Privacy Literacy and the Everyday Use of Social Technologies

Zablon Pingo(✉) and Bhuva Narayan

University of Technology Sydney, Sydney, Australia
{Zablon.pingo,Bhuva.narayan}@uts.edu.au

Abstract. The increased privacy concerns and risks associated with the misuse of personal information collected, processed and re-purposed from various digital technologies calls for users' understanding of their own informational privacy. While regulatory and technical mechanisms exist to protect individuals' information privacy, these approaches have failed to be effective. This study presents the case for privacy literacy from an information literacy perspective as a complementary mechanism to the existing approaches to protecting individuals' information privacy. The research used a constructivist paradigm, through interviewing twenty-one participants, and through online observation of SNS (social network services), and a privacy-settings walkthrough specifically on Facebook, and asking participants to track their online footprints and talk about any personal information found online.

Keywords: Privacy · Privacy literacy · Information literacy · Information privacy

1 Introduction

In digital economies, the prevalence of dataveillance [1] and monitoring of people through data from self-archiving technologies [2, 3] and online personalized and customized services [4, 5] are raising privacy concerns, debate and discussions. While these technologies provide great benefits in everyday life for the purposes of online purchases, access to information, socialization, and entertainment among other benefits, they also pose the risk of revealing too much personal information about users and of repurposing this collected information without the users' knowledge [6].

In studying privacy issues, researchers often take legal and IT systems approaches but little is known about the users' own experiences, perceptions and responses towards the efforts of managing information flows in digital technologies [7]. Privacy literacy is presented here as complementary and essential to the existing mechanisms to ensure individuals have some level of awareness and understanding of how information is tracked and used (or misused) in online environments [8]. The concept is further defined as the means and abilities to assess the collection, processing, distributing and use of personal data in digital environment [9]. Givens [10] adds that privacy literacy enables people to have an informed concern and deploy effective strategies against any privacy mismatch. Therefore privacy literacy is positioned as part of information literacy and as a means for individuals to have some level of understanding of how

S. Kurbanoğlu et al. (Eds.): ECIL 2018, CCIS 989, pp. 33–49, 2019.
https://doi.org/10.1007/978-3-030-13472-3_4

information flows, and the ability, knowledge, and skills to assess the risks and rewards associated with disclosing personal information within online environments [10].

Previous studies have quantitatively measured users' privacy perceptions and attitudes [9, 11–13]. These studies indicate that people weigh the cost-benefits and risks of sharing particular information with others [11, 14]. This study provides a qualitative perspective of users everyday privacy practices within social technologies using the lens of Sandra Petronio's communication privacy management theory [15]. In doing so, the study aims to make a case for the inclusion of privacy literacy as a fundamental aspect of promoting information literacy.

2 Research Problem and Research Question

Recent research findings demonstrate that people care about their privacy and security more than other factors in regard to information technologies [16]. The current approaches to privacy protections have "assumptions [that] users of digital technologies are omni-competent" in evaluating the present benefits and potential risks [17], and that the presumption of individuals' informational privacy is protected by legal and technical means; however, researchers have noted that these approaches do not keep up with digital innovations [18]. Additionally in the data driven society, privacy discussions have shifted from structuralistic towards individualistic perspectives due to the changes brought by economic and technological contexts [19]. Therefore, the research question is: How do users of social media (Facebook, Twitter, LinkedIn among others) understand and manage their privacy, including the risk of personal information exposure?

3 Literature Review

Scholars have theorized the concept of privacy from multiple perspectives including legal, technological, and philosophical [20]. The legal perspective conceptualizes privacy as a human right or a right to be left alone [21] while the social psychology perspective sees it as a human need for solitude, intimacy, anonymity and reserve [22]. The struggle to pin down the concept of privacy is not only because of cultural and social or contexts, but also because of complications from the digital technology innovations that Froomkin [23] refers to as 'privacy-destroying technologies', which continue to blur the lines between public and private. In this paper, we use Westin's [22] definition of privacy as a 'claim of individuals, groups or institutions to determine by themselves when, how, and to what extent information about them is communicated to others'. In the current information economies there is apparent negative impact to individuals occasioned by use of personal information without their knowledge or understanding consequently violating individuals' rights to privacy [24]. Informational privacy has become important due to the increased exposure and associated risks in digital technologies [7, 25, 26] making it an important aspect worth exploring from multiple perspectives to understand how people respond to privacy concerns. Scholars have explained people's privacy attitudes, perceptions and behaviors [27, 28] indicating a discrepancy between behavior and perception popularly referred as the privacy paradox [27, 29].

3.1 Communication Privacy Management

This study addresses privacy literacy informed by the perspectives of the communication privacy management theory (CPM) [15] to understand how consumers or users of digital technologies respond to privacy and data sharing practices in social technologies. The CPM theory [15] builds upon Altman's early conceptualization of privacy as a boundary regulation process where individuals determine their accessibility along the dimension of closedness and openness depending on the context [30, 31]. The CPM theory uses a boundary metaphor to explain how people make decisions about revealing and concealing personal information for everyday privacy management [32]. Thus the boundary erection becomes a mechanism for determining/controlling who has access to personal information or space and how much information is accessible by others [15, 33]. The theory explains that in everyday life people regulate open- and closedness to others along three different dimensions; the boundaries of disclosure, time, and identity [15]. Petronio [15] notes that in our daily lives we struggle with the question of "what to tell or not to tell" and using 'a mental calculus' helps people decide on what to disclose and to whom. That is, when to let others know our private information or thoughts and when to make it confidential; just as in interpersonal relationships, revealing information online is never a straightforward decision and is a constant balancing act. The theory identifies various factors that impact and influence privacy boundary formation rules that include: culture, gender, motivations, contexts, and risk-benefit [15], in this study we used the lens of the last three factors. Thus this theory ideal to be applied in understanding how individuals build and develop rules to aid decisions about what to reveal or conceal to best protect personal privacy through: boundary rule formation, boundary coordination and boundary turbulence [15, 32].

3.2 Information Literacy and Privacy Literacy

Over the decades information literacy (IL) has been conceptualized within the confines of education and library science as a means of identifying a need, planning to search information, consulting appropriate sources, determining the authoritativeness and authenticity of the information and finally the use of information [34]. In contexts such as new media and digital information worlds, IL has shifted significantly and expanded to other areas such as Internet literacy, media literacies and digital literacies, making it complex to determine its boundaries [34, 35]. This extends information literacy to complex models and practices including digital, media, algorithmic and privacy literacies. For instance, digital literacy is conceptualized as the ability to use information and communication technologies to find, evaluate, create, and communicate information requiring both cognitive and technical skills [36] while privacy literacy as a subcategory encompasses aspects of use of technology and awareness of personal and information privacy. The privacy literacy framework [8] identifies five cognitive processes of managing personal information disclosures that include: (1) understanding different privacy contexts related to personal information disclosures, (2) recognizing where (or which platform) to share or disclose specific information, (3) realizing the implications of sharing information in social circumstances, (4) evaluating possible threats to privacy in a given interaction, and (5) deciding what to information to share under what circumstances.

3.3 Privacy Literacy in Online Environments

Privacy literacy is positioned as a need for individuals to develop technology skills to competently use and understand issues of safe online privacy practices [10]. But privacy literacy is not only confined to online privacy practices but also includes the understanding of ones' rights to privacy, awareness of data practices, and knowledge of the institutions that safeguard data protection and privacy. Thus privacy literacy is not limited to one's ability to limit access to one's own information but extends to information from others and an understanding of how information flows in digital technologies referred to as 'networked publics' [37]; as it is also increasingly complex to control privacy in social networks due to the 'context collapse', with information flowing beyond one's control or to unintended audiences [38].

In spite of the solutions offered by technology-based and legal mechanisms to protect users' privacy, issues are still prevalent from the misuse of personal information by service providers and data brokers through their current business models [39]. Privacy literacy provides requisite awareness and knowledge for users to navigate the contexts and understanding of how such technologies work. This includes the understanding of the nature and openness of various Internet platforms, and the exposure and permanence of one's personal information once it's out there [40].

Scholars are also insisting on the need for people to understand the new information technologies and the new privacy concerns to master the information control strategies [41]. In this context a privacy-literate person is deemed to be a person who understands the constantly shifting ground of how digital technologies are over-exposing personal information to wider public and having the necessary tools to protect their privacy [8]. In addition, the person should have the ability to recognize and differentiate the type of information disclosed openly as a means of self-governance and autonomy to their privacy [28].

4 Research Design

The broader study was aimed at understanding how users of digital technologies (fitness trackers, loyalty cards and social networking sites) respond to privacy concerns. The privacy issues surrounding these technologies are associated to collection, processing repurposing, dissemination and exposure of personal information [24, 42, 43] consequently posing privacy risks to individuals (Table 1).

Table 1. Participant demographics

Participants (Pseudonym)	Gender		Occupation	Age range	Level of education	Social media used
	M	F				
Kelly		X	Professional/Student	35–40	PhD (Ongoing)	Facebook, LinkedIn, Twitter
Vera		X	Student	25	MBA (Ongoing)	Facebook, Instagram, LinkedIn
Marcello	X		Professional/Student	27	PhD (Ongoing)	Facebook, Twitter
Deepak	X		Student	22	BSc (Ongoing)	Facebook, Instagram, LinkedIn,
John	X		Professional	43	PhD	Facebook, LinkedIn
Molly		X	Professional	38	MSc	Facebook, LinkedIn
Elaine		X	Professional	25	PhD (Ongoing)	Facebook, LinkedIn
Dolly		X	Professional/Student	25–30	PhD (Ongoing)	Facebook, Instagram, LinkedIn, Twitter
Janet		X	Professional	30–35	PhD	Facebook, LinkedIn, Twitter
Sue		X	Student	23	MSc (Ongoing)	Facebook, Instagram, LinkedIn
Harry	X		Student	25	PhD (Ongoing)	Facebook, LinkedIn
Teresa		X	Professional	45–50	PhD (Ongoing)	Facebook, Flickr, Instagram, LinkedIn, Pinterest, YouTube
Michael	X		Professional/student	45	PhD (Ongoing)	Facebook, LinkedIn, Twitter
Evelyn		X	Professional/Student	45–50	PhD (Ongoing)	Facebook, LinkedIn,
Ivan	X		Student	45	MBA (Ongoing)	Facebook, LinkedIn
Lillian		X	Student	25	PhD (Ongoing)	Facebook, LinkedIn, Instagram
Pauline		X	Professional	45	MSc	Facebook, LinkedIn
Julie		X	Professional	44	MEd.	Facebook, LinkedIn, Twitter
Daniels	X		Student	19	BSc (Ongoing)	Facebook, Snapchat, Instagram, Twitter
Joe	X		Professional/Student	23	MBA (Ongoing)	Facebook, Instagram, LinkedIn, Reddit, Snapchat, Twitter
Andrew	X		Professional	52	MA	Facebook, LinkedIn, Twitter, YouTube

The participants fulfilled the following criteria: all were 18 years or older and had been using at least one of the social networking sites (Twitter, Facebook, Instagram, LinkedIn) for at least one year. All participants used the English language version of the SNS. Among all the participants, twenty-one used Facebook, eighteen (LinkedIn) nine (Twitter) and seven Instagram. Prior to conducting this research the university ethics committee checked and approved the study methods to ensure the research participants were protected. General descriptors of “professional” and student are used to describe the participants’ occupations rather than providing specific occupations to avoid exposing their identities in addition to using anonymised pseudonyms.

The research used a qualitative approach to collect data through face-to-face interviews and online observation of participants’ social network sites (SNS) and checking privacy settings using a cognitive walkthrough to see how they use and manage their privacy settings in relation to their privacy expectations and preferences. The use of semi-structured interviews offered a flexible way of exploring participants’ experiences and awareness through the guiding interview questions. Additionally, during the interviews, the participants searched their names on search engines to reflect upon any personal information accessible to the public and how it related to their privacy expectations.

Twenty-one participants (N = 21) were recruited through word of mouth, email circulation in university listservs, and through various Facebook groups. All participants were based in Australia: fifteen (n = 15) were students out of which two (n = 2) were undertaking undergraduate and thirteen (n = 13) were post-graduate students in various universities within Australia, six (n = 6) were fulltime industry professionals, nine (n = 9) participants doubled as part time students and professionals and nine (n = 9) were full-time students.

The participants took part in semi-structured interviews of between forty-five minutes to one-hour between November 2017 and December 2017. The use of semi-structured interviews supported the research findings with direct quotations from the participants [44]. The interviews were audio-recorded and transcribed for analysis. Finally, the data was coded manually and later exported to NVivo for thematic analysis. The data analysis used elements of communication privacy management theory [15] and thematic analysis [45] which are presented in the findings.

5 Findings

Our findings offer insights into participants' experiences, knowledge and skills toward privacy management on various digital and social technologies.

5.1 Appropriateness and Minimization of Personal Information Exposure

In this study the majority of the participants (14) termed the provision of some information on social media as sensitive, making them uncomfortable to share all sorts of information with services providers or with others. To counter the excessive information collection or exposure, the respondents indicated that they limited the information to only compulsory or mandatory information. For example Teresa said: "I just provide my name email address and any other compulsory data that would have been indicated as required".

Additionally the participants were concerned about disclosing information related to location such as home address due to security reasons. Kelly explained her responses as: "On Facebook I'm quite careful so no address no phone numbers, year of birth, gender, location. My current status is like I'm studying I'm married. So I would share that. So some very basic demographics but nothing that can link me to where I live unless they can still find it somehow".

In addition another participant Elaine indicated she limits personal information to minimum: "I don't post where I work on Facebook because they don't need to know. I don't have any relationship information because also they don't need to know. I think all I have is where I study and where I was born".

These data minimization practices essentially means the reduction of the personal data shared online and determining the contexts and appropriateness of sharing particular information. Thus participants purposefully use this strategy to protect their informational privacy and reduce online risks. Most participants cited the provision of (only) mandatory information as a strategy to reducing the risk of overexposing personal information. These practices are necessitated by the constant wariness and concerns associated to possible misuse of personal information (phone numbers, emails and addresses) for junk/spamming mails, selling, targeted marketing or advertisements from marketers and data brokers.

5.2 Privacy Boundary Management Practices

In online platforms it is evident people manage the type of information others can have access to as a privacy management strategy. While in social media platforms its difficult to effectively control how information flows, participants in this study deployed various strategies by actively managing what others can access about them. These practices manifest in different ways through: audience selection, managing the boundaries with their connections, self-censorship, and deletion of information accidentally or intentionally disclosed information with the goal of protecting their privacy. Some of these practices are detailed below:

Boundary Opening and Closure Across Platforms and Organizations. As part of privacy management process, people enact boundary rules to determine whether to link to others, who to be included or excluded and the type of information to be shared or revealed to others [15]. Personal information from users' social media profiles can easily permeate to unintended persons or organizations depending on how individuals manage personal information. The social media platforms provide opportunities for users to log in to other third parties applications to access other services using sign-in with Facebook or Google+ affordances. The consequent use of these conveniences effectively authorizes access of the user's profile personal information. While the "signing in with" provides convenience for the users this means one is combining boundaries of two organizations that give access to personal information to both organization, and the individual has little knowledge how their personal information will be used. In the study the majority (15 of 21) participants expressed concerns over using this convenience by purposively avoiding linking the boundary by attempt to limit information to a single organisations rather than making the link across many entities. For instance Michael indicated in the past he used the social media signing-in functionality but later on avoided it due to privacy concerns associated with enabling tracking by application providers. Michael reflected how he changed his signing in practices by creating a new account whenever using online services or applications rather than using the sign-in affordances: "I am careful about what data they allow to be shared with others. So using Facebook to log in to other things for instance is not something I would like to do, I would create a separate account for each separate one. And I won't allow to log in Facebook across, once Facebook gets into something then you know as my boss would tell me the only other thing that's got worse than terms and conditions in Facebook site is they make it easy for people to log in with Facebook everywhere. So people take the easy path all and the Google generation just don't care about".

The participants indicated taking precaution in using the “sign-in with” affordance as a way to avoid connecting boundary between two different organizations that collect personal information. Kelly also indicated in the past she used the functionality but due to increased privacy concerns, she started to create new accounts like Michael whenever signing-up for any new online services: “….I think once or twice I did sign in with Facebook because of the convenience. But now I usually get them to e-mail me a link to reset my password and then I’m go to reset everywhere else, so even though they say would you like to sign in through Facebook. I usually say no, I just prefer to have account with just that. And Facebook with just Facebook, sometimes I don’t see the relevance of signing up with… because I don’t want Facebook to know what I’m buying or doing. Of course they might soon know for some reason but I don’t want to be the one creating the direct link”.

The findings indicate awareness to online data collection practices and active privacy management in controlling the information boundaries between companies through the avoiding linking of personal information between platforms. The boundary closure practices reflect increased participants’ knowledge and awareness of privacy risks, associated with using such affordances to prevent any potential privacy risk.

Connecting and Disconnecting of Boundaries in Social Networking Sites. Facebook, Twitter, LinkedIn and Instagram are common “places” where people provide self-identifying and expressive information [8]. The privacy boundary in these platforms is managed through connecting and disconnecting with other people through sending and accepting “friend” requests and also determine what is open to others or not.

Most participants indicated they have clearly segmented their social media according to their own predefined purposes in order to determine with whom to connect. For instance all twenty-one (21) participants used Facebook to link with friends, family, new acquaintances and sometimes colleagues, and seventeen (19) used LinkedIn to connect with other professional and colleagues, while nine participants used Twitter for connecting with colleagues, professionals and others in their areas of interest and with the general public due to its open nature.

The participants indicated they were very cautious on how they responded to requests from colleagues and unknown people, for instance four participants: Teresa, Molly, Pauline and Julie all female all over 38 years old, indicated they decline accepting friend requests from colleagues or bosses on Facebook unless they have been working together for a long time or have developed close relationship. Deepak (male, student) also indicated similar views of determining boundaries with whom to connect and not, in his part time job, especially the bosses due to concerns of allowing them access to his social life. The participant explained there should be a boundary to separate formal and social relationships.

These deliberate practices of purposively and cautiously managing the boundary between personal life and work was expressed by most of the participants, citing it as a means to avoid any potential problems or mixing-up of personal life with work relationships. For example Teresa explained: “I’m very selective when I get invitations from people, for example former work colleague that I don’t usually like, sent me an invitation recently and I said I’m going to be friends with her on Facebook. So with that I rejected it. But if she approached me on LinkedIn, probably would accept. Because I use them differently I want to keep them very calm and compartmentalized, LinkedIn is my work my professional life and Facebook is my personal life"

This segmentation of the platforms social and formal relationships enables people to decide whom to connect with on what platform and what type of information can be accessed by whom, which helps users to draw their privacy boundary. For instance Joe indicated that: "There's a big difference between work life and social; that's sort of a big line there" This illustrates how people manage their privacy boundaries on an interpersonal level by selectively concealing and revealing personal information to others [46] with an increased manifestation in social media platforms [15]. The active boundary management allows people to decide with whom to have access through connecting and disconnecting boundaries (accepting or ignoring "friend" requests) in social media platforms as a way of regulating and maintaining one's privacy.

These findings are in line with previous studies; people are constantly engaged in privacy management by determining what information about them is accessible to others, and by managing personal and professional boundaries through selective disclosure of information on the Internet [47]; we found that this also applies to online social media.

Selective Information Disclosure for Reputation Management. Prior studies indicate people purposefully and selectively reveal or share information online with the goal of reputation management [46, 47], which is a privacy management goal to distinguish what is accessible and not to others through online platforms. Social media platforms easily open up personal information to the public. People share a variety of information including: academic qualifications, place of work, photos, opinions or comments, and other information, which a person may not want open to everyone.

In our study, all participants used more than one of the popular social media platforms: Twitter, Facebook, LinkedIn, and Instagram. The participants indicated a clear segmentation of the use of each social media platforms for particular purposes: LinkedIn for professional promotional and connection purposes, Facebook and Twitter are used for social and quasi-professional purposes, Instagram for personal hobbies, and personal self-promotion among other purposes. Most of the participants have categorized the use of each platform according to its perceived functionality. For instance Joe explained: "I really don't get a lot out there in my Facebook timeline. Twitter is sort of quasi-professional, I think my main motivation in maintaining that profile to appear visible; to be able to tweet at conferences, look like a somewhat active member of the field. LinkedIn is purely a sort of networking for work purposes and on Snapchat I will snap regularly with friends and Instagram is kind of much about myself - sort of a record of my photos".

Joe, who is also a casual teacher at a university, elaborated that while he uses his personal Facebook account for teaching purposes, he is careful to manage what is visible to the students by not allowing them access to his profile: "When I started teaching, I just wanted make sure students are not seeing the huge amount of personal stuff. So I guess that would have been the last time I checked sort of Facebook because we'll have like a Facebook group for the class and so people will be messaging me so I wanted to make sure that they don't see too much - I sort of treat it like my CV".

Most of the participants (19 of 21) had LinkedIn profiles, out of which twelve participants were still undertaking their studies (bachelors, masters and doctoral studies) and considered it as an important promotional tool to promote themselves to potential employers and to connect to other professionals within their field of interest. For instance Elaine (female, PhD student) said: “I do want that when people Google me I do want them to see my LinkedIn profile, that’s really the only thing I try to publish as much as possible. I do want people to see my YouTube video because it’s about my research; staff profiles, that’s fine. My Facebook doesn’t come up and I think and that’s the way I want it”

In contrast, two participants (Andrew and John) working as higher education professionals indicated a lack of interest in having LinkedIn profiles; however, due to workplace pressure they had to set-up their profiles against their wish or interest. For example John expressed his displeasure as: “We were told to have LinkedIn so I had to set-up the account”.

Andrew further expressed his concerns that LinkedIn profiles are publicly accessed terming it a vulnerable “place” where people expose too much personal information with a potential of negative impact to individuals. Andrew was weary of privacy concerns due to the possibility of over-disclosing information, which might aid identity theft given that one discloses a lot of information including personal interests. Andrew noted that: “I’ve never really thought of LinkedIn as a public document and that if somebody knew mine, because you know, the literal meaning of curriculum vitae is the story of your life. If someone knew everything in that CV, I think that it definitely can compromise your privacy. Yeah, I think, things like your personal interests, I don’t think the world needs to know my personal interests. And some of those pieces of information can be clues for passwords or those security type questions”

Generally the determination of what sort of information to share on particular platforms and with whom to connect is an indication of privacy management, thus avoiding linking information and personas, which one does not necessarily want other audiences to see or connect. This segmentation and selective disclosure enables participants to manage their reputation by controlling and determining what to reveal, conceal and with whom, which supports earlier research findings [47].

Privacy Management Through Audience Selection. By default, social media platforms open up personal information, both expressive information and self-identifying information [8, 48] to a wider public access. To navigate these privacy challenges participants are constantly managing by deciding what information is accessible to unintended audiences using the privacy settings [48]. While information sharing in social media is platform dependent, audience selection plays a key role in determining who has access to particular information. For instance, Joe explained how he actively manages audiences on Facebook: “There are some people that I chose to hide some of my posts from rather than actually deleting them from my friends list because I don’t want them to know that I deleted them. I do so because they’re posting too much, or I found their views annoying, or I don’t want them to see my posts”

To manage the audience the participants actively use the privacy controls to keep certain information within the intended target audience rather than broadcasting to “all friends” on their social media platforms by using the blocking feature, deleting posts, unfriending when there is a breakdown of a relationship, and limiting of information posting to friend lists or groups as a way of managing privacy. For example, Janet limits access to some people by blocking them or filtering them from the posts to avoid getting comments or being associated with their views. She pointed out that: “My mom posted things that has made me really angry. So I’ve put her on “very limited”. I have blocked her and she can’t see anything because my mom is older and doesn’t understand the concept of digital footprint and that sort of thing. So I don’t want to be associated with some of her views”.

Although participants indicated that on social media they generally connect with people they trust, especially Facebook, but when their reputation is potentially compromised, they limit access to information for a targeted audience, irrespective of their closeness or their pre-existing or social relationships. For those who have connected with colleagues on social media platforms they actively engage in deleting old posts as a way to avoid giving people access to their previous views which might not necessarily represent their current status. For example Joe indicated he has deleted photos to avoid people having access to them: “I feel that there were a lot of people out there that I had nothing in common with. So I’ve done a bit of cleaning of the account since its quite old maybe from 2008. So like there are some photos on I’m still seeing stuff that is quite frustrating because I made terrible decisions when I was younger like silly things and I don’t find it particularly useful in the platform”.

Monitoring Online Digital Footprint and Self-censorship. Managing personal information and digital footprint in our data-driven society is of importance but hard to control what information about an individual is publicly available and accessible on the Internet [49]. People care about what is out there about them and strategize on how to manage their footprint by routinely searching their names, videos and images on popular search engines in order to evaluate their online digital footprint or presence.

In this study the participants indicated they actively and regularly search the Internet to see what is accessible publicly about them. For example Julie, who works as a department manager, occasionally searches her name to reflect upon what personal information is out there about her on a regular basis. The self-searching or name search seemed to be a popular tool for privacy management. Julie was excited to see her publicly accessible information through search engine referring it as “googleable” with a positive connotation of good presence: “I’m very googleable because I made up my name, so when I Google I can see what I’ve posted. Like I can see who I am. You can find quite a lot about me and there’s not much you can do about that, so I just let it go and I like what I see”.

In addition, during the research interview the participants were asked to search their names and reflect on the search results as a way of understanding how people manage online footprints. All the respondents were satisfied with the results, since most of the personal information was related to their professional profiles in LinkedIn, personal websites, publications, or conference presentations and images. For instance Molly expressed her constant concern, which motivates her to engage in regular self-searching to see if there is any inappropriate information or images accessible online: “I always wonder what is there in the net about me. Because sometimes for example you can find your name or images you posted and forgotten it, right?” Dolly also narrated her experience of using Facebook from her teenage years as being careful in making decisions on whatever she posts for everyone to see. "I was quite young when I signed up because I was quite vulnerable to the Internet. I am a little bit more responsible now that I know that whatever goes up onto the Internet, I basically need to be aware that at some point it might be hacked, and it might be spread out to the world. Whatever I post has to be something that I am happy to go out to the world".

The awareness of the open nature of the online platforms informs participants' engagement in self-censorship, guiding what they post on particular online platforms as a way of protecting their reputation and privacy. These awareness and social media practices could be attributed to participants' level of education and profession. The continuous and careful management of information on respective social media indicate the deliberate development of new professional images by intentionally portraying "the fronts" [47] as professional in LinkedIn and Twitter while limiting "the back" personal life to platforms like Facebook.

Context Collapse Navigation Using Anonymous Accounts as a Means to Creating a Personal "Space". Although previous research indicate users of social media increasingly use their real names as a strategy to build reputation [49], some people maintain more than one account to enable them to express their opinions anonymously to protect their privacy or avoid other people's access to their expressive information. In this study Julie, Teresa, and Molly used anonymous names on Twitter as a means of concealing their identity and allowing them to share things they want, without the fear of being judged or their real identity known. For instance Julie has two Twitter accounts: one with her real name and the other one anonymous in what she referred to as a "secret account".

Each of the two accounts serve specific purposes with the anonymous one as a strategy to protect her privacy while on other one is actively used for professional purposes and general information sharing. The anonymous account is used to share information related to her common interests, particularly about her swimming achievements and religious views, which she does not necessarily want her colleagues or people in her professional circles to know. Julie said she decided to use the account to avoid mixing her personal and professional boundaries: "I have two accounts one is my real name and I'm happy because that's my work one, the one I use to connect with people in my industry and at conferences and in teaching and learning forums and stuff like that. But I only post stuff that is related to work or related to something or management, that sort of stuff. On my "secret account", I've deliberately not given Twitter any information about who I am. So essentially I've got this random e-mail address, because otherwise people can search for you via email address".

The use of the pseudonyms or anonymous accounts names is a strategy to protect one's personal identity and reputation by avoiding linking two personas, which corroborates with early research on reputation management [49]. For instance, Julie maintains two online personas, one as a professional and the other one as a Christian and an individual who is actively working out to lose weight using the two different Twitter accounts. This indicates that although anonymous accounts can be misused to infringe on other people's privacy, in this case the anonymous account provided a personal "space" for people to express their opinions openly without fear of being judged by colleagues or other close relations. The interviewee added further: “I would share a lot of things, I don’t really want to be that public because Twitter is a very public medium. When I’m frustrated with work or something else I didn’t want people to be out to link me to that person who works or when I’m frustrated with life or because I’m a Christian. Sometimes I’ll post Christian stuff. I don’t want people necessarily at work to think that’s how I think about life”.

The recognition of the openness and public nature of the social media platforms necessitates people to manage personal views, which represent multiple personas and the separation of them as a way of avoiding any potential conflicts and contrary perceptions against individual expectations.

5.3 Protection of Individuals Locational Privacy in Social Technologies

Social media permits people to share locational information with others within the platforms, but individuals have some forms of control to disclose or not use the locational feature for various reasons.

Although all twenty-one participants indicated they use location features in Google maps for navigational purposes, Facebook checks-ins and locational tagging, they were highly concerned about locational privacy concerns, especially in disclosing their home addresses and their real-time location for security reasons. To control the flow of locational information, participants indicated constant attempts to limit access by deactivating locational features on their smartphones or applications and avoided using the location features in social media platforms. For instance, Pauline expressed why she limits access to some location for locational privacy reasons: “I want to limit the exposure of my personal information as much as possible. I don’t use my location on my phone because I don’t want people to know where I’m located. So only when I’m desperate and I need to go somewhere I use Google Maps then I put my location on and then as soon as I finish up I takeoff my location”.

Additionally Teresa indicated she always denies access to location while using some of the smartphone and social media applications, and only activates when using specific applications: “I don’t like sharing my location for every application. I have a bad feeling about being monitored, about people knowing exactly where I am and I just… it’s just doesn’t sit comfortably with me”.

Although most participants (fourteen) indicated occasional use of the social media locational check-in feature, two of them (Michael and Kelly) indicated they only use the feature after leaving the place rather than doing it in real-time while seven indicated they had never used it and only enable the location functionality when using the applications on their smartphones applications are necessary. The protection of location privacy takes multiple perspectives both technical and active use of the social media controls, with an indication of individuals deploying all necessary means to control their locational privacy.

5.4 Managing Targeted Ads and Information Collection by Organizations

The targeted ads refer the practices of advertisers using individual users' online profiles to provide ads [50]. The targeted ads are increasingly termed as intrusive to privacy due to the collection of too much personal data about individuals. In this study participants expressed annoyance about the unwanted ads from social media and search engine providers, telemarketers and data brokers. The participants indicated active resistance to profiling and targeted ads in the browsers and on social media. For instance, 10 of 21 participants delete their search histories in the browsers, avoid using the "like button" on Facebook for things to acknowledge their personal interests in social media. The respondents were uncomfortable about targeted ads and felt being stalked, terming it as unnerving especially when reflecting on how it's done.

The respondents' attempt to control and avoid the targeted ads by using a different email address, which they use to register for all sorts of online services and subscriptions in order to avoid receiving advertisement emails or junk emails, or so as to pay special attention in their work or formal email. For example Michael said: "I have different email accounts, my personal one, the one that I give out to friends and family and other people. Then there's the Gmail account I tend to use for mailing lists and other online stuff that doesn't necessarily disclose too much personal information. It allows me to segregate out a whole bunch of junk mail that I don't necessarily want clogging up my primary email account".

Although the participants recognized targeted advertisement as unavoidable and beyond individual control in the online platforms the attempt to counter the targeted ads through active deletion of browser search histories and avoid clicking on the ads was a way to protect their privacy. Elaine explained: "I get pretty pissed off and mind-boggled, when I've done something not associated with what I did on Facebook, and then it comes up. I think that's quite annoying. I try not to search it again or go back to my history and delete all my history".

These practices of attempting to avoid online personalized services reflects some level of understanding and awareness of the omnipresent online profiling practices, and the deletion of the search histories is a form of response to counter the practices. As Dolly says: "When I see ads on my Facebook related to what I shopped for, I freak out, but I can't do anything" or as Kelly says: "I have been a bit apprehensive when you log into my email address or website and on the side there's a bar of like of everything that you visited yesterday or something… It kind of it monitors everything that you do, which is a little bit uncomfortable but I usually don't click on those things anyway because it looks like a virus to me, even though I know it's not. I don't like clicking on it".

Although some (three) participants prefer targeted ads due to the relevance to their interest they still felt uncomfortable about the tracking. Therefore, to counter the tracking, the respondents avoid clicking on the ads as a way of countering prevalent online tracking and information collection and use beyond users understanding or expectations.

6 Discussion and Conclusion

Our findings indicate that the majority of participants engage in managing privacy on social networking sites through data minimization, blocking others, unfriending, and declining friend requests, reflecting a growing awareness about privacy issues across social technologies.

The participants have clearly segmented information on particular platforms through audience selection and also by managing the boundaries between their social and professional lives, through making a deliberate choice of connecting with colleagues using LinkedIn and Twitters platforms, and using Facebook for social purposes. Although they connected with others outside their circle on Facebook, this was dictated by the already-established social relationships between individuals. In general, our findings align with earlier privacy research [46] where the participants indicated they selectively disclose and conceal some information to specific individuals by managing which audience has access to particular information. This reflects a sense of awareness of the openness of the platforms that necessitated these particular practices.

Urban and Hoofnagle [51] categorized people into privacy vulnerable and privacy resilient. We found that although participants are potentially vulnerable when ignoring terms of services and sharing their personal information to online services in exchange for benefits such as easy networking, keeping in touch, personal image management, and entertainment, they also managed their risks in a way that they could be resilient. They monitored their own data and erased data as needed. Some limited their personal information across devices and online applications, which reflects an awareness of the risks, but this also needed continual effort and continuous management on their part, and hence was also a constant negotiation. Nevertheless, this negotiation requires an informed understanding of the fast-changing world of digital social media, which reiterates the role of privacy literacy.

References

1. Clarke, R.: Introduction to Dataveillance and Information Privacy, and Definitions of Terms (1999). http://www.rogerclarke.com/DV/Intro.html
2. Sellen, A.J., Whittaker, S.: Beyond total capture: a constructive critique of lifelogging. Commun. ACM **53**, 70–77 (2010)
3. Lupton, D.: The Quantified Self. Polity Press, Malden (2016)
4. Kobsa, A.: Pseudonymous yet personalized interaction with websites that utilize network-wide user modeling services. In: HCIC Winter Workshop, Winter Park, CO (2003)
5. Garcia-Rivadulla, S.: Personalization vs. privacy. IFLA J. **42**, 227–238 (2016)
6. Etzioni, A.: A Cyber Age Privacy Doctrine: Policy and Practice. Polgrave Macmillan, New York (2015)
7. Correia, J., Compeau, D.: Information privacy awareness (IPA): a review of the use, definition and measurement of IPA. In: Proceedings of the 50th Hawaii International Conference on System Sciences, Hawaii (2017)
8. Rotman, D.: Are you looking at me? Social media and privacy literacy. In: Poster in the 4th iSchool Conference, Chapel Hill, USA (2009)

9. Veghes, C., Orzan, M., Acatrinei, C., Dugulan, D.: Privacy literacy: what is and how it can be measured? Ann. Univ. Apulensis Ser. Oeconomica **14**, 704 (2012)
10. Givens, C.L.: Information Privacy Fundamentals for Librarians and Information Professionals. Rowman & Littlefield, Lanham (2015)
11. Rainie, L., Duggan, M.: Privacy and Information Sharing. Pew Research Center (2016). http://www.pewinternet.org/2016/01/14/2016/Privacy-and-Information-Sharing/
12. Veghes, C., Popescu, I.C., Orzan, M., Acatrinei, C.: Mapping the private space of the romanian consumer: micro and macroeconomic implications. Ann. Univ. Apulensis Ser. Oeconomica **16**, 1 (2014)
13. Smith, C.L.: Privacy and trust attitudes in the intent to volunteer for data-tracking research. Inf. Res.: Int. Electron. J. **21**, 32 (2016)
14. Acquisti, A.: Privacy in electronic commerce and the economics of immediate gratification. In: Proceedings of the 5th ACM Conference on Electronic Commerce, pp. 21–29. ACM (2004)
15. Petronio, S.: Boundaries of Privacy: Dialectic of Disclosure. State University of New York Press, Albany (2002)
16. Office of the Australian Information Commissioner: Australian Community Attitudes to Privacy Survey (2017)
17. Park, Y.J.: Digital literacy and privacy behavior online. Commun. Res. **40**, 215–236 (2013)
18. Svantesson, D., Clarke, R.: A best practice model for e-consumer protection. Comput. Law Secur. Rev. **26**, 31–37 (2010)
19. Fornaciari, F.: Pricey privacy: framing the economy of information in the digital age. First Monday **19** (2014)
20. Newell, P.B.: Perspectives on privacy. J. Environ. Psychol. **15**, 87–104 (1995)
21. Warren, S., Brandeis, L.: The right to privacy. Havard Law Rev. **4**(5), 193–220 (1890)
22. Westin, A.F.: Privacy and Freedom. Athenaeum, New York (1967)
23. Froomkin, A.M.: The death of privacy? Stanford Law Rev. **52**, 1461–1543 (2000)
24. Haynes, D., Robinson, L.: Defining user risk in social networking services. Aslib J. Inf. Manag. **67**, 94–115 (2015)
25. Christl, W., Spiekerman, S.: Networks of Control: a Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy. Facultas, Vienna (2016)
26. Papacharissi, Z., Fernback, J.: Online privacy and consumer protection: an analysis of portal privacy statements. J. Broadcast. Electron. Media **49**, 259–281 (2005)
27. Bandara, R., Fernando, M., Akter, S.: Is the privacy paradox a matter of psychological distance? An exploratory study of the privacy paradox from a construal level theory perspective. In: Proceedings of the 51st Hawaii International Conference on System Sciences, Hawaii (2018)
28. Floridi, L.: Four challenges for a theory of informational privacy. Ethics Inf. Technol. **8**, 109–119 (2006)
29. Barnes, S.B.: A privacy paradox: social networking in the United States. First Monday **11** (2006)
30. Altman, I.: The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding. Brooks/Cole, Monterey (1975)
31. Altman, I.: Privacy regulation: culturally universal or culturally specific? J. Soc. Issues **33**, 66–84 (1977)
32. Petronio, S.: Boundaries of Privacy: Dialectics of Disclosure. Suny Press, Albany (2012)
33. Metzger, M.J.: Communication privacy management in electronic commerce. J. Comput.-Med. Commun. **12**, 335–361 (2007)
34. Cox, A.M., McKinney, P., Goodale, P.: Food logging: an information literacy perspective. Aslib J. Inf. Manag. **69**, 184–200 (2017)

35. Dinev, T., Hart, P.: Internet privacy concerns and social awareness as determinants of intention to transact. Int. J. Electron. Commer. **10**, 7–29 (2005)
36. ALA Digital Technology Taskforce: What is Digital Literacy? (2011)
37. Boyd, D.: Why youth (heart) social network sites: the role of networked publics in teenage social life. In: Buckingham, D. (ed.) Macarthur Foundation Series on Digital Learning–Youth, Identity, and Digital Media Volume, pp. 119–142. MIT Press, Cambridge (2007)
38. Marwick, A.E., Boyd, D.: Networked privacy: how teenagers negotiate context in social media. New Media Soc. **16**, 1051–1067 (2014)
39. Rappa, M.: Business Models on the Web (2003). http://digitalenterprise.org
40. Park, Y.J., Jang, S.M.: Understanding privacy knowledge and skill in mobile communication. Comput. Hum. Behav. **38**, 296–303 (2014)
41. Hargittai, E.: A framework for studying differences in people's digital media uses. In: Kompetenzzentrum Informelle Bildung (ed.) Grenzenlose Cyberwelt, pp. 121–136. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-531-90519-8_7
42. Stvilia, B., Choi, W.: Mobile wellness application-seeking behavior by college students: an exploratory study. Libr. Inf. Sci. Res. **37**, 201–208 (2015)
43. Christiansen, L.: Personal privacy and internet marketing: an impossible conflict or a marriage made in heaven? Bus. Horiz. **54**, 509–514 (2011)
44. Williamson, K., Johanson, G.: Research Methods: Information, Systems and Contexts. Tilde Publishing, Australia (2013)
45. Braun, V., Clarke, V.: Using thematic analysis in psychology. Qual. Res. Psychol. **3**, 77–101 (2006)
46. Nippert-Eng, C.E.: Islands of Privacy. University of Chicago Press, Chicago (2010)
47. Ryan, F.V.C., Cruickshank, P., Hall, H., Lawson, A.: Blurred reputations: managing professional and private information online. J. Librarianship Inf. Sci. (2017). https://doi.org/10.1177/0961000618769977
48. Madden, M., Smith, A.: Reputation Management and Social Media. Pew Internet & American Life Project (2010)
49. Ryan, F.V., Cruickshank, P., Hall, H., Lawson, A.: Managing and evaluating personal reputations on the basis of information shared on social media: a generation x perspective. Inf. Res.-Int. Electron. J. **21** (2016)
50. Xia, H., Wang, Y., Huang, Y., Shah, A.: "Our privacy needs to be protected at all costs": crowd workers' privacy experiences on amazon mechanical turk. ACM Hum.-Comput. Interact **1**, 22 (2017)
51. Urban, J.M., Hoofnagle, C.J.: The Privacy Pragmatic as Privacy Vulnerable. UC Berkeley Public Law Research Paper, no. 2514381 (2014)