Article

SM+S
social media + society

Social Media + Society
April-June 2019: 1–14
© The Author(s) 2019
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/2056305118824199
journals.sagepub.com/home/sms
SAGE

Awareness of Indirect Information Disclosure on Social Network Sites

Ali Padyab[1], Tero Päivärinta[1,2], Anna Ståhlbröst[1], and Birgitta Bergvall-Kåreborn[1]

Abstract
This research investigates user awareness and attitudes toward potential inferences of information posted on social network sites (SNSs). The study reports how user attitudes change after exposure to inferences made based upon information they have disclosed on an SNS, namely, on Facebook. To demonstrate this, two sub-studies involving three focus group sessions were conducted with Facebook users. In the first sub-study, the users received a general introduction to information that can be inferred from posts by using a prototypical privacy-enhancement tool called DataBait. Then, the second sub-study allowed the users to witness the potential inferences of their own Facebook photos and posts by using the DataBait tool. Next, qualitative content analysis was conducted to analyze the results, and these showed that the participants' attitudes toward privacy on SNSs changed from affective to cognitive when they became aware of potential inferences from actual information posted on their own Facebook accounts. The results imply that end users require more cognitive awareness regarding their genres of disclosure and the effect of their disclosures on their privacy. Moreover, as privacy awareness is contextual, there is a need for more research and development of online tools that will allow users to manage and educate themselves.

Keywords
social network site, privacy awareness, affective attitude, cognitive attitude, genre of disclosure, secondary use of personal information, data mining

Introduction

Social network sites (SNSs) enable users to create a profile on the Internet through which they can present a description of themselves and participate in various social activities. Users post many types of personal information on SNSs, particularly concerning their personal networks, relationships, online behavior, and personal preferences; however, such disclosure of personal information makes individuals susceptible to data mining and analytics, which may jeopardize privacy. A recent scandal involving Facebook and Cambridge Analytica has sparked a public outrage that once again attracted attention to the usage of personal information. This revelation by *The Observer* and *The Guardian* in March 2018 involved a highly complex story concerning data analytics firm Cambridge Analytica and its use of data from the Facebook profiles of 87 million people for political campaigning. After profiling those citizens with respect to their interests, the firm crafted personalized micro-ads and targeted voters with the aim to influence their votes in the 2016 U.S. presidential election (Cadwalladr & Graham-Harrison, 2018).

Another issue is that many SNS providers mine social media data for secondary purposes, such as for targeted advertisements, marketing, improvement of their own services, or even for behavioral surveillance; in fact, such secondary use of personal information is within the business models of several SNSs (Fuchs, 2013). Secondary information use "occurs when personal information collected for one purpose is subsequently used for a different purpose" (e.g., an SNS provider or a third party) (Culnan, 1993, p. 341). Social media users lack understanding of the business models of SNSs, as well as an awareness of how their personal information is processed by such organizations (Orito, Fukuta, & Murata, 2014; Tavani, 2013); further, a large amount of individuals' data, which they are often unable to monitor, protect, or even control in terms of its subsequent use, is sensitive

[1] Luleå University of Technology, Sweden
[2] University of Oulu, Finland

Corresponding Author:
Ali Padyab, Luleå University of Technology, 971 87 Luleå, Sweden.
Email: ali.padyab@ltu.se

(Kosinski, Stillwell, & Graepel, 2013; Krasnova, Günther, Spiekermann, & Koroleva, 2009; Narayanan & Shmatikov, 2009).

Personal information processing via data mining and profiling by third parties has been criticized for representing a loss of autonomy over personal information (Tavani, 2013) as well as for its psychological effects such as embarrassment or shame (Shoemaker, 2010). Previous research has shown that people are often unaware of how personal data can be used (Acquisti, Brandimarte, & Loewenstein, 2015), and has therefore demanded greater public awareness about social media data mining (Hugl, 2011; Marwick & Hargittai, 2018). Psychological reactions and attitudes of individuals to invasions of privacy caused by the abovementioned practices (e.g., the Facebook/Cambridge Analytica case) need to be understood with regard to both cognitive and affective attitudes towards information privacy (Choi, Jiang, & Yap, 2012); the cognitive component of individuals' attitudes is related to thoughts, appraisals, or understandings, whereas affective components include feelings or drives associated with an attitude object (i.e., secondary information use and information privacy).

This study seeks to determine *whether, and if so, how, improved user understanding of the potential inferences that can be made from information shared on SNSs influences privacy awareness and attitudes toward further disclosure*. As such, our research approach complements previous literature by enlightening end users, through the use of a privacy-enhancement tool, of the potential sensitivity of their *personal* SNS information and the inferences that can be made from this information. The findings suggest that the use of tools that illustrate the potential secondary uses of personal disclosures have an impact on awareness and, thus, change attitudes toward disclosure.

The remainder of the article is structured as follows: first, an overview of privacy research and information disclosure on SNSs is presented; then, we describe the research process, detailing the demonstration of a privacy-enhancement tool in two sets of focus group sessions; next, after presenting the findings of this study, the contributions and implications are discussed; finally, the article concludes with propositions for further research.

Theoretical Background

This section first introduces the basic concepts used to describe information disclosure on SNS sites and then summarizes previous studies concerning potential inferences that can be made from such information. We also introduce the concept of "genre of disclosure," which is employed as the theoretical lens for the data analysis conducted in our study.

Indirect Disclosure of Personal Information on SNSs

Personal information shared on SNSs is a key area of privacy research. In legislation, this involves any piece of information that can be used to distinguish an individual through factors such as physical, physiological, mental, economic, cultural, or social characteristics (Art. 4.1 General Data Protection Regulation [GDPR], 2016). Secondary use of personal information is the main focus in this area; in secondary use, information gathered for one purpose (e.g., SNSs facilitating content sharing via their site) is used for another purpose (e.g., improving services and advertising) (Culnan, 1993). In the early information systems literature, secondary information use was focused on direct marketing (Culnan, 1993, 1995), that is, information is shared directly by a user, though he or she has disclosed it for purposes different than those for which the provider uses it. For example, the location of residency is shared with the intention of receiving a purchased product and not necessarily for receiving company brochures.

However, the landscape has changed considerably since then: with enhancements in information technology, many have become aware of the economic value that can be gained from processing information for the personalization of services and behavioral advertising (Hann, Hui, Lee, & Png, 2007). Using information has become a necessary part of delivering a service that is typically done outside of the user's sphere of influence (Spiekermann & Cranor, 2009). Targeted personalized advertising is a standard feature of most commercial SNSs (Fuchs, 2013), which implies that many SNSs that are free also collect and use their users' data as part of their business model to earn money through advertising.

Most SNSs are sharing more than just basic demographic information about individuals; instead, they provide features that include, though not limited to, the ability to share opinions, make comments, write private messages, and share photos, videos, and blog posts, among other things (boyd & Ellison, 2007). Through these activities, individuals may disclose information indirectly that is embedded in other shared information (e.g., posts, comments, likes, and photos) in the form of identity and personality cues (Min, 2016). Indirect personal information cannot be conspicuously found in the profile of a user profile but needs to be processed to become available. Several studies have shown that information technologies, such as data mining, can reveal these identity cues in SNS data with high accuracy. For example, Kosinski et al. (2013) showed that human behavior can be predicted by analyzing the digital records possessed by SNSs. Specifically, the authors analyzed the Facebook "likes" of 58,466 users and mined the following user attributes with the following accuracy: 95% for ethnicity, 93% for gender, 88% for homosexuality among men, 75% for homosexuality among women, 85% for political affiliation, 82% for religion, 73% for cigarette smoking, 70% for alcohol consumption, 67% for relationship status, and 65% for drug use.

Several SNSs, such as Facebook, make use of information gathered from personal data mining to create accurate "profiles" of individuals for the secondary purpose of personally targeted advertising (Al-Saggaf & Islam, 2015). Obviously, third-party applications in SNSs make use of data mining as well (Rizk, Gürses, & Guenther, 2010). While secondary information use is legal by SNSs and third-party applications, illegal third parties can create a digital dossier using relevant inferred information (Gross & Acquisti, 2005), and nefarious individuals can exploit it to embarrass, blackmail, or even smear the public images of the profile holders (Al Hasib, 2009). However, illegal secondary use is not within the scope of this article.

These technical advances can make individuals' information available to institutions and third parties (Raynes-Goldie, 2010; Young & Quan-Haase, 2013). A great deal of ethical dispute about privacy violations through data mining is related to issues such as discrimination, deindividualization, loss of autonomy, misuse of data, and the consequences of erroneous information (Custers, Calders, Schermer, & Zarsky, 2013; Hildebrandt, 2009; Tavani, 2013). The relationship between data miners and the user is occasionally referred to as a "one-sided affair," since users are often unaware of the methods by which their SNS data are processed and eventually used (Al-Saggaf & Islam, 2015; van Wel & Royakkers, 2004). If this is the case, what then are SNS users' thoughts and feelings concerning inferred information from their own disclosed data? This question must be explored by considering concepts of awareness and attitude, which will be addressed in the following section.

Privacy Awareness and Attitudes Toward Inferences Made Using SNSs

Privacy awareness relates to the extent to which users are knowledgeable of privacy problems and violations, as well as privacy procedures, related to SNSs (Nemec Zlatolas, Welzer, Heričko, & Hölbl, 2015). In relation to information-privacy-related issues caused by data mining on SNSs, Hugl (2011: 401) notes that "identity theft caused by profiling and data mining seems to be a current trend with exponential growth for advertising and other purposes." Additionally in this vein, Livingstone and Brake (2010) highlighted that one challenge for policymakers and researchers is the education of users, especially young ones, in new practices of embedded marketing, potential misuse of personal data, data mining, and profiling; they proposed that increased knowledge of new practices may positively influence their behavior in this regard. Education designed to provide an enhanced awareness of SNS privacy should involve knowledge concerning what and how data are stored on SNSs, how these data might be used, and who is likely to have access to it (Lawler & Molluzzo, 2010). Moreover, data mining might reveal something private such that a lack of awareness about it leads us to present ourselves on SNSs in a way that does not fit our self -understanding (Tavani, 2013). Thus, our study is also motivated by calls for further research into user awareness of SNS privacy, particularly in relation to data mining and inference programs (Hull, Lipford, & Latulipe, 2010; Shoemaker, 2010).

Privacy awareness affects people's behavior in a wide range of contexts. Awareness can provide user empowerment, but this is dependent on knowledge of how mechanisms operate and from what premise, as well as on the skills to change these mechanisms (van Dijck, 2013). For example, Tow, Dell, and Venable (2010) argued that it is possible to alter users' privacy-related behavior through education and raising awareness; they suggested that when users become aware of information about identity theft, the users consider altering their behavior. Following the theory of planned behavior, Ajzen (1991) suggests that behavioral intention, attitude, subjective norms, and perceived behavioral control reveal different aspects of the behavior, and each can serve as a point of attack in attempts to change it (Ajzen, 1991).

The study of *attitude* has been an important topic in privacy research for some time. An attitude is "an evaluative integration of cognitions and effects experienced in relation to an object" (Crano & Prislin, 2006, p. 347). Attitudes can involve both *affective* and *cognitive* components. The affective component contributes to the feeling-related aspect of an attitude, while the cognitive component involves the subject's rational reactions to the object of the attitude; both cognitive and affective reactions to information privacy are equally important for understanding individual reactions to privacy invasions (Choi et al., 2012; Park, Campbell, & Kwak, 2012). In information systems literature in general, and in SNS literature in particular, a large number of studies have been conducted on user attitudes toward directly sharing information on SNSs. Regarding the cognition aspect, one example is "privacy calculus," which relates to when individuals attempt to maximize the difference between the benefits and costs (Dinev & Hart, 2006). For the affective aspect, an example is a study by Debatin, Lovejoy, Horn, & Hughes (2009), which showed that privacy invasions create feelings of fear and anger, deterring the disclosure of personal information on SNSs. However, studies of attitudes toward inferred information from disclosed user data remain scant. While a small number of studies on secondary use exist (Adjei & Olesen, 2012; Boateng & Okoe, 2015; Iyilade, Orji, & Vassileva, 2015; Soczka, Brites, & Matos, 2015), they are focused on SNSs' practices of handling personal information.

We acknowledge that there are studies that argue for a dichotomy of information privacy attitudes and actual behavior, which is known as the "privacy paradox" (Norberg, Horne, & Horne, 2007). That stream of research has shown that while many users are concerned about their privacy and maintain a positive attitude toward privacy-protection behavior, this rarely translates into actual protective behavior (e.g., Hann et al., 2007; Oomen & Leenes, 2008; Taddicken, 2014). However, other studies indicate that an individual's privacy behavior is in line with their attitude (e.g., boyd & Hargittai, 2010; Miltgen & Peyrat-Guillard, 2014; Tsai, Egelman, Cranor, & Acquisti, 2011). The debate is not over, and the complexity of the privacy paradox has not been fully explained yet.

In an extensive literature review on the privacy paradox, Kokolakis (2017) made some recommendations that allow us to build a clearer picture of the relation between privacy attitudes and behavior. First is that personal information is diverse, and the privacy paradox may result from a failure to account for information sensitivity (Mothersbaugh, Foxx, Beatty, & Wang, 2012). In our research, we are only concerned with two types of personal information: SNS photos and textual posts. Therefore, our results should not be interpreted as applicable for all types of personal information.

Second is the methodological approach. Surveys rely on self-reported behavior, which often differs from actual behavior (Hughes-Roberts, 2013; Kokolakis, 2017). The dominant research on secondary use is based on surveys (Dinev & Hart, 2006; Ham, 2017; Kim & Huh, 2017; Son & Kim, 2008), while other papers have been largely based on researcher-centric preconceptions of privacy concerns, often slightly disconnected from users' own interpretations of privacy, for example, fictional case scenarios (Culnan, 1993; Krasnova, Hildebrand, & Guenther, 2009) and scenarios concerning real-world social-media data-mining activities (Kennedy, Elgesem, & Miguel, 2015). One factor that leads to the privacy paradox is the users' lack of awareness of possibilities to protect their privacy due to incomplete information about how institutions use or misuse their information (Barth & de Jong, 2017; Raynes-Goldie, 2010). Individual self-reports on privacy attitudes and behaviors cannot fully capture the phenomenon if privacy concerns are studied outside the actual context of the user's own SNS actions and experience. Therefore, research "should be conducted in realistic settings that provide a rich and relevant context" (Kokolakis, 2017, p. 132).

Finally, creating privacy awareness in combination with the availability of privacy enhancing tools that support users in their privacy decisions should help users to avoid paradoxical behavior (Deuker, 2009). While this study is concerned with attitudes and intention to disclose rather than privacy behavior, it should provide insights for further investigation into the relation between privacy behavior with privacy awareness and the availability of privacy-enhancing technologies as an under researched area (Barth & de Jong, 2017; Kokolakis, 2017).

In summary, our study aims to shed more light on the following knowledge gaps. First, despite recent emphasis on educating users about the potential secondary uses of information featured on SNSs (i.e., via SNS data mining) (Debatin et al., 2009; Hugl, 2011; Lawler & Molluzzo, 2010; Marwick & Hargittai, 2018), the literature does not address how such awareness might influence disclosure behavior. In this vein, attitude, as an antecedent factor of behavioral intention, requires exploration. The present study focuses on an in-depth investigation into raising awareness of SNS data mining and its effect on user attitudes toward these practices. Second, related information systems literature concerning secondary information use (Culnan, 1993; Hann et al., 2007; Krasnova, Günther, et al., 2009) has regarded the phenomenon as a single construct, without distinguishing directly disclosed information from inferences based on subsequent information processing; both aspects are important because direct and indirect information disclosures are affected by different privacy concerns (Min, 2016).

Genres of Disclosure

Altman (1975) defines privacy as a boundary-regulation process in which people optimize their accessibility along a spectrum of different spheres. Such boundary regulation is a dialectical and dynamic process in which an individual constantly chooses between revealing certain information to other people and keeping it from them. Palen and Dourish (2003) proposed that this dynamic process is fundamentally dependent on people having control over three boundaries concerning privacy management in the presence of information technology: disclosure, identity, and temporality; these can be explained as follows:

- The disclosure boundary addresses the tension between privacy and publicity. Following Altman's theory of privacy regulation, Palen and Dourish (2003) argue that people determine "what information might be disclosed under what circumstances, albeit with varying degrees of direct control." Living in the social world requires us to disclose public information concerning ourselves, such as our opinions, views, and actions. For example, a desire to present oneself via social media to the public while keeping a degree of privacy about certain aspects of self is determined via negotiation of the disclosure boundary. In this regard, the person allows themselves to negotiate their privacy in a public space.
- The identity boundary implies a tension between oneself and others. Not only are people's actions designed to benefit the self but information receivers are also distinguished from others and, thus, treated differently. For example, some argue that people's actions in public spaces (e.g., via security cameras) are already public and thus offer no threat to individual privacy. They fail to consider that we have very little control over representations of ourselves to the information receivers. Thus, the tension within the identity boundary does not refer to the identity of the person disclosing but rather to the one receiving, and how one's actions are interpretable to others.
- The temporal boundaries take place and form tensions among the past, present, and future. Our present actions may have impacts in the future; as such, the decision-making process concerning whether to disclose something is regarded in the context of actions taken in the past and their possible effects in the future. This boundary has become ever more relevant in the era of information technology. The storage and distribution of information has become simple and accessible to many; for example, incriminating photos of participation in drunken or embarrassing situations

that are shared while attending college might become troublesome later when seeking a job.

These three boundaries must have a coordinated and single coherent resolution within a context, that is, a specific time and place, the receiver, and content that can be concealed. The balance of these three boundaries forms a communicative action, which Palen and Dourish (2003) conceptualized as the *genres of disclosure*, or specifically as the "socially constructed patterns of privacy management." Further, they (p. 6) characterize a genre of disclosure as "the relationship between *forms of disclosure* and *expectations of appropriate use*." Central to the concept of the genres of disclosure is the adoption of the social patterns of expectation and response as recognizable, socially relevant forms of interaction and information disclosure that genres embody. Upon the moment of disclosure, for example, on an SNS, an individual must be able to find a balance between the above-mentioned boundaries. A decision on whether to disclose something or to limit the depth and breadth of the shared information can thus be characterized by the genre of disclosure that the user wishes to apply. However, problems can arise when users adhere to a genre while unaware of the danger that personal information can potentially be misappropriated after it is stored by an SNS. For example, if a user is made aware that by posting comment X on Facebook, it could be inferred that he or she is a cannabis smoker or if it reveals something about their other more or less sensitive habits, it could well impact communicative decisions at present or in the future. We employed this theoretical framework in this study to uncover underlying relationships between inferred information from SNS data over disclosure and consequently on attitudes toward further disclosure.

Methodology

In this study, exploratory focus groups were created with the goal of capturing participants' attitudes toward online disclosure once they had been exposed to potential inferences from their Facebook posts. Since users' perspectives of potential inferences from information on SNSs is a relatively under researched area, we opted for an exploratory study. The next section introduces the DataBait tool and describes our focus group data-collection and analysis process.

DataBait Tool

The DataBait[1] tool was developed in the USEMP[2] project. The USEMP architecture, platform, and tools aim to provide instruments that empower users of SNSs to have more informed control over their data and to understand how the data may be used by SNS providers and third parties. DataBait tools enhance users' awareness of personal-data sharing and privacy management (Popescu et al., 2016). For this project, Facebook was chosen as the representative SNS.

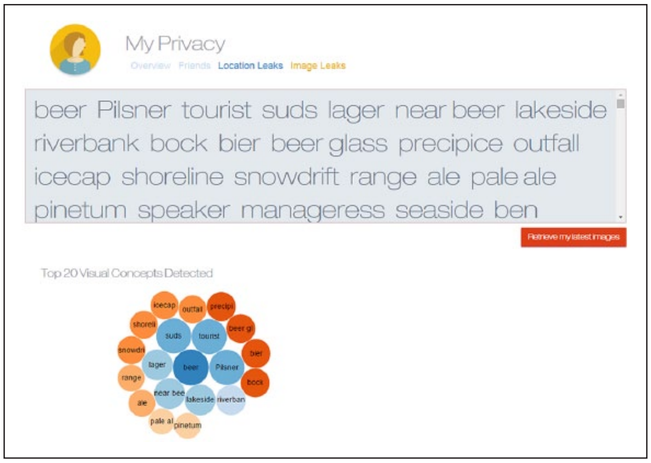

My Privacy
Overview
Friends
Location Leaks
Image Leaks
beer Pilsner tourist suds lager near beer lakeside riverbank bock bier beer glass precipice outfall icecap shoreline snowdrift range ale pale ale pinetum speaker manageress seaside ben
Retrieve my latest images
Top 20 Visual Concepts Detected
icecap
outfall
precipi
shoreli
suds
tourist
beer gl
snowdri
bier
lager
beer
Pilsner
range
bock
near bee
lakeside
riverban
ale
pale al
pinetum

Figure 1. A concept cloud retrieved from a Facebook user's uploaded/shared images.

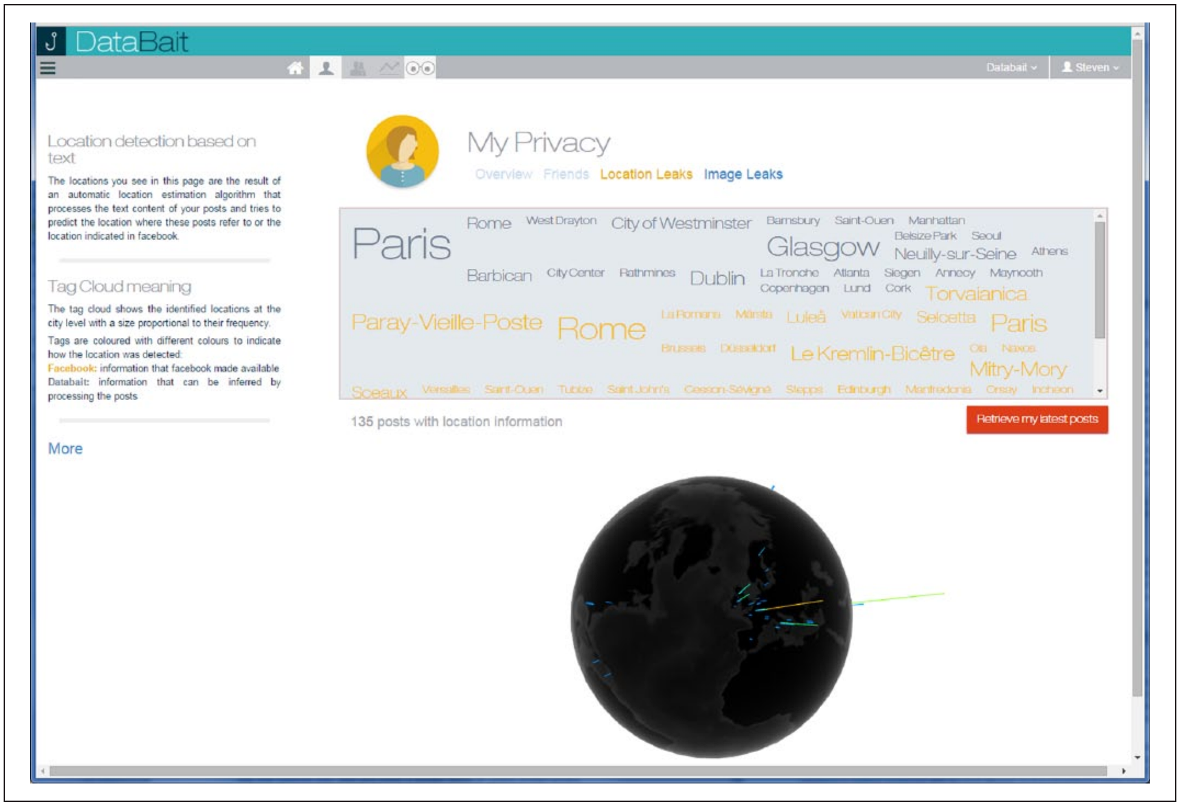
Once a user registers with DataBait and links it to his or her Facebook account, DataBait performs extraction and classification of their personal data using advanced data mining algorithms. We note that these inferences do not necessarily coincide with the inferences made by SNS providers or third parties, but instead provide an overview of inferences that *could* be made and used to target or exclude a user. In this study, two DataBait functionalities were used to illustrate user privacy inferences: Image Leaks and Location Leaks.

Image Leaks/Visual Concept Mining provides the user with the list of concepts that can be inferred from the images the user has uploaded or shared with others on Facebook. DataBait predicts tags from a set of over 17,000 visual concepts relating to objects present in a scene or the general atmosphere perceived (Ginsca et al., 2015). This tag cloud is then visually presented by showing the identified concepts in sizes proportional to the frequency with which they appear in the posted SNS images; if the user clicks a concept, the images in which this concept has been detected are shown, along with a measure of confidence in the accuracy of the detection (Figure 1).

Location Leaks/Prediction gives the user a list of locations that can be inferred from the posts. The detected locations are produced by an automatic location-estimation algorithm that processes the text content of Facebook posts and predicts locations referred to or indicated by the user. The tag cloud shows the identified locations at the city level with a size proportional to their frequency. If the user selects a location, the posts in which this location has been detected are shown, along with a measure of confidence in the accuracy of the detection (Figure 2).

Focus Groups

The focus group method involves identifying and clarifying emerging concepts through group discussion (Belanger,



Location detection based on text

The locations you see in this page are the result of an automatic location estimation algorithm that processes the text content of your posts and tries to predict the location where these posts refer to or the location indicated in facebook.

Tag Cloud meaning

The tag cloud shows the identified locations at the city level with a size proportional to their frequency.

Tags are coloured with different colours to indicate how the location was detected:
Facebook: information that facebook made available
Databait: information that can be inferred by processing the posts

135 posts with location information

Figure 2. The displayed places indicate the locations that were extracted from the user's posts.

2012; Edmunds, 2000). This method also facilitates the observation of changes in attitudes (if any) by analyzing the "synergistic effects" of focused interactions, which can provide greater insights than the sum of individual interviews (Morgan, 1996).

Procedure and Data Collection. Our empirical data stems from two sub-studies. In the first sub-study, illustrative mock-ups of the DataBait tool were introduced, while in the second sub-study, the participants were encouraged to test and experiment with the tool on their own Facebook profiles. The first sub-study was performed in February and March 2015, and consisted of three focus group sessions with twelve participants in total. In the second sub-study, conducted in August 2015, three sessions featuring fifteen participants (different than the first sub-study) were performed. Data were gathered in English, on a university campus. The participants volunteered for the study via a Living Lab and by responding to invitations made to students and employees of our university. After receiving an initial expression of interest and analyzing the candidate profiles, a mixture of participants in terms of occupation (13 students, 14 non-students), educational background (5 from high school, 11 from BA, and 11 from MA level), gender (15 male, 12 female), cultural background (14 Swedish, 13 non-Swedish), and age (from 18 to 58 years old) were invited. The reason for selecting a panel of people with varying backgrounds was to decrease bias imposed by a specific demographics as well as to incorporate as much diversity in terms of experiences as possible (Bouma, Atkinson, & Dixon, 1995).

A semi-structured interview guide consisting of both open-ended and specific questions was created. The questions were piloted internally within the research team in order to determine if they were readily understandable. To stimulate discussion in the group, the notion of *genres of disclosure* (Palen & Dourish, 2003) was employed to capture users' disclosures and to account for situations of potential privacy violations; that is, if potential use differs from expectations (e.g., inferences made from one's private photos), privacy violations occur. Thus, the two notions of "forms of disclosure" and "expectation of use" were used to design the focus group protocol.

Each focus group session took, on average, 100 minutes. To ensure that all participants had an appropriate base understanding of the topic, all participants of Sub-study 1 were familiarized with the concept of data mining and inferences from personal information. As this point, the participants were free to raise and discuss issues and concepts that they regarded to be most important, with minimum influence from the moderator in order to maintain the credibility of the study (Lincoln & Guba, 1985). This was followed by a general discussion concerning the group members' use of social media, the types of information they disclose, and privacy concerns related to social media. This phase counted as attitudes *before* being

Table 1. Attitudes Toward Inferred Information from SNSs.

Attitude	General awareness concerning inference mechanisms (Sub-study 1)	Awareness of personal disclosures as a result of using the DataBait tool (Sub-study 2)
Affective	Interested—scared—shocked—unsure if tool is beneficial—feeling of being watched -suspicious—afraid—boring-endangered—unlike	Interesting—concerning—scary
Cognitive	Self-awareness is adequate; reliance on own ability to control direct information disclosure—alerted to being profiled—what others know about me—cautious—restrictive—resistance toward tool use	Increased understanding of the potential for inferences—what others know about me—avoid unwanted disclosure—cautiousness—avoid unwanted inferences—clearer idea of the commercialization of content—unintended disclosure—wrongly profiled—being profiled—assertion through inferences—manipulation of online presence—noting others' privacy—alarming

SNSs: social network sites.

exposed to potential inferences, during which the *cognitive* and *affective* aspects of the participants' attitudes were recorded. Participant awareness in regard to indirect information-sharing was examined by gathering insights into the personal information they think they reveal through Facebook. The focus was on why participants share their locations and/or photos and the impact the *expected level of privacy* has on their shares. A brief introduction of the DataBait tool followed. In this segment, participants were shown screenshots of the tool's interface and results, but there was no active interaction with the tool in terms of their own data. Finally, a group discussion took place that focused on attitudes toward inferred information and its effects on the participants' private information disclosures. This phase counted as *after*, as it involved gathering data concerning *affective* and *cognitive* aspects of participant attitudes. Additionally, the impacts of *awareness* on possible inferences of personal information and attitudes toward future *disclosure* were also examined.

In Sub-study 2, the participants were able to compare their intended privacy preferences with DataBait's results for the actual photos and/or locations they shared. The design of this workshop was identical to that of Sub-study 1, with the exception that participants used the DataBait tool on their own profiles. First, the participants discussed their attitudes toward photo- and location-sharing and then used the tool to analyze their Facebook profile. The tool visualized possible inferences that could be made in terms of predicting their locations and extracted concepts from their photos (similar to the features presented in Figures 1 and 2). After receiving the potential inferences, participants reflected on how close the results were to their initial expectations. The focus group concluded with a discussion on attitudes toward inferred information and its effects on their information disclosure. Experience with data mining helped us to address the study's research question on whether and how contextualization differs from the case in which only mock-ups are presented, as in the first sub-study. In this regard, two sub-studies allowed us to explore perceived disclosure intention in relation to users' understanding of potential inferences when they were only told these inferences versus experimented to discover them.

Data Analysis. All six sessions were transcribed from audio recordings. We used qualitative content analysis and performed deductive categorization of the data (Mayring, 2000). The researchers determined the initial coding scheme by basing it on identified core concepts; specifically, these core concepts included disclosure, identity, and temporal boundaries, as well as affective and cognitive attitudes both before and after the presentation and usage of the tool. After this, sub-categories of the core concepts were identified by following the principles of inductive content analysis (Elo & Kyngäs, 2008). The final sub-categories extracted are those stated in Table 1 in the rows labeled as affective and cognitive. Three researchers were involved in the data analysis. For the first step in this process, the authors each coded 15% of the entire transcription independently using the qualitative data analysis software NVivo. The second step in the analysis was to develop a common view of the main themes and acquire a shared understanding; as such, all categories were iteratively discussed within the research group. Third, after a consensus was reached among the researchers, the rest of the transcription was analyzed by the first author; therefore, when uncertainties arose, all authors read the relevant section of the transcript and discussed it to ensure a high level of credibility in the analysis.

Findings and Discussion

The qualitative analysis showed that the DataBait tool helped users to better understand the potential consequences of their SNS disclosure practices. This became evident when comparing the first sub-study with the second: the participants became more cognitive toward their genres of disclosure through extra awareness of the three boundaries (disclosure, identity, and temporality).

Disclosure Boundaries

Sub-study 1 participants, after witnessing screenshots from the DataBait tool (Figures 1 and 2), made affective responses to possible disclosures; for example, stating that they were scared or shocked. These affective responses were not only shown in words but also through facial expressions. They became interested in the tool, but they had doubts if the results concerning their own data would highlight serious problems. In fact, they were rather confident in their own disclosure habits and saw no reason to deviate from their normal disclosure habits because they were sure that nothing out of the ordinary could be inferred from the material they were sharing. For example, Mary (49)[3] had doubts if she would use the DataBait tool in the future:

> *I think if I do use it I will use it only like once to analyze something on my profile and then forget about it; I don't want to have it telling me all the time be careful of this and that, I prefer to do that kind of analysis myself. I will use it to scan my profile only once.*

While Sub-study 1 participants were confident that their privacy was under control, the second sub-study provided the participants with further enlightenment concerning the potential undesired disclosure. The second sub-study encouraged them to speculate more cognitively (rather than affectively) upon aspects of their profile; the study also stimulated them to speculate cognitively about private information that others could potentially discern concerning them.

During the second sub-study, a tool-based misinterpretation in the inferences led to the realization among participants that their personal information could be misinterpreted by third parties. A small number of detected concepts in photos and locations of two participants were inaccurate and arguable; for example, the visual concept "gun" emerged by mistake:

> *Some bad words were shown, but when I clicked on them they weren't accurate. So, like it gave the word "gun," but the picture showed a camera, so now I think I should maybe erase those pictures . . . (all laughing). (Tina, 25)*

Users manage their disclosures depending on the level of privacy of the information in question and the level of publicity associated with the communication channel (Masur & Scharkow, 2016). In the present case, when confronted with possible interpretations of their personal disclosed information, the participants realized that inferences could be made in relation to their more private information. The discovery that certain information could potentially be inferred impacts disclosure decisions. Users may make disclosures, such as posting photos, assuming that there are no private elements featured in the photo (Krasnova, Günther, et al., 2009), but without being concretely exposed to potential analyses revealing *disclosure boundaries* (such as by using the DataBait tool), they can only imagine or guess how private or public a photo will be. Thus, users' cognitive abilities often trail technological advances. Consequently, users require assistance in terms of determining if their disclosures are truly aligned with their socially constructed and self-regulatory privacy practices.

Identity Boundaries

All the participants said they thought of their audience when they shared something, and they stated that their decisions to share certain content depended on its expected audience. The participants constantly mentioned "they" in relation to who performs data mining without possessing a clear idea of who *they* actually are, indicating a sense of ambiguity with regard to potential audiences, such as SNS owners, affiliated third parties, third-party applications, advertisers, governments, and criminals. In Sub-study 1, the participants stated that they relied on privacy settings in Facebook, although they were skeptical that the settings were effective:

> *I guess some private settings are good, but then when you really think about it, it just, it feels like they are tricking everyone with the privacy settings to let us think that is ok, that it is safe to use Facebook. (Nancy, 25)*

In the second sub-study, the DataBait tool gave the participants a better idea of the potential inferences that can be construed from photos and locations. Consequently, some expressed shock and fear, as if this information was completely new to them. Others noticed that their privacy-related behavior affected that of other users; examples of this involved posting photos that featured other persons or being tagged in photos from a friend's album. The participants found that some concepts highlighted through the DataBait experimentation were more related to other individuals featured within their photos than to themselves. This finding alerted them to a new genre of unwanted disclosures:

> *Now that I see them [inferences], it makes me think about the people with me in the pictures and about their privacy as well. I don't usually give much thought to what could be interpreted from the other people with me in the picture, but this photo shows my best friend, who is from Egypt and who is wearing a veil, and I see a lot of Muslim references in the tags, so I think that the inference is accurate and describes my friends. (Aida, 27)*

It can be seen here that data mining can lead to undesirable third-party discoveries concerning people. Palen and Dourish (2003) problematize this tension using the phenomenon of "recipient design," "the way that one's actions and utterances are designed with respect to specific others" (p. 4), but with secondary use, people may have difficulty filtering the disclosed information for unintended audiences. Inferences of photos and locations in Sub-study 2 helped users realize that some of the inferences were related to others appearing in their profiles and that the privacy of members in a network is interwoven (Litt & Hargittai, 2016). Each category of inferred information has its own intended beneficiary; for example, Facebook has made agreements with data brokers that provide conceptual categories to ad buyers. Possible recipients of inferred sensitive information or extracted attributes are largely hidden from SNS users as a result of a lack of transparency, and this exacerbates user concerns. Consequently, people need to be in control of their indirect disclosures in addition to their direct disclosures (Tavani, 2013).

Temporal Boundaries

Before using DataBait, when asked about information visible on their profiles, many participants mentioned having deleted something they had shared in the past because they recently felt it was inappropriate. However, some felt powerless about their ability to remove previous disclosures. Salman and Edi believed that information posted on Facebook can sometimes be hard to control and, once posted, difficult to erase:

> *Edi (23):* *It is scary, because if you upload something, you don't own it anymore, the Internet owns it. You can never get it back.*
>
> *Salman (32):* *Yeah, that is true, and it is also somewhat troubling that Facebook has changed its privacy settings so many times. They are changing the data flow, and even though you delete something from your Facebook news feed, it is still going to be there [. . .] so you don't really own it as such, even though you try to delete it, the traces are still there. (Sub-study 1)*

When participants were confronted with potential inferences from their content (related to, e.g., religion or employment), they stated that they would like to have a clearer picture of how data disclosed in the past can be used for profiling; consequently, the DataBait tool was used to show how photos and status updates contribute to creating a digital dossier (Gross & Acquisti, 2005). Trends found in photos as well as locations associated with status updates were found to enrich such predictions, which conforms with the findings of previous research (Kosinski et al., 2013). Shoemaker (2010) argues that patterning pieces of information provided by a user which, when considered separately, might not implicate one's identity, nonetheless purport to provide substantial information about the person in question when taken together; our results similarly showed that when concepts are consistently included in photos uploaded from the time when the profile was created to the most recent shares, many personality dimensions can be predicted; moreover, if the inferences are incorrect, this can cause embarrassment or shame for the affected person. Our results also showed that if photos are mined out of context and aggregated over time, potentially incorrect attributes could be attached to users; this bothered the participants, consequently blurring the *temporal boundary* of intended disclosure.

Increased Awareness of Potential Inferences Changes User Attitudes

By comparing attitudes between the two sub-studies (Table 1), the results suggest that users' attitudes are more inclined to be affective rather than cognitive if they cannot directly see the possibilities of secondary disclosure. Participants from Sub-study 1, after increasing their awareness about information that can be inferred from profile photos and status updates, made affective responses to the possible inferences, including expressions of fear, suspicion, shock, and the need to be more cautious. However, Sub-study 2 provided contradictory insights. After experimentation with the tool, the participants' attitude had become more cognitive, demonstrating clearer ideas of how their information could be utilized for different purposes (e.g., commercial). Sub-study 2 showed that users now realized how their photos and location shares were actually prone to inferences beyond their initial sharing purposes. For example, one participant found that many military concepts were present in his analysis; this was because he had shared photos of himself wearing a military uniform while he was fulfilling his military service in his own country. However, he became concerned that others could interpret this differently, which could impact his career in another country:

> *The information that presented [by DataBait] is surprisingly accurate, more accurate than I thought it would be . . . this can also be used in the future by a company, for example, to look you up and see what kind of person you are, which is a little freaky in a sense. (Roland, 23)*

Table 2 summarizes the results of the two workshops with respect to boundaries of genres of disclosure. This is presented in terms of the participants' awareness of possible inferences after the issue had merely been demonstrated and discussed (Sub-study 1) in comparison to their opinions after the performance of experiments with participants' own information (Sub-study 2).

Users may be unable to recognize how advances in technology can alter previous public and private boundaries in terms of *genres of disclosure relating to SNSs* because the form of disclosure was not always aligned with the expectation of use. This was evident in the initial negative *affective*-oriented responses that the end users gave as the result of their low level of awareness concerning indirect information-sharing; if such awareness is limited, spontaneously evoked affective reactions rather than cognitions tend to have a greater impact on choice (Shiv & Fedorikhin, 1999). On the other hand, all cognitive theories suggest that a cognitive process occurs before a behavior is undertaken or a choice is made (Hann et al., 2007); hence, a lack of awareness of inferred information for a cognitive process regarding boundaries related to disclosure genres will lead to a privacy violation within a disclosure genre because the disclosure will not be aligned with the expected use (Palen & Dourish, 2003). Depending on the inferred information and the expectations of the user in question, the form of disclosure is subject to change. However, there is uncertainty surrounding the arrangements of those inferences; therefore, means of developing *cognitive awareness* are required in order to strengthen the decisions a user makes with respect to their genre of disclosure. Consequently, the findings herein suggest that when users are actively made more aware of potential

Table 2. Boundaries in Genres of Disclosure in Relation to the Two Sub-studies.

Boundaries	General awareness concerning inference mechanisms (Sub-study 1)	Awareness of personal disclosures as a result of using the DataBait tool (Sub-study 2)
Disclosure	• Perceived control of own disclosures	• Inferences are considered to be too private • Tool-oriented errors in inferences could affect privacy
Identity	• Ambiguity in regard to potential audiences beyond primary target users • Trust in audience settings on SNSs	• Increased awareness of potential audiences as a result of secondary use • One's disclosures could influence the privacy of others and vice versa
Temporal	• General awareness that past/current actions will have consequences in the future; lack of clarity in regard to such consequences	• Tracking over time becomes more visible • All shared data contributes to digital profiling • Past content could become undesired

SNSs: social network sites.

inferences that can be made from their disclosure genres, their attitudes about disclosure change.

Implications for Research and Practice

Our findings have implications in terms of both methodology and research. With regard to its *methodological contribution*, this research complements previous approaches in which informants were exposed to imaginary or speculative scenarios relating to the secondary use of disclosed information. The results especially contribute to the privacy paradox dispute by showing that attitude and intention to disclose change with context because common preconceptions do not seem to equip most users with sufficient critical knowledge in this regard. To give an example of this contribution, there can be many different interpretations of personal content that end users might not be aware of at the time they answer questions in surveys or case scenarios; thus, future research should not rely solely on a user's self-reporting attitude (Kokolakis, 2017). Moreover, individuals react and behave differently based on the sensitivity of their information; and therefore, privacy behavior is context-dependent (Acquisti et al., 2015). In contrast to previous research (e.g., Kennedy et al., 2015; Krasnova et al., 2009; Marwick & Hargittai, 2018) that studied privacy attitudes from a holistic view (i.e., not considering the granularity of personal information), this research sheds more light on the attitudes towards indirect disclosure through two specific information types, namely, photos and posts. The results suggest that inferred information from SNS user data (photos and posts) disrupts boundaries within the genres of disclosure. While our intention was not to study privacy behavior, the results from Sub-study 2 were promising with regard to the effects of contextualization of possible inferred information on the intentions to disclose. Further research might investigate how contextualization affects actual disclosure.

Second, this research showed that direct use of user data and information that is inferred from user data must be distinguished when studying secondary use on SNSs. Previous research on secondary use has considered it to be a single construct that, from a user's point of view, is either understood as direct use, inferred, or both. In either case, this single construct cannot adequately explain a user's choice of disclosure genre since both types of information use are governed by different types of privacy concerns and therefore by different attitudes. While behavioral reactions including disclosure are associated with privacy concerns (Min, 2016; Smith, Dinev, & Xu, 2011), different privacy concerns about direct data use and inferred information influence behavioral intentions to different extents. Therefore, our research suggests that secondary use is not a single construct but a composition of direct and inferred constructs. If users recognize the differences between both forms of disclosure, the research will yield a more accurate understanding of users' attitudes and privacy behavior.

Regarding practical implications, this research reinforces the established value orientation that posits users should be dynamically educated about their own disclosures and that methods of increasing their awareness and ability to use this knowledge to behave accordingly should be sought (Hugl, 2011; Lawler & Molluzzo, 2010; Marwick & Hargittai, 2018). SNS researchers must focus to a greater extent on changing user attitudes toward inference mechanisms. It has been proposed that cognition determines affect, which ultimately influences behavior (Holbrook & Batra, 1987; Parboteeah, Valacich, & Wells, 2009); based on our results, we speculate that negative affective reactions to secondary use could be minimized via cognitive deliberation and that this shift can be implemented via privacy-enhancing tools (Barth & de Jong, 2017; Deuker, 2009). Despite the danger to privacy that data-mining presents, the technique can be utilized for developing educational tools for SNS users. As in our case, these tools can help to make users aware of their disclosure genres. One possible track for future practice is to create SNS-privacy-enhancing tools that analyze content in order to inform users before the content is shared on SNSs about possible indirect disclosures that can be made through inference mechanisms. In this way, users can prevent the sharing of sensitive information.

Study Limitations

Focus groups may be generally prone to group effects and participants' attitudes may change with the circumstances of the focus groups; therefore, follow-up interviews would give a better understanding of such changes in attitude. Moreover, the current study was conducted during 2015, and individuals' privacy awareness could have evolved in light of recent events concerning Facebook and Cambridge Analytica in 2018. To the best of our knowledge, the DataBait tool was the first tool made available that allowed users to experiment with data mining in SNSs, and we believe that the findings reported here are important and make a valuable contribution to directing future research. Additional studies are expected to provide more insights on the potential discrepancy between individuals' privacy attitudes and awareness from 2015 to 2018 in the light of recent discussions about behavioral profiling and the misuse of data.

Conclusion

This paper reported a study of privacy awareness in relation to sharing personal information on social network sites. In this study, users of such networks were made aware of inferences that could be drawn from the personal information they post with the help of privacy-enhancing software. It was consequently found that participant attitudes on privacy and disclosure shifted from affective to cognitive when they experienced first-hand the potential inferences that could be made from their own data. It was also observed that user preawareness of the potential for indirect personal information disclosure was relatively low. Initially, the participating users only considered their direct disclosure of information; by observing potential inferences, however, the participants became more aware of potential impacts on their privacy. The results showed that if users are made aware of inferences that can be made from their content, negative affective responses decrease and cognitive reactions increase through the processing of information related to their disclosure genres. In support of the suggestion from cognitive theories that a cognitive process occurs before a behavior is undertaken or a choice is made, we conclude by stating that there is a need for more dynamic privacy awareness tools that can empower users by providing them with increased awareness of the inferences that could be made from the information they are sharing. Such tools should help users become dynamically aware of the potential privacy consequences of their intended disclosures before they disclose the information on an SNS. When armed with such tools, users will be able to view their own information from different angles and become aware of the situations when the expectation of disclosing actions is violated. Furthermore, the usability, user experience, adoption and availability aspects of such tools that employ data mining techniques form an avenue for future research that is worth exploring.

Authors' Note

Tero Päivärinta is also affiliated with University of Oulu, Finland.

Declaration of Conflicting Interests

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was funded by the European Commission in the context of the Horizon 2020 project U4IoT (Grant Agreement No. 732078) and the FP7 project USEMP (Grant Agreement No. 611596).

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Notes

1. For a detailed overview of the tool, see Popescu et al. (2016).
2. Full title: "User Empowerment for Enhanced Online Presence Management".
3. Names of the participants have been pseudonymized. The number in front of the names corresponds to the participant's age.

ORCID iD

Ali Padyab https://orcid.org/0000-0002-5286-4850

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*, 509–514. doi:10.1126/science.aaa1465

Adjei, J. K., & Olesen, H. (2012). Secondary uses of personal identity information: Policies, technologies and regulatory framework. *Communications & Strategies*, *1*, 79–98.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*, 179–211.

Al Hasib, A. (2009). Threats of online social networks. *International Journal of Computer Science and Network Solutions*, *9*, 288–293.

Al-Saggaf, Y., & Islam, M. Z. (2015). Data mining and privacy of social network sites' users: Implications of the data mining problem. *Science and Engineering Ethics*, *21*, 941–966. doi:10.1007/s11948-014-9564-6

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, crowding*. Monterey, CA: Brooks/Cole Pub.

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox—Investigating discrepancies between expressed privacy concerns and actual online behavior—A systematic literature review. *Telematics and Informatics*, *34*, 1038–1058. doi:10.1016/j.tele.2017.04.013

Belanger, F. (2012). Theorizing in information systems research using focus groups. *Australasian Journal of Information Systems*, *17*, 109–135.

Boateng, H., & Okoe, A. F. (2015). Consumers' attitude towards social media advertising and their behavioural response: The moderating role of corporate reputation. *Journal of Research in Interactive Marketing*, *9*, 299–312. doi:10.1108/JRIM-01-2015-0012

Bouma, G. D., Atkinson, G. B. J., & Dixon, B. R. (1995). *A handbook of social science research*. Oxford, UK: Oxford University Press.

boyd, d., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, *13*, 210–230. doi:10.1111/j.1083-6101.2007.00393.x

boyd, d., & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday*, *15*(8). doi:10.5210/fm.v15i8.3086

Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). How Cambridge analytica turned Facebook "likes" into a lucrative political tool. *The Guardian*. Retrieved from http://www.the-guardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm

Choi, B. C. F., Jiang, Z., & Yap, E. (2012). Information sharing in online dyadic exchange: A relational dialectic perspective. In R. H. J. Sprague (Ed.), *2012 45th Hawaii International Conference on System Science* (HICSS, pp. 743–752). Maui, HI: IEEE. doi:10.1109/HICSS.2012.324

Crano, W. D., & Prislin, R. (2006). Attitudes and persuasion. *Annual Review of Psychology*, *57*, 345–374. doi:10.1146/annurev.psych.57.102904.190034

Culnan, M. J. (1993). "How did they get my name?": An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly*, *17*, 341–363. doi:10.2307/249775

Culnan, M. J. (1995). Consumer awareness of name removal procedures: Implications for direct marketing. *Journal of Direct Marketing*, *9*, 10–19. doi:10.1002/dir.4000090204

Custers, B., Calders, T., Schermer, B., & Zarsky, T. (Eds.) (2013). *Discrimination and privacy in the information society* (Vol. 3). Berlin, Germany: Springer. doi:10.1007/978-3-642-30487-3

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, *15*, 83–108. doi:10.1111/j.1083-6101.2009.01494.x

Deuker, A. (2009). Addressing the privacy paradox by expanded privacy awareness—The example of context-aware services. In M. Bezzi, P. Duquenoy, S. Fischer-Hübner, M. Hansen, & G. Zhang (Eds.), *Privacy and identity management for life* (pp. 275–283). Berlin, Germany: Springer. doi:10.1007/978-3-642-14282-6_23

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-Commerce transactions. *Information Systems Research*, *17*, 61–80. doi:10.1287/isre.1060.0080

Edmunds, H. (2000). *Focus group research handbook*. Lincolnwood, IL: McGraw-Hill.

Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of Advanced Nursing*, *62*, 107–115. doi:10.1111/j.1365-2648.2007.04569.x

Fuchs, C. (2013). *Social media: A critical introduction*. London, England: SAGE.

General Data Protection Regulation. (2016). *European parliament and the council of the European Union*. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection_en

Ginsca, A. L., Popescu, A., Borgne, H. L., Ballas, N., Vo, P., & Kanellos, I. (2015). Large-scale image mining with Flickr groups. In X. He, S. Luo, D. Tao, C. Xu, J. Yang, & M. A. Hasan (Eds.), *Multimedia modeling* (pp. 318–334). Cham, Switzerland: Springer. doi:10.1007/978-3-319-14445-0_28

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society* (pp. 71–80). New York, NY: ACM. doi:10.1145/1102199.1102214

Ham, C.-D. (2017). Exploring how consumers cope with online behavioral advertising. *International Journal of Advertising*, *36*, 632–658. doi:10.1080/02650487.2016.1239878

Hann, I.-H., Hui, K.-L., Lee, S.-Y. T., & Png, I. P. L. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems*, *24*, 13–42. doi:10.2753/MIS0742-1222240202

Hildebrandt, M. (2009). Who is profiling who? Invisible visibility. In S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne, & S. Nouwt (Eds.), *Reinventing data protection?* (pp. 239–252). Dordrecht, The Netherlands: Springer. doi:10.1007/978-1-4020-9498-9_14

Holbrook, M. B., & Batra, R. (1987). Assessing the role of emotions as mediators of consumer responses to advertising. *Journal of Consumer Research*, *14*, 404–420.

Hughes-Roberts, T. (2013). Privacy and social networks: Is concern a valid indicator of intention and behaviour? In 2013 International Conference on Social Computing (Socialcom, pp. 909–912). doi:10.1109/SocialCom.2013.140

Hugl, U. (2011). Reviewing person's value of privacy of online social networking. *Internet Research*, *21*, 384–407. doi:10.1108/10662241111158290

Hull, G., Lipford, H. R., & Latulipe, C. (2010). Contextual gaps: Privacy issues on Facebook. *Ethics and Information Technology*, *13*, 289–302. doi:10.1007/s10676-010-9224-8

Iyilade, J., Orji, R., & Vassileva, J. (2015). Factors influencing user's attitude to secondary information sharing and usage. *Journal of Computing and Information Technology*, *23*, 231–244.

Kennedy, H., Elgesem, D., & Miguel, C. (2015). On fairness: User perspectives on social media data mining. *Convergence: The International Journal of Research into New Media Technologies*, *23*, 270–288. doi:10.1177/1354856515592507

Kim, H., & Huh, J. (2017). Perceived relevance and privacy concern regarding online behavioral advertising (OBA) and their role in consumer responses. *Journal of Current Issues & Research in Advertising*, *38*, 92–105. doi:10.1080/10641734.2016.1233157

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. doi:10.1016/j.cose.2015.07.002

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences of the United States of America*, *110*, 5802–5805. doi:10.1073/pnas.1218772110

Krasnova, H., Günther, O., Spiekermann, S., & Koroleva, K. (2009). Privacy concerns and identity in online social networks. *Identity in the Information Society*, *2*, 39–63. doi:10.1007/s12394-009-0019-1

Krasnova, H., Hildebrand, T., & Guenther, O. (2009). Investigating the value of privacy in online social networks: Conjoint analysis. In *Proceedings of the 30th International Conference on Information Systems* (ICIS 2009, p. 173). Phoenix, AZ. Retrieved from https://boris.unibe.ch/47455/1/Boris3.pdf

Lawler, J. P., & Molluzzo, J. C. (2010). A study of the perceptions of students on privacy and security on social networking sites (SNS) on the internet. *Journal of Information Systems Applied Research*, *3*, 3–18.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Thousand Oaks, CA: SAGE.

Litt, E., & Hargittai, E. (2016). The imagined audience on social network sites. *Social Media + Society*, *2*(1), 1–12. doi:10.1177/2056305116633482

Livingstone, S., & Brake, D. R. (2010). On the rapid rise of social networking sites: New findings and policy implications. *Children & Society*, *24*, 75–83. doi:10.1111/j.1099-0860.2009.00243.x

Marwick, A., & Hargittai, E. (2018). Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online. *Information, Communication & Society*, 1–17. Advance online publication. doi:10.1080/1369118X.2018.1450432

Masur, P. K., & Scharkow, M. (2016). Disclosure management on social network sites: Individual privacy perceptions and user-directed privacy strategies. *Social Media + Society*, *2*(1), 1–13. doi:10.1177/2056305116634368

Mayring, P. (2000). Qualitative content analysis—Research instrument or mode of interpretation? In M. Kiegelmann (Ed.), *The role of the researcher in qualitative psychology* (pp. 139–148). Tübingen, Germany: Huber.

Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *European Journal of Information Systems*, *23*, 103–125. doi:10.1057/ejis.2013.17

Min, J. (2016). Personal information concerns and provision in social network sites: Interplay between secure preservation and true presentation. *Journal of the Association for Information Science and Technology*, *67*, 26–42. doi:10.1002/asi.23376

Morgan, D. L. (1996). Focus groups. *Annual Review of Sociology*, *22*, 129–152.

Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., & Wang, S. (2012). Disclosure antecedents in an online service context: The role of sensitivity of information. *Journal of Service Research*, *15*, 76–98. doi:10.1177/1094670511424924

Narayanan, A., & Shmatikov, V. (2009). De-anonymizing social networks. In *2009 30th IEEE Symposium on Security and Privacy* (pp. 173–187). Berkeley, CA: IEEE. doi:10.1109/SP.2009.22

Nemec Zlatolas, L., Welzer, T., Heričko, M., & Hölbl, M. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. *Computers in Human Behavior*, *45*, 158–167. doi:10.1016/j.chb.2014.12.012

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*, 100–126. doi:10.1111/j.1745-6606.2006.00070.x

Oomen, I., & Leenes, R. (2008). Privacy risk perceptions and privacy protection strategies. In E. de Leeuw, S. Fischer-Hübner, J. Tseng, & J. Borking (Eds.), *Policies and research in identity management* (pp. 121–138). Boston, MA: Springer. doi:10.1007/978-0-387-77996-6_10

Orito, Y., Fukuta, Y., & Murata, K. (2014). I will continue to use this nonetheless: Social media survive users' privacy concerns. *International Journal of Virtual Worlds and Human Computer Interaction*, *2*, 92–107. doi:10.11159/vwhci.2014.010

Palen, L., & Dourish, P. (2003). Unpacking privacy for a networked world. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 129–136). New York, NY: ACM. doi:10.1145/642611.642635

Parboteeah, D. V., Valacich, J. S., & Wells, J. D. (2009). The influence of website characteristics on a consumer's urge to buy impulsively. *Information Systems Research*, *20*, 60–78. doi:10.1287/isre.1070.0157

Park, Y. J., Campbell, S. W., & Kwak, N. (2012). Affect, cognition and reward: Predictors of privacy protection online. *Computers in Human Behavior, 28*(3), 1019–1027. doi:10.1016/j.chb.2012.01.004

Popescu, A., Hildebrandt, M., Breuer, J., Claeys, L., Papadopoulos, S., Petkos, G., . . . Padyab, A. (2016). Increasing transparency and privacy for online social network users—USEMP value model, scoring framework and legal. In B. Berendt, T. Engel, D. Ikonomou, D. Le Métayer, & S. Schiffner (Eds.), *Privacy technologies and policy* (Vol. 9484, pp. 38–59). Cham, Switzerland: Springer.

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday*, *15*(1). doi:10.5210/fm.v15i1.2775

Rizk, R., Gürses, S., & Guenther, O. (2010). SNS and 3rd party applications privacy policies and their construction of privacy concerns. In *ECIS 2010 Proceedings*. Retrieved from https://aisel.aisnet.org/ecis2010/143

Shiv, B., & Fedorikhin, A. (1999). Heart and mind in conflict: The interplay of affect and cognition in consumer decision making. *Journal of Consumer Research*, *26*, 278–292. doi:10.1086/209563

Shoemaker, D. W. (2010). Self-exposure and exposure of the self: Informational privacy and the presentation of identity. *Ethics and Information Technology*, *12*, 3–15. doi:10.1007/s10676-009-9186-x

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*, 989–1016.

Soczka, L., Brites, R., & Matos, P. (2015). Personal information disclosure and perceptions about data usage by Facebook. In A. Mesquita & P. Peres (Eds.), *Proceedings of the Second European Conference on e-Learning* (pp. 413–420). Reading, UK: Academic Conferences Limited.

Son, J.-Y., & Kim, S. S. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly*, *32*, 503–529.

Spiekermann, S., & Cranor, L. F. (2009). Engineering privacy. *IEEE Transactions on Software Engineering*, *35*, 67–82. doi:10.1109/TSE.2008.88

Taddicken, M. (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*, 248–273. doi:10.1111/jcc4.12052

Tavani, H. T. (2013). *Ethics and technology: Controversies, questions, and strategies for ethical computing* (4th ed.). Hoboken, NJ: Wiley.

Tow, N.-F. H., Dell, P., & Venable, J. (2010). Understanding information disclosure behaviour in Australian Facebook users. *Journal of Information Technology*, *25*, 126–136. doi:10.1057/jit.2010.18

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research*, *22*, 254–268. doi:10.1287/isre.1090.0260

van Dijck, J. (2013). *The culture of connectivity: A critical history of social media* (1st ed.). Oxford, UK: Oxford University Press.

van Wel, L., & Royakkers, L. (2004). Ethical issues in web data mining. *Ethics and Information Technology*, *6*, 129–140. doi:10.1023/B:ETIN.0000047476.05912.3d

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook. *Information, Communication & Society*, *16*, 479–500. doi:10.1080/1369118X.2013.777757

Author Biographies

Ali Padyab (PhD, Luleå University of Technology) is a researcher of Information Systems at Luleå University of Technology. His research interests include information privacy, social media, Internet of Things, information security, and living labs.

Tero Päivärinta (PhD, University of Jyväskylä) is a professor of Information Systems at Luleå University of Technology, Sweden, and a visiting professor of Empirical Software Engineering on Software, Systems and Services (M3S) at University of Oulu, Finland. His research interests include systems and software development practices, information management, e-Government, and benefits realization from IT investments.

Anna Ståhlbröst (PhD, Luleå University of Technology) is a professor of Information Systems at Luleå University of Technology. Her research interests include living labs, user-driven innovation processes, smart cities, domestic IT use, and online privacy.

Birgitta Bergvall-Kåreborn (PhD, Luleå University of Technology) is the Vice-Chancellor and a professor of Information Systems at Luleå University of Technology. Her research interests include human-centric and appreciative methodologies for design and learning, participatory design, stakeholder-participation and labor-sourcing.