, more serious repercussions were imagined or had indeed occurred in relation to members' close personal networks and known users learning of private information being disclosed in the group (comp. [15, 30, 31]). In order to avoid theses situations, members of this group engage in privacy management at three levels, where several strategies were employed both by the group and by individual members to avoid unintended breaches of privacy.

4.2 Collective privacy management in the Facebook group

In the terminology of CPM, "once a person is permitted to know private information belonging to someone else, the individual becomes a co-owner, confidant, shareholder, or guardian" of this information [23, p.180]. Becoming a co-owner or confidant of someone else's private information entails co-owned privacy boundaries that must be managed and coordinated together. This often occurs through a privacy coordination process where privacy rules are negotiated through interaction between the original owner and new co-owners of the private information, whether implicitly or by explicitly stating privacy rules [22]. For obvious reasons, such negotiations are difficult to achieve for individual members in a large online group. Yet, our analysis shows that group members rely on different strategies at multiple levels of privacy boundaries to navigate perceived information disclosure risks within the Facebook group, including group, intragroup, and individual levels.

4.2.1 Group privacy management. At the group level, members of the Facebook group employ strategies to co-manage and protect an exterior collective privacy boundary between members and outsiders (preventing outsiders from gaining access to information in the group) and an interior collective privacy boundary maintained between members (preventing members from leaking information outside the group). Both privacy boundaries are collectively shared by all members of the group, thus they aim to protect the privacy of the whole group and by extension the privacy of individual group members. Strategies employed by members to regulate and protect the group's collective exterior and interior privacy boundaries include: 1) changing the group's privacy settings; 2) verification of member identities; 3) including only members who fit the group's identity; 4) defining explicit group privacy rules, which are upheld by group members and maintained and enforced by group administrators when broken; and 5) removing members who violate the group's privacy.

4.2.1.1 Regulating an exterior collective privacy boundary. As the group has evolved over time (see 3.2), strategies were employed to ensure increased protection of the privacy of the group and its members. This has included changing the group's privacy settings from closed to secret, which happened between the two data collection stages. The administrator described that they had changed the group's privacy settings to "secret" to make it difficult for others to locate or find the group, as the group was continuously spammed with inauthentic membership requests (with various types of malicious intent, such as spamming, trolling, and advertising). As such, the group implements very exclusive rules about who can be accepted as a group member, with an aim to maintain a very specific group identity as a mothers' only group for international mothers who are either living in or are planning to move to Sweden.

Both members and the administrators help in managing the exterior boundary by maintaining the exclusivity of the group. The administrator emphasized that members are expected to follow the group's privacy rules and only invite and share the group with those who fit the group's membership

specifications, as it often happened that members have invited others who live in Sweden but who do not match the group's identity (e.g., fathers, Swedish mothers, childcare workers): "We ask people 'when you add somebody to the group, one of your friends, please make sure that they are mothers, with a foreign connection', 'please make sure to message the admin and say: well this is my friend and I am adding them for this particular reason'".

Additionally, the administrator clarified that all potential members have to answer a predetermined set of questions, which one of the administrators would pre-screen before any membership requests were considered and approved. These questions, the administrator clarified, were intended to verify the identities of those who request to join the group:

> "We ask a set of questions, like 'do you have children?', 'how old are your children?', and 'are you trying to move to Sweden?'. Like we can be intrusive and ask all kinds of questions for people who want to join the group, but we do it for the safety and for the best of the group." [Administrator]

Thus, those requesting to join the group had to present themselves and answer questions posed by the administrators concerning information about themselves (e.g., the reason for wanting to join, place of residence, number/ages of children, occupation), which would help verify their identities. They were also required to make some identifying information public on their personal Facebook profiles to further aid the administrators' verification process. The administrator explained: "if the profile information is not public, then we will not be able [to] verify you and thus will not admit you." These intensive vetting practices are thus aimed at verifying prospective members' identities and authenticity and to add an overall protective boundary to safeguard the privacy of the group and its members from potential outsider threats. The aim of doing so, the administrator explained, was to ensure that only those who belong to and may benefit from the group are part of it. Whereas this means that there are exterior privacy boundaries in place intended to control the visibility of the group and who can gain access to information disclosed within its collective privacy boundary, it simultaneously means that as a rule, when information is shared in the group, it becomes tied to a member who is likely to be identifiable outside the group, thus raising the stakes of disclosing private information.

4.2.1.2 Regulating an interior collective privacy boundary. In addition to regulating accessibility and visibility of the group to outsiders (non-members), the group has privacy rules aimed to protect the interior collective privacy boundary of the group from potential insiders' threats and violations. The administrator emphasized, for instance, that members have a shared responsibility to respect and maintain fellow members' privacy by not disseminating or leaking what is disclosed in the group outside the group. She explained: "it is not allowed to take screenshots of people posting information and share them outside of the group. This is just not okay. This is, for me, a place where people should not feel scared to post."

Following a breach of confidence that occurred in the group when a member violated another member's – and by extension the group's – privacy by intentionally leaking the latter member's private information to her employer, the group has established explicit privacy rules that regulate access and dissemination of members' information and are intended to protect the group from information being leaked to unintended recipients. These rules are stated in a pinned post at the top of the group page. The episode thus became a "catalyst […] for boundary shifts" [23, p.184] as explicit privacy rules were introduced in the group to clarify the responsibility of its members to each other [23]. At the collective level, these are strategies to avoid privacy turbulence from occurring again because expectations of privacy are unfulfilled, poorly defined, or misunderstood,

resulting in privacy rules being violated or broken by some members [22, 23]. Administrators of the group uphold and enforce these rules by imposing sanctions when the privacy rules are not respected. In this way, group members are held accountable for any privacy violations. The privacy rules serve to maintain a thick exterior, and interior, privacy boundary around members' private information and activities in the group, with the aim to protect the collective privacy boundary shared by group members both from the inside and from the outside. Similar management of privacy boundaries around a group have been observed in other studies (e.g., [3, 6, 7, 12, 13, 63]), which emphasized the importance of such assurances for creating safe places for members to discuss various private topics.

4.2.2 Intragroup privacy management. At an intragroup level, members of the Facebook group protect each other's privacy by forming small-scale boundaries (e.g., one-to-one, one-to-few, smaller groups) around private information in the group to minimize its visibility and accessibility by other members. Whereas both group and intragroup privacy management are concerned with cooperative strategies employed by members, the key difference is that while group management is cooperation in managing the privacy boundary of the whole group, intragroup management is cooperation by two or a few members in managing the privacy boundary of an individual member's information. In this way, group members share co-ownership with one or a select few others from the group by creating intragroup boundaries with them to be able to engage in more private and discrete information disclosures that are invisible, inaccessible, and unidentifiable to others in the group, thus preventing and controlling information leaking. Two main strategies that members of the group employ to cooperate around managing privacy were identified in our analysis: 1) Hidden information disclosures (through private messages and spin-off groups); and 2) anonymous information disclosures (through anonymous group posts).

When the participants' informational or emotional needs could only be satisfied through others in the group, they made these needs known to others, but often only to a very limited few. Many participants, for instance, preferred to seek and share private information in more contained and private settings where they could both decrease the visibility of the information they (or others) disclosed and, to a certain extent, control and limit accessibility to this information. That is, participants only sought and shared information with trusted or very limited audiences. For example, when P2 needed local insights and recommendations, she posted a general question to the group in order to be connected with members living in a specific local area. She subsequently moved the conversation to private messages, a more contained, one-on-one communication channel, with the aim to gain candid replies to her questions, but also as a way to be mindful of her own and others' privacy:

> "Some of the questions I have asked them, they might not feel happy to give their responses in a public forum. Whereas, if you have a personal message, in most people's minds that message will not go any further, it will not be copied and pasted somewhere. So, people may feel more likely to be able to give an honest answer and not be judged by more people than the person that is receiving it."

Indeed, P19 went as far as to suggest that seeking information on personal matters privately through Facebook messages would be a more appropriate way than revealing them publicly in the group: "they could say it in a light way like 'could anyone private message me, I am having my personal issues regarding da da and need really someone to talk to.'"

Another way members controlled their visibility and the boundaries and conditions of sharing information was by asking a group administrator or a friend to post a question anonymously on their behalf, a strategy also employed in other Facebook groups (e.g. [5]). This typically involved

members sending their questions in a private message to an administrator who would in turn – and on their behalf – post the inquiry marked as an anonymous post in the group. The administrator described it as follows: "We do have the possibility to write to us and we will post your question anonymously, if you feel that what you are discussing is private. It is something that has happened for quite a while. People ask, 'can you ask this anonymously for me?'" By using statements such as "can you ask this anonymously for me?" when asking somebody to do this, the information owner is issuing a "disclosure warning" explicitly stating the privacy rules she expects others to follow [23, p.180]. Based on this agreement, the original information owner permits the other person to know and to further disclose the information on her behalf, but on the condition of confidentiality. In this way, the owner of the information renegotiates privacy linkage rules by determining additional co-owners (e.g., a friend, an administrator) who can be linked into her privacy boundary and collaboratively manage it, while keeping other members outside of this boundary [23, p.181]. The original information owner can therefore maintain her right to control and coordinate her ownership rules by deciding who and how much others are allowed to know about her, as well as managing and coordinating to what degree others who come to know her private information can independently manage it [23, p.181]. In this way, a friend or administrator becomes collaboratively engaged in the management of a member's personal privacy boundary. It should be noted that none of the participants interviewed for this study explicitly described employing such a strategy to seek or share information and support. However, as observed by some participants (e.g., P7) and the administrator, this strategy seemed to have grown in popularity among members who wished to access information and support and simultaneously protect their identities from being revealed to others in the group.

Lastly, a few participants shared that they had formed their own private spin-off Facebook groups after connecting with fellow members through the group. Such private groups were very exclusive, with even more strict access policies regarding who was allowed to join. Membership in these groups often pertained to a particular social circle, neighbourhood, or nationality. In these groups, the participants described feeling more open in sharing information with similar others (e.g., same nationality) who, as P18 explained, "will kind of get it." She and her fellow members in the private spin-off group felt safer and freer to complain about their spouses, families and in-laws, and rant about cultural differences among themselves; information that P18 emphasized they would "never post on the [larger group]".

The intragroup strategies employed by our study participants to manage their privacy within the group are similar to the targeted information disclosures and preventive strategies (e.g., private Facebook messages, secret Facebook groups) other studies have shown that Facebook users employ on personal profiles to navigate context collapse, prevent privacy turbulence, and control information leaking (e.g., [1, 10, 13, 14, 16, 20, 36, 40, 41, 44, 47, 63-65]).

4.2.3 Individual privacy management. Individual privacy management concerns the strategies that individual group members employ to maintain their information ownership by managing a personal privacy boundary. Our results demonstrate that the overwhelming majority of our participants associated information disclosure in the group with high risk. Consequently, they maintained a thick and rigid boundary around their private information and only allowed limited permeability to their information in the group. Our findings indicate that members adopted two main strategies to regulate a personal privacy boundary within the group: 1) self-censorship; and 2) public information disclosures that were deemed appropriate for all potential audiences.

The majority of the interviewees viewed the group as a public space, even though the administrators had employed the 'private' Facebook group setting. Many participants were very aware of the risks involved in posting information online in general, as online activity will leave permanent traces, and posts and comments can be copied, pasted, and (un)intentionally leaked outside of Facebook and the group's boundary (see also [40, 43, 66]). This was further complicated by the fact that information disclosures in the group are instantly made visible and accessible to other members, and hence automatically become co-owned by a large and homogenous audience, making it difficult to control or prevent information leaks. Consistent with this previous work on this topic, many participants considered that the only way to completely protect their privacy was by concealing or self-censoring private information from others in the group. For instance, P15 set self-regulating privacy rules for some off-limit topics (e.g., marital problems, sex life, custody, and divorce) that she refrained from discussing in the group: "I am from a generation where you do not, you know, like really share too much information on a forum like that." Likewise, P2 said:

> "Even if [the group] is closed or secret, you are always worried whether someone is judging you first of all, will this be taken out of context? Will this message be put somewhere else? And it could be silly things, but you still worry about what happens with this message, because it is there, its permanent."

In contrast to prior work (e.g., [6, 7, 12, 13]), these examples highlight that having the group set as secret on Facebook, with a *thick* exterior privacy boundary and with strict moderation, was not enough or a guarantee for the participants that what was disclosed in the group would remain safe. Only disclosing information that was considered appropriate to all potential audiences was another strategy the participants used to regulate their personal privacy boundary; a strategy commonly known as the 'lowest common denominator' [67]. As P4 described:

> "I only share information that, you know, if somebody went into Google or another search engine and wrote my name and then tried to find something I have written, it's not anything that I would be ashamed of. For instance, if I was in a job interview and somebody said, 'can I look at your Facebook page?' there is nothing there that I would be ashamed of."

Similarly, P13 avoided revealing too many details about herself and family members because she believed that it was unnecessary to share private details within the group context: "The information I share about me and my family is largely what I told you, if relevant to an answer I am giving – the age and gender of my children, my marital status and my nationality […] but it's not my place to share everything about the other members of my family".

According to previous research, both strategies (self-censorship and public information disclosure) have consistently been used when the risks of information disclosure were perceived to be very high within the context of Facebook profiles where users had too many Facebook friends [40, 68], and across other SNSs that were more easily accessed by the public (e.g., blogs, Twitter, dating apps) (see [66, 69, 70]). That is, echoing Marwick and colleagues' [66] observations, a majority of our participants perceived that it was their individual responsibility to protect their privacy in the group, which led them to privacy strategies at the individual level to protect both their own private information and information they co-owned with family members or friends. Several participants also alluded to the current discussion about what, if any, information parents share about their children online (e.g., P4 and P12), and it was clear that the privacy of family and friends was also a concern when sharing information in the group (also consistent with [8, 25, 26, 44, 45, 65, 71]). In a decision negotiated and coordinated with her husband (comp. see [25, 26]), P12 censored "a lot of information" about her daughter online, and in the group; she only disclosed

information that could be shared in public or with a stranger. She described: "I do not know if I even shared my daughter's name. My husband and I are protective of her privacy online. I usually refer to her [in the group] as my toddler or my baby."

It is important to note that although a majority of participants expressed concerns about the risks involved in disclosing private information in the group (see 4.1), not all participants necessarily perceived these risks in a similar manner. One participant, P5, described that she treated the group as a private space and felt little hesitation when inviting others inside her personal privacy boundary, with the implicit expectation that other group members will respect her privacy. Other participants' stories of what was shared in the group further indicate that there were also other members who considered the risks in the group to be low, or to whom the benefits outweighed the risks of disclosing private information in the group.

4.3 Summary

In conclusion, if the costs of information disclosures are expected to exceed the benefits gained, the study participants maintain thick and rigid privacy boundaries, where no permeability is allowed and the private information is not disclosed to anyone. The need for such boundaries arises at least in part from the difficulties of assessing who becomes a co-owner of the information in a group setting. Furthermore, the administrators, on behalf of the members, manage and guard thick exterior privacy boundaries providing protection for the information shared in the collective privacy boundary from the outside world. This is particularly important because the information disclosed in the group will be persistently accessible and searchable. Explicit rules regulating privacy have also been introduced and are enforced, to maintain interior privacy boundaries in the group. Members also mention maintaining intragroup privacy boundaries around their information, where they, together with other trusted users, cooperatively provide a layer of protection for the information, which allows for a degree of autonomy and anonymity from others within, and outside, the community [22, p.152]. In this regard, in online communities where private information is shared in collective privacy boundaries, as in this Facebook group, privacy is not, and cannot, only be managed by individual users but it is also collaboratively coordinated and regulated with and by others to both protect individual members and the group (see Table 1 for an overview).

Table 1. Overview of the various types of privacy management in the Facebook group

Privacy management	Definition	Strategies	Boundary Level	Information ownership	Implications
Group privacy management	Strategies members employ to co-manage and protect the collective (interior and exterior) privacy boundaries of the group and the information shared within these boundaries.	1) Changing group's privacy settings; 2) Verification of member identities; 3) Exclusive membership; 4) Explicit group privacy rules; 5) Removing members.	Interior and exterior group privacy boundaries (members-members; members-outsiders)	Collective ownership (all current and future members of the group)	Co-management of the group's audience; Regulating the group's visibility; Regulating the group's accessibility; Regulating information ownership.
Intragroup privacy management	Strategies group members employ cooperatively with a few other members to manage small-scale intragroup privacy boundaries.	1) Hidden information disclosures; 2) Anonymous information disclosures.	Intragroup privacy boundaries (one-one; one-select few)	Collective ownership (select/few members)	Information leaking control; Regulating visibility; Regulating accessibility; Regulating the audience; Regulating identity.
Individual privacy management	Strategies individual group members employ to maintain their information ownership by managing a personal privacy boundary.	1) Self-censorship; 2) Public information disclosures .	Personal privacy boundary	Individual ownership	Maximize individual information control

5 DISCUSSION

In the discussion, we consider how the present study adds to communication privacy management theory by investigating how participants handle co-ownership of private information with a mix of known others and strangers, who may be co-located. We also explore three tensions that arose in the analysis above, with regards to lack of anonymity, to audience, and to location. Following this we present possible considerations of design implications brought about by the study, and suggestions for issues that should be explored further.

5.1 Theoretical contributions

Members in the group manage and protect their privacy on (at least) three main levels: individual, intragroup, and group. At these different levels, group members engage in various privacy management activities individually or in cooperation with others to manage nesting and intersecting privacy boundaries. They define and establish rules to regulate links to others, permeability, and ownership rights to information contained within each boundary. Taken together, these activities help us conceptualize privacy management within this Facebook group setting as a collective and multilayered information practice that requires constant consideration, coordination, negotiation, and collaboration by and among members. The study confirms findings from previous research in Facebook settings, which have indicated that members use both individual and group privacy management strategies [64]. However, intragroup strategies also come across as important in this study, when associates (e.g., friends, administrators) are tasked with helping keep up the privacy boundaries around one person's private information using various tools, such as direct messaging, separate groups, and posting for others. The members regulate privacy boundaries by taking into account the sociotechnical context for an information disclosure, including the visibility and permanence of the posted information.

5.1.1 Potential conflicts caused by strategies for protecting privacy boundaries at different levels. The group's privacy management exhibited a potential conflict between strategies for protecting the group's exterior collective privacy boundary and maintaining individual members' privacy. Primarily, the careful vetting of prospective members required recommendation by a current member, the use of a Facebook account with their real name, and to disclose information about themselves to the administrators. These conditions had consequences for members' possibilities to share information and questions anonymously in the group, since membership was always linked to a profile with their actual name (see also [39]). The creation of an exterior collective privacy boundary to restrain access to the group by making it secret and by restricting membership was intended to create a safe space for information sharing in the group; an intention explicitly expressed by the administrator that we interviewed. However, many of the study participants did not experience the group in this way. This led to the development of strategies to circumvent being identified when disclosing information in the group. These strategies were intended to create interior privacy boundary spheres around the private information by deciding the permeability to the information (i.e., how much others know) and the kinds of links allowed (i.e., who else can know) [22]. When the participants were in need of information and support that could only be attained through other community members and which required them to share private information, they used strategies at the individual or intragroup level to control the depth of what they disclosed, with whom it was disclosed, and the appropriate setting and context for the information disclosures. This allowed members to more easily control the identity of potential co-owners than when sharing the information in the large group, thus forming privacy boundary cells [23, p.183] with select members. Whereas the administrators' vetting may keep out advertising and trolling, it seems there were other factors, further explored below, which limited trust and a sense of security when it came to sharing private information in the group.

5.1.2 Privacy management in relation to different imagined audiences in a large Facebook group. We identify the lack of a sense of security in the group on the part of the study participants as resulting from tensions arising in relation to the existing and potential audiences present in the group. On the one hand, the group contained unknown others, which caused concerns about information being disclosed to strangers. On the other hand, participants experienced difficulties in

controlling the risk of leaks of private information to one's close (current and future) networks through the group. Litt [38] has proposed a framework for describing the audiences that SNS users envision for their information disclosures when managing their privacy, which can be useful to approach the concerns expressed by the study participants. The framework consists of two main types of "imagined audience": an abstract imagined audience, according to Litt, is vague and general/broad (i.e., unknown users/members), while a specific imagined audience is often known, consisting of people in one's immediate networks (e.g., family, friends, and colleagues). In this case, the study participants were addressing an abstract imagined audience, but worried that it included a specific imagined audience that they could not directly identify in the group, partly because of the group's size. The group thus became unsuitable for sharing both private information that could be shared with strangers (anonymously) and private information that could be shared with friends and family. Based on the findings above, we also suggest extending Litt's framework to include future imagined audiences (e.g., future employers and grown-up children) as an additional type of audience that our participants considered when assessing the future implications of their current information disclosures both for themselves and for their children. This is in line with emerging research highlighting growing concerns for future implications of information disclosure on SNSs, disclosures that can be traced to past, present, and future identities [8, 25, 26, 62, 72, 73].

The specific imagined audience may in turn include known others from different paths of life: friends, relatives, colleagues, neighbours, etc. We note that context collapse and control of who is invited within one's privacy boundaries can be even more complicated to handle in Facebook groups than, for instance, on Facebook users' personal profiles. The individual member has very limited possibilities to control with whom the information is shared in a Facebook group, as it is difficult to control and maintain awareness of the current audience, especially in a large group, and as the audience changes over time. This is the third tension we have found. Previous studies (e.g., [6-8, 11-13]) have shown that some social groups (e.g., stay-at-home-fathers, grieving parents, LGBT parents, patients) use Facebook groups as a "privacy-protective strategy" [11] or "safe havens" [12] to safely discuss socially stigmatizing experiences with others who share their experiences, as information disclosures in such groups are often associated with minimal risks compared to disclosing the same information to one's close networks. This was not how the Facebook group under study in this article was perceived by most of the participants we interviewed. We argue that several of our participants associated risks with disclosing private information in the group due to a combination of group size and the fact that the group has a local anchoring. Mudliar and Raval [5] also made similar observations in two Facebook groups, noting that the presence of offline connections in those groups was a primary privacy concern which led members to be more selective, and in some instances to self-censor their information seeking about private matters (e.g., health, marital problems, and travel).

5.1.3 Privacy management implications of time and spatial collapse. The size of the group (a few thousand members) and the fact that new members were continuosly added, made it difficult to know who was in the group at a particular time (since not every member was necessarily an active poster) and who could be added to the group in the future. Brandtzaeg and Lüders [62] note that when social media profiles are linked to an identifiable person, as on Facebook, and the posts are searchable and retrievable over time, a potential "time collapse" may occur, where previous content may damage the current self-performance. This is clearly the case also in our Facebook study, with the added aspect that future inclusion of members could result in risks that were not predicted at the time of posting.

Furthermore, although the group formed an online community, many group members acted in geographical and social proximity to other members, whether known or unknown, and the overlap between offline and online encounters in the present and in the future was not unlikely. This added a further complication with regard to knowing whom one could trust with personal information or who would see the information. Without the safety of anonymity, participants were overall hesitant to disclose their private information. We refer to this converging of online and offline spaces and audiences into a single whole, connecting members who are co-located offline, as *spatial collapse*; a distinct dimension of context collapse. Spatial collapse in groups may occur with known others who share the same local space, but also with strangers in the same neighbourhood or community, such as neighbours, colleagues, parents in the same school, or someone one encounters in a shop. Related types of platforms, where spatial collapse can be expected, are dating apps [74] and sale groups on Facebook [19]. In fact, similar observations were made by Gibbs et al. [74] with regard to dating apps, where users were cautious about how they crafted their dating profiles and how they disclosed information because of the potential of developing future relations with prospective partners. However, there are also differences between the platforms. On dating apps and sale groups, the motivation for participating is to meet people or to exchange products, which is different from the information sharing and emotional support provided on the Facebook group in our study. In the latter case, members could benefit from the information without actually meeting other members, although contacts did sometimes lead to playdates for the kids or other types of in-person meetings.

Unlike the dyadic or small-scale information disclosures on dating apps, Facebook groups also afford members a broadcast-to-all possibility that allows members to make their information visible on a much larger scale and engage in dynamic communications that can instantly and constantly be monitored by a large audience (e.g., see [4]). In the group, some of the members were likely to share the same offline space, which could lead to unexpected offline encounters in people's everyday activities and social spaces. This formed yet another reason for members to be careful with the private information they shared in the group. Taken together, these specific group dynamics complicate information disclosures in the Facebook group as members have to communicate in a large group, by using their real name; addressing varied audiences; and navigating context collapse [36, 37] (including time collapse [62] and spatial collapse) all at once.

5.2 Design considerations for improved privacy design for Facebook groups

As identified above, there are a number of design features and affordances that the participants perceived as constricting their information disclosure in the Facebook group. Previous research has noted that people are more willing to disclose private information and details on SNSs if they are given a sense of control over their privacy (see [75]). We acknowledge, though, that such an approach might involve other types of risks as this may give users an illusion of control over their private information [48].

5.2.1 Increasing awareness of the audience in Facebook groups. The privacy management tools currently available in Facebook groups can only be utilized by Facebook group administrators, which means that regular members have more limited opportunities than on personal profiles to maintain awareness of who the audience for their information disclosures will be, and to control or segregate the audience or the context of information disclosures (for a comparison with personal profiles, see [41]). The one-size-fits-all broadcasting system in the group turns out to be problematic for privacy management. It resembles Twitter's broadcast to all (public or private) that Marwick

and boyd note "ruptures the ability to vary self-presentation based on audience, and thus manage discrete impressions." [70, p.2]. Similarly, our study illustrates how individual group members need better tools for privacy management that provide decentralized privacy controls and thus increase members' awareness of audiences in the group, as well as enable individual members to control the access to and visibility of their individual information disclosures. Such tools could, for instance, allow users to be notified about new members and show extended connections, so as to provide them with information to better control context, time, and spatial collapse. In this context, however, it would be important to balance the benefits of sharing information about members with potential risks for the member whose profile is shared.

5.2.2 Controlling information visibility, accessibility, and permanence in Facebook groups. Platform designers could also draw on the strategies used by the study participants, to develop enhanced privacy tools that enable members to share information with a select subset of members, to include specific members in a temporary, exclusive private subgroup to discuss without having to form a new group. Members could also have the possibility to post and comment anonymously on issues without revealing their identity, once they have been accepted as members to a Facebook group. It must be noted that at the time of writing this paper (in late 2020) Facebook introduced a new anonymous post feature in Facebook groups, which allows group members to publish their posts anonymously without revealing their identities to other members. However, this feature still has some limitations. The current anonymous post feature only allows the author of the post to publish and comment on their post thread anonymously; other members who may wish to, for instance, comment are not anonymous. By expanding this feature to allow all group members to post anonymously and comment on a post anonymously, members could leverage the full potential of engaging in group conversations and exchange resources without risks to privacy.

The risk of context and time collapse could also be more easily managed if Facebook allowed users to put a 'visible until' tag on their posts or comments, as well as to allow users to hide or control the visibility of their activities in groups. Finally, a function such as on Snapchat, which notifies the administrators and the posting member if someone makes a screenshot of a post, could make users aware that the activity may be problematic, as well as to help control damage if information is shared outside the group in this way.

5.3 Study limitations and future directions

While this research provides in-depth insights into privacy management practices within the context of a Facebook group, given the small sample of participants in this study, the findings cannot be viewed as representative of all other members' privacy management in the group, nor is their management generalizable across Facebook groups. The findings are partly supported by previous studies, but future work would be needed to extend and compare our findings with more diverse samples and groups. Further, we acknowledge that as this study mainly relies on self-reported accounts of the participants' information disclosures, there may be discrepancies, or a "privacy paradox" [33], between users' descriptions of how they disclose private information online and their actual information disclosures. Chalklen and Anderson [11], for instance, observed that although mothers express high levels of concerns about disclosing information about their children on Facebook, they still unknowingly reveal a lot of details about children when socializing with family and friends and in Facebook groups. Future work could complement our findings by studying this through observations, surveys, and longitudinal studies.

We collected data between 2014 and 2017, which potentially imposes some limitation on current applicability of our findings due to the rapid change of users' practices and platform design

developments over time. For instance, over the past few years, Facebook has changed the design and features of Facebook groups, and privacy controls have either been added or improved. As discussed in section 5.2 above, in late 2020 (at the time of writing this paper) , Facebook introduced a new anonymous posts feature in Facebook groups. However, there are still privacy issues that arose in our study which remain unsolved. Future work could extend our findings by examining the extent to which these improved privacy management tools in Facebook groups influence information disclosure and privacy management practices.

Our findings also contribute insights into Facebook group administrators' privacy management practices, although with a very limited sample. The results indicate that this is an issue well worth further exploration in other groups and settings. In addition, the concept of spatial collapse needs to be further investigated in similar and different online settings, where online participants connect with strangers who are potentially geographically co-located with each other offline. Finally, another intriguing future research direction would be to examine whether SNS users, such as Facebook group members, actually perceive a responsibility for upholding and respecting the privacy of those who disclose private information in the group, in their role as recipients of private information.

6 CONCLUSIONS

Facebook groups afford users unique opportunities to connect and collaborate with others, and to access a wide range of information and support resources. However, Facebook groups present new privacy challenges for users who must balance their needs for connectivity, information, and support with their needs for privacy. To understand what privacy concerns people have about information disclosure in a Facebook group and how they have managed those concerns, we interviewed twenty members from a closed Facebook group, including one of the group's administrators. Our analysis highlights the unique privacy challenges members face in managing their privacy and information disclosures within a privacy boundary that is collectively shared and co-managed with a large and potentially co-located audience.

Drawing on Communication Privacy Management theory as an analytical lens, our findings demonstrate that privacy management within a large online group forms a complex and multi-layered process that entails a continuous individual, intragroup, and group effort to address various privacy needs of group members. The process is managed, coordinated, and regulated at different intersecting levels of privacy boundaries among group members. Consideration of not only individual, but also intragroup and group privacy activities are thus necessary to fully grasp the nature of collective privacy management and regulations that can be particularly prominent in large and dynamic online groups (see [22, 23]). The study contributes to the growing body of work on collective privacy management within networked environments. It particularly contributes insights into privacy management within dynamic online groups where users communicate and share their privacy boundaries with audiences that are large, evolving, with known and unknown members, who are potentially co-located, thus raising several privacy challenges (e.g., context collapse, time collapse, and spatial collapse) which further complicate users' information disclosures.

Our study suggests that unlike personal profiles, Facebook group members, especially of large groups, have limited technical possibilities to maintain awareness of who the audience for their information disclosures will be, and to control or select the audience or the context of their information disclosures. The paper concludes with considerations on how changes to Facebook

groups' design can contribute to increased control over privacy boundaries and visibility for group members.

ACKNOWLEDGMENTS

We thank the study participants for their valuable contribution to the paper and we thank the anonymous reviewers for their helpful comments and suggestions. We are grateful to the "Information Practices: Communication, Culture and Society" research group at Lund University, Sweden for hosting the first author during the writing of this paper. The study was conducted within the Linnaeus Centre for Research on Learning, Interaction, and Mediated Communication in Contemporary Society (LinCS) at the University of Gothenburg and the University of Borås, Sweden.

REFERENCES

[1] Andrew Smock, Nicole Ellison, Cliff Lampe, and Donghee Yvette Wohn. 2011. Facebook as a Toolkit: A Uses and Gratification Approach to Unbundling Feature Use. *Computers in Human Behavior* 27, 6(2011), 2322-2329. DOI: https://doi.org/10.1016/j.chb.2011.07.011

[2] Mark Zuckerberg. 2017. Bringing the World Closer Together. Retrieved September 7, 2020 from https://www.facebook.com/notes/mark-zuckerberg/bringing-the-world-closer-together/10154944663901634/.

[3] Leah Williams Veazey. 2018. Navigating the Intersections of Migration and Motherhood in Online Communities: Digital Community Mothering and Migrant Maternal Imaginaries. PhD Dissertation. Department of Sociology and Social Policy, University of Sydney.

[4] Ameera Mansour. 2020. Affordances Supporting Mothers' Engagement in Information-Related Activities through Facebook Groups. *Journal of Librarianship and Information Science* 53, 2,(2020), 211-224. DOI: https://doi.org/10.1177/0961000620938106

[5] Preeti Mudliar and Noopur Raval. 2018. "They Are Like Personalized Mini-Googles": Seeking Information on Facebook Groups. In *Proceedings of the 51st Hawaii international conference on system sciences* (HICSS). Curran Associates, NY, USA, 2058–2067. http://hdl.handle.net/10125/50147

[6] Tawfiq Ammari and Sarita Schoenebeck. 2015. Networked Empowerment on Facebook Groups for Parents of Children with Special Needs. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (CHI '15). Association for Computing Machinery, New York, NY, USA, 2805–2814. https://doi.org/10.1145/2702123.2702324

[7] Tawfiq Ammari and Sarita Schoenebeck. 2016. "Thanks for your interest in our Facebook group, but it's only for dads": Social Roles of Stay-at-Home Dads. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing* (CSCW '16). Association for Computing Machinery, New York, NY, USA, 1363–1375. https://doi.org/10.1145/2818048.2819927

[8] Lindsay Blackwell, Jean Hardy, Tawfiq Ammari, Tiffany Veinot, Cliff Lampe, and Sarita Schoenebeck. 2016. LGBT Parents and Social Media: Advocacy, Privacy, and Disclosure during Shifting Social Movements. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (CHI '16). Association for Computing Machinery, New York, NY, USA, 610–622. https://doi.org/10.1145/2858036.2858342

[9] Ameera Mansour. 2020. Shared Information Practices on Facebook: The Formation and Development of a Sustainable Online Community. *Journal of Documentation* 76, 3(2020), 625-646. DOI: https://doi.org/10.1108/JD-10-2018-0160

[10] Jessica Vitak and Nicole Ellison. 2013. 'There's a Network out There You Might as Well Tap': Exploring the Benefits of and Barriers to Exchanging Informational and Support-Based Resources on Facebook. *New Media & Society* 15, 2(2013), 243-259. DOI: https://doi.org/10.1177/1461444812451566

[11] Charlotte Chalklen and Heather Anderson. 2017. Mothering on Facebook: Exploring the Privacy/Openness Paradox. *Social Media+ Society* 3, 2(2017), 1-10. DOI: https://doi.org/10.1177/2056305117707187

[12] Ylva Hård af Segerstad and Dick Kasperowski. 2015. A Community for Grieving: Affordances of Social Media for Support of Bereaved Parents. *New Review of Hypermedia and Multimedia* 21, 1-2(2015), 25-41. DOI: https://doi.org/10.1080/13614568.2014.983557

[13] Shruti Sannon, Elizabeth L. Murnane, Natalya N. Bazarova, and Geri Gay. 2019. "I was really, really nervous posting it": Communicating about Invisible Chronic Illnesses across Social Media Platforms. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (CHI '19). Association for Computing Machinery, New York, NY, USA, Paper 353, 1–13. https://doi.org/10.1145/3290605.3300583

[14] Moira Burke, Robert Kraut, and Cameron Marlow. 2011. Social capital on Facebook: differentiating uses and users.

In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '11). Association for Computing Machinery, New York, NY, USA, 571–580. https://doi.org/10.1145/1978942.1979023

[15] Nicole Ellison, Jessica Vitak, Charles Steinfield, Rebecca Gray, and Cliff Lampe. 2011. Negotiating Privacy Concerns and Social Capital Needs in a Social Media Environment. In *Privacy Online*. Springer Berlin, 19-32. https://doi.org/10.1007/978-3-642-21521-6_3

[16] Donghee Yvette Wohn, Cliff Lampe, Jessica Vitak, and Nicole B. Ellison. 2011. Coordinating the ordinary: social information uses of Facebook by adults. In *Proceedings of the 2011 iConference* (iConference '11). Association for Computing Machinery, New York, NY, USA, 340–347. https://doi.org/10.1145/1940761.1940808

[17] Lauren Britton, Louise Barkhuus, and Bryan Semaan. 2019. "Mothers as Candy Wrappers": Critical Infrastructure Supporting the Transition into Motherhood. In *Proceedings of the ACM on Human-Computer Interaction*, Vol. 3, GROUP, Article 232 (December 2019), 20 pages. https://doi.org/10.1145/3361113

[18] Ameera Mansour and Helena Francke. 2017. Credibility assessments of everyday life information on Facebook: a sociocultural investigation of a group of mothers. *Information Research* 22, 2(2017). http://InformationR.net/ir/22-2/paper750.html

[19] Carol Moser, Paul Resnick and Sarita Schoenebeck. 2017. Community Commerce: Facilitating Trust in Mom-to-Mom Sale Groups on Facebook. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (CHI '17). Association for Computing Machinery, New York, NY, USA,, 4344–4357. https://doi.org/10.1145/3025453.3025550.

[20] Nicole Ellison, Charles Steinfield, and Cliff Lampe. 2011. Connection Strategies: Social Capital Implications of Facebook-Enabled Communication Practices. *New Media & Society* 13, 6(2011), 873-92. DOI: https://doi.org/10.1177/1461444810385389

[21] Irwin Altman. 1975. The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding. Brooks/Cole Publishing Company.

[22] Sandra Petronio. 2002. Boundaries of Privacy: Dialectics of Disclosure. Suny Press, Albany, NY.

[23] Sandra Petronio. 2010. Communication privacy management theory: What do we know about family privacy regulation? *Journal of family theory & review* 2, 3(2010), 175-196. DOI: https://doi.org/10.1111/j.1756-2589.2010.00052

[24] Sandra Petronio and Jeffrey Child. 2020. Conceptualization and Operationalization: Utility of Communication Privacy Management Theory. *Current Opinion in Psychology* 31, (2020), 76-82. DOI: https://doi.org/10.1016/j.copsyc.2019.08.009

[25] Tawfiq Ammari, Priya Kumar, Cliff Lampe, and Sarita Schoenebeck. 2015. Managing Children's Online Identities: How Parents Decide what to Disclose about their Children Online. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (CHI '15). Association for Computing Machinery, New York, NY, USA, 1895–1904. https://doi.org/10.1145/2702123.2702325

[26] Priya Kumar and Sarita Schoenebeck. 2015. The Modern Day Baby Book: Enacting Good Mothering and Stewarding Privacy on Facebook. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (CSCW '15). Association for Computing Machinery, New York, NY, USA, 1302–1312. https://doi.org/10.1145/2675133.2675149

[27] Nazanin Andalibi. 2019. What Happens After Disclosing Stigmatized Experiences on Identified Social Media: Individual, Dyadic, and Social/Network Outcomes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (CHI '19). Association for Computing Machinery, New York, NY, USA, Paper 137, 1–15. https://doi.org/10.1145/3290605.3300367

[28] Nazanin Andalibi and Andrea Forte. 2018. Responding to Sensitive Disclosures on Social Media: A Decision-Making Framework. ACM Trans. Comput.-Hum. Interact. 25, 6, Article 31 (December 2018), 29 pages. https://doi.org/10.1145/3241044

[29] Nazanin Andalibi and Andrea Forte. 2018. Announcing Pregnancy Loss on Facebook: A Decision-Making Framework for Stigmatized Disclosures on Identified Social Network Sites. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (CHI '18). Association for Computing Machinery, New York, NY, USA, Paper 158, 1–14. https://doi.org/10.1145/3173574.3173732

[30] Helen Nissenbaum. 2009. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press.

[31] danah boyd. 2008. Taken out of Context: American Teen Sociality in Networked Publics. PhD Dissertation. University of California, Berkeley.

[32] Ariane Ollier-Malaterre and Luneau-De Serre. 2018. Connecting with Coworkers on Social Network Sites: Strategies, Social Norms and Outcomes on Work Relationships. In *Proceedings of the 51st Hawaii International Conference on System Sciences*, Curran Associates, New York, USA, 441-450. http://hdl.handle.net/10125/49945

[33] Monika Taddicken. 2014. The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual

Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure. *Journal of Computer-Mediated Communication* 19, 2(2014), 248-273. DOI: https://doi.org/10.1111/jcc4.12052

[34] Leysia Palen and Paul Dourish. 2003. Unpacking "privacy" for a networked world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '03). Association for Computing Machinery, New York, NY, USA, 129–136. https://doi.org/10.1145/642611.642635

[35] Jeffrey Treem and Paul Leonardi. 2012. Social Media Use in Organizations: Exploring the Affordances of Visibility, Editability, Persistence, and Association. *Annals of the International Communication Association* 36, 1(2012), 143-189. DOI: https://doi.org/10.1080/23808985.2013.11679130

[36] Jessica Vitak. 2012. The Impact of Context Collapse and Privacy on Social Network Site Disclosures. *Journal of broadcasting & electronic media* 56, 4(2012), 451-470. DOI: https://doi.org/10.1080/08838151.2012.732140

[37] Alice Marwick and danah boyd. 2014. Networked Privacy: How Teenagers Negotiate Context in Social Media. *New Media & Society* 16, 7(2014), 1051-1067. DOI: https://doi.org/10.1177/1461444814543995

[38] Eden Litt. 2015. The Imagined Audience: How People Think About Their Audience and Privacy on Social Network Sites. PhD Dissertation. Field of Media, Technology and Society, Northwestern University.

[39] Bernie Hogan. 2012. Pseudonyms and the Rise of the Real-Name Web. In *A Companion to New Media Dynamics*. Blackwell Publishing, Chichester, UK. https://ssrn.com/abstract=2229365

[40] Jessica Vitak and Jinyoung Kim. 2014. "You can't block people offline": examining how Facebook's affordances shape the disclosure process. In *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing* (CSCW '14). Association for Computing Machinery, New York, NY, USA, 461–474. https://doi.org/10.1145/2531602.2531672

[41] Jessica Vitak, Stacy Blasiola, Sameer Patil, and Eden Litt. 2015. Balancing Audience and Privacy Tensions on Social Network Sites: Strategies of Highly Engaged Users. *International Journal of Communication* 9, 1485-1504. https://ijoc.org/index.php/ijoc/article/view/3208

[42] Natalya Bazarova and Philipp Masur. 2020. Towards an Integration of Individualistic, Networked, and Institutional Approaches to Online Disclosure and Privacy in a Networked Ecology. *Current Opinion in Psychology* 36, 118-123. https://doi.org/10.1016/j.copsyc.2020.05.004

[43] Jeffrey Child and Shawn Starcher. 2016. Fuzzy Facebook Privacy Boundaries: Exploring Mediated Lurking, Vague-Booking, and Facebook Privacy Management. *Computers in Human Behavior* 54, 483-490. https://doi.org/10.1016/j.chb.2015.08.035

[44] Airi Lampinen, Vilma Lehtinen, Asko Lehmuskallio, and Sakari Tamminen. 2011. We're in it together: interpersonal management of disclosure in social network services. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '11). Association for Computing Machinery, New York, NY, USA, 3217–3226. https://doi.org/10.1145/1978942.1979420

[45] Jeffrey T. Child, Angela R. Duck, Laura A. Andrews, Maria Butauski, and Sandra Petronio. 2015. Young Adults' Management of Privacy on Facebook with Multiple Generations of Family Members. *Journal of Family Communication* 15, 4(2015), 349-367. DOI: https://doi.org/10.1080/15267431.2015.1076425

[46] Anne Oeldorf-Hirsch, Jeremy Birnholtz, and Jeffrey T. Hancock. 2017. Your Post Is Embarrassing Me: Face Threats, Identity, and the Audience on Facebook. *Computers in human behavior* 73, (2017), 92-99. DOI: https://doi.org/10.1016/j.chb.2017.03.030

[47] Haiyan Jia and Heng Xu. 2016. Autonomous and Interdependent: Collaborative Privacy Management on Social Networking Sites. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (CHI '16). Association for Computing Machinery, New York, NY, USA, 4286–4297. DOI: https://doi.org/10.1145/2858036.2858415

[48] Frederic Stutzman, Ralph Gross, and Alessandro Acquisti. 2013. Silent Listeners: The Evolution of Privacy and Disclosure on Facebook. *Journal of privacy and confidentiality* 4, 2(2013), 7-41. https://doi.org/10.29012/jpc.v4i2.620

[49] Yunan Chen and Heng Xu. 2013. Privacy management in dynamic groups: understanding information privacy in medical practices. In *Proceedings of the 2013 conference on Computer supported cooperative work* (CSCW '13). Association for Computing Machinery, New York, NY, USA, 541–552. https://doi.org/10.1145/2441776.2441837

[50] Jessica Vitak, Pamela Wisniewski, Xinru Page, Airi Lampinen, Eden Litt, Ralf De Wolf, Patrick Gage Kelley, and Manya Sleeper. 2015. The Future of Networked Privacy: Challenges and Opportunities. In *Proceedings of the 18th ACM Conference Companion on Computer Supported Cooperative Work & Social Computing* (CSCW'15 Companion). Association for Computing Machinery, New York, NY, USA, 267–272. https://doi.org/10.1145/2685553.2685554

[51] Alison R. Murphy, Madhu C. Reddy, and Heng Xu. 2014. Privacy practices in collaborative environments: a study of emergency department staff. In *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing* (CSCW '14). Association for Computing Machinery, New York, NY, USA, 269–282. https://doi.org/10.1145/2531602.2531643

[52] Jennifer Jiyoung Suh, Miriam J. Metzger, Scott A. Reid, and Amr El Abbadi. 2018. Distinguishing Group Privacy

from Personal Privacy: The Effect of Group Inference Technologies on Privacy Perceptions and Behaviors. *Proceedings of the ACM Conference on Human Computer Interaction* 2, CSCW, Article 168 (November 2018), 22 pages. https:// doi.org/10.1145/3274437

[53] Ralf De Wolf, Koen Willaert, and Jo Pierson. 2014. Managing Privacy Boundaries Together: Exploring Individual and Group Privacy Management Strategies in Facebook. *Computers in Human Behavior* 35, (2014): 444-454. DOI: https://doi.org/10.1016/j.chb.2014.03.010

[54] Ralf De Wolf. 2020. Contextualizing How Teens Manage Personal and Interpersonal Privacy on Social Media. *New Media & Society* 22, 6 (2020), 1059-1074. DOI: https://doi.org/10.1177/1461444819876570

[55] Hichang Cho and Anna Filippova. 2016. Networked Privacy Management in Facebook: A Mixed-Methods and Multinational Study. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing* (CSCW '16). Association for Computing Machinery, New York, NY, USA, 503–514. https://doi.org/10.1145/2818048.2819996

[56] Ralf De Wolf. 2016. Group Privacy Management Strategies and Challenges in Facebook: A Focus Group Study among Flemish Youth Organizations. *Cyberpsychology-Journal of Psychosocial Research on Cyberspace* 10, 1, Article 5 (2016). https://doi.org/10.5817/CP2016-1-5

[57] Philip Fei Wu, Jessica Vitak and Michael Zimmer. 2020. A contextual approach to information privacy research. *Journal of the Association for Information Science and Technology* 71, 4 (2020), 485-490. DOI: https://doi.org/10.1002/asi.24232

[58] Deborah Lupton, Sarah Pedersen, and Gareth Thomas. Parenting and Digital Media: From the Early Web to Contemporary Digital Society. *Sociology Compass* 10, 8(2016), 730-43. DOI: https://doi.org/10.1111/soc4.12398

[59] Meredith Ringel Morris. 2014. Social networking site use by mothers of young children. In *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing* (CSCW '14). Association for Computing Machinery, New York, NY, USA, 1272–1282. https://doi.org/10.1145/2531602.2531603

[60] Maeve Duggan, Amanda Lenhart, Cliff Lampe and Nicole Ellison. 2015. Parents and social media. Retrieved April 7, 2021 from http://www.pewinternet.org/2015/07/16/parents-and-social-media/

[61] Lorna Gibson and Vicki L. Hanson. 2013. Digital motherhood: how does technology help new mothers? In *Proceedings of the 2013 CHI Conference on Human Factors in Computing Systems* (CHI'13). Association for Computing Machinery, New York, NY, USA, 313–322. https://doi.org/10.1145/2470654.2470700

[62] David Silverman and Amir Marvasti. 2008. *Doing Qualitative Research: A Comprehensive Guide*. Sage Publications. Thousand Oaks, CA.

[63] The Swedish Research Council. 2017. Good Research Practice. Retrieved September 7, 2020 from https://www.vr.se/english/analysis/reports/our-reports/2017-08-31-good-research-practice.html

[64] Annette Markham, Elizabeth Buchanan, and I. R. Ethics Working Committee. 2012. Ethical Decision-Making and Internet Research: Version 2.0. Retrieved September 7, 2020 from http://aoir.org/reports/ethics2.pdf

[65] Yvonna Lincoln and Egon Guba. 1985. *Naturalistic Inquiry*. Sage Publications. London and Newbury Park, CA.

[66] Tawfiq Ammari, Sarita Schoenebeck, and Daniel Romero. 2019. Self-declared Throwaway Accounts on Reddit: How Platform Affordances and Shared Norms enable Parenting Disclosure and Support. *Proc. ACM Hum.-Comput. Interact*. 3, CSCW, Article 135 (November 2019), 30 pages. https://doi.org/10.1145/3359237

[67] Petter Bae Brandtzaeg and Marika Lüders. Time Collapse in Social Media: Extending the Context Collapse. *Social Media + Society* 4, 1(2018), 1-10. DOI: https://doi.org/10.1177/2056305118763349

[68] Alice Marwick, Clair Fontaine and danah boyd. 2017. "Nobody sees it, nobody gets mad": Social media, privacy, and personal responsibility among low-SES youth. *Social Media + Society 3*, 2(2017), 1-14. DOI: https://doi.org/10.1177/2056305117710455

[69] Bernie Hogan. 2010. The Presentation of Self in the Age of Social Media: Distinguishing Performances and Exhibitions Online. *Bulletin of Science, Technology & Society* 30, 6(2010), 377-386. DOI: https://doi.org/10.1177/0270467610385893

[70] Petter Bae Brandtzæg, Marika Lüders and Jan Håvard Skjetne. 2010. Too Many Facebook "Friends"? Content Sharing and Sociability Versus the Need for Privacy in Social Network Sites. *International Journal of Human–Computer Interaction* 26, 11-12(2010), 1006-1030. DOI: https://doi.org/10.1080/10447318.2010.516719

[71] Jeffrey Child, Paul Haridakis and Sandra Petronio. 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, 5(2012), 1859-1872. DOI: https://doi.org/10.1016/j.chb.2012.05.004

[72] Alice Marwick and danah boyd. 2010. I Tweet Honestly, I Tweet Passionately: Twitter Users, Context Collapse, And The Imagined Audience. *New Media & Society 13*, 1(2010), 114-133. DOI: https://doi.org/10.1177/1461444810365313

[73] Sarita Schoenebeck, Nicole B. Ellison, Lindsay Blackwell, Joseph B. Bayer, and Emily B. Falk. 2016. Playful Backstalking and Serious Impression Management: How Young Adults Reflect on their Past Identities on Facebook.

In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing* (CSCW '16). Association for Computing Machinery, New York, NY, USA, 1475–1487. https://doi.org/10.1145/2818048.2819923

[74] Xiaoyun Huang, Jessica Vitak, and Yla Tausczik. 2020. "You Don't Have To Know My Past": How WeChat Moments Users Manage Their Evolving Self-Presentation. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (CHI'20). Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376595

[75] Jennifer Gibbs, Nicole Ellison and Rebecca Heino. 2006. Self-presentation in online personals: The role of anticipated future interaction, self-disclosure, and perceived success in Internet dating. *Communication Research 33*, 2(2006), 152-177. DOI: https://doi.org/10.1177/0093650205285368

[76] Laura Brandimarte, Alessandro Acquisti, and George Loewenstein. 2013. Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science* 4, 3(2013), 340-347. DOI: https://doi.org/10.1177/1948550612455931

Received October 2020; revised April 2021; accepted July 2021.