Abstract
This paper argues that there is a need for extending the concept of information literacy to include privacy literacy, which we conceptualise as the awareness and tools needed to understand and navigate our contemporary world of connected information and synergistic technologies whilst also protecting ones personal information. The paper is based on an interview study of participants in combination with online ethnographic observations of social media, and a cognitive walkthrough of their social media use.

Background
In our information age, all of our lives are increasingly monitored and configured by digital technologies (Lupton, 2015) and this has implications on the goods and services we receive, including health, car, and home insurance (Pingno & Narayan, 2016). Google, Facebook, Twitter, and YouTube provide platforms for people to create a personal profile, share information, link to others, befriend strangers, connect with others, subscribe to channels, and follow people. This involves the sharing of personal information for verification that is later used to profile individuals for advertisements and other purposes (Buchman, 2013; Meikle, 2016). Such massively generated data from use of digital devices or applications is referred to as “big data” (Agnellutti, 2014), with a huge trend in data mining and machine learning in order to understand users’ preferences, and behaviour patterns. Such personal information can potentially be used beyond intended purposes (Pierson, 2012), and has sparked discussions on how they simultaneously empower and disempower users in various ways, creating opportunities and exposing users to vulnerabilities (Christiansen, 2011; Pierson, 2012; Rosenblat, Kneese, & Boyd, 2014). They also point to a shift in the responsibility of privacy to the user as is evident from the messaging from the Office of the Australian Information Commissioner, which says ‘privacy in your hands.’ (OAIC, 2016). This raises the question of whether users have the awareness, knowledge, and tools to take privacy in their hands. Therefore, the research question this study addresses is: Do everyday users of social media understand its implications for personal information privacy, and what measures do they take to protect their privacy?

Conceptual framework
Westin (1967) defined privacy as ‘the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others’. The process of regulating privacy is a dynamic process of optimizing two psychological needs: the need to preserve one’s privacy and control access to and distribution of personal information, and the need to interact socially, where one has to disclose personal information (Altman, 1975). Hence, privacy is constructed and negotiated in social processes (Solove, 2002).
Information privacy is often considered a technical design problem in information systems research (Cavoukian & Jonas, 2012, p. 863; Lehikoinen, 2008). Rather than this system-centred approach, Debatin (2011, p. 57) recommends that people need to develop an understanding of technology and its unintended consequences. In other words, users of digital technologies need to develop an informed concern about their privacy, avoiding both moral panic and ignorant or naïve indifference towards information technologies (Debatin, 2011, p. 57). Christiansen (2011) notes two distinct information sharing practices which users of technologies need to know or understand: voluntary sharing and involuntary disclosures.

Debatin (2011) defines privacy literacy as ‘an informed concern for individuals privacy and effective strategies to protect it’. From an information literacy perspective, privacy literacy is proposed as one’s level of understanding and awareness of how personal information is tracked and used in online environments, and how information can retain or lose its private nature (Givens, 2015, p. 53). Möllers and Hälterlein’s (2013) argue that people need to exhibit active participation in negotiating for their privacy through understanding what is at stake when using digital technologies. When people use digital devices or applications, they need to decide on whether to give personal information by consciously considering the terms and conditions of the service (Debatin, 2011), which often requires high-level cognitive effort, which users hardly have the time or the tools for (Gindin, 2009; Solove, 2012), and hence avoid engaging with it. This information avoidance is a stress and coping method deployed by humans to deal with cognitive dissonance or is a result of cognitive bias (Case, Andrews, Johnson, & Allard, 2005). Narayan, Case, and Edwards (2011) note that ‘people tend to seek out information that agrees with their pre-existing world-view and cognitive skill levels rather than acknowledge or seek new information that may cause an uncomfortable conflict in their minds’. The negotiated nature and commodification of privacy (Barnes, 2006; Thrift, 2005) causes such a cognitive dissonance and hence attracts information behaviour perspectives. The reason people avoid this information is not deliberate, but due to the sheer amount of time needed to read the privacy terms and the complexity of the language [and the interfaces] used (Potter, 2015).

**Methodology**

Perik, de Ruyter, and Markopoulos (2005) noted that there is a methodological problem especially in the domain of privacy in computer-mediated communication research. In a study of people’s information privacy perceptions though observations of actual use of a system, many respondents demonstrate risk-taking behaviours compared to interview responses (van de Garde-Perik, 2009, p. 21). To address these issues, a triangulation of methods was used in our study (Yin, 2013); we used a combination of online observations or *digital ethnography* (Talip, Narayan, Edwards, & Watson, 2015) and cognitive walkthroughs (Blackmon, 2004) alongside interviews with participants about their perceptions, awareness, and use of social media. Six university students participated in this study.
Findings
Findings show that privacy is a negotiated process wherein users decide on how much personal information they want to disclose online, and for what returns. Participants also exhibited various information behaviours such as information avoidance, due to information overload and the lack of cognitive tools to process the information. The cognitive walkthrough revealed that the interface of social media sites was a huge issue also — they are designed to be seamless which also means that most users did not know how to work the privacy settings. That said, we found two distinct groups amongst the participants. Those who, when there are two competing needs, choose to ignore their need for privacy over the immediate gains they can get from a transaction or interaction, while others were so paranoid about their privacy that it inhibited their online social interactions. We believe that both of these groups can benefit from privacy literacy that helps them engage with the online world without compromising their personal information. This calls for a need to incorporate privacy literacy as an essential complement to information literacy.

References


