Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon

Research article

Selectivity in posting on social networks: the role of privacy concerns, social capital, and technical literacy

Hadas Schwartz-Chassidim [a,b,*], Oshrat Ayalon [a], Tamir Mendel [a], Ron Hirschprung [c], Eran Toch [a]

[a] Department of Industrial Engineering, Tel Aviv University, Tel Aviv, Israel
[b] Software Engineering Department, Shamoon College of Engineering, Beer Sheva, Israel
[c] Faculty of Engineering, Ariel University, Ariel, Israel

ARTICLE INFO

Keywords:
Privacy
Online social networks
Privacy controls
Social capital
Behavior analysis
Boundary regulation theory
Facebook
Computer privacy
Cognitive aspect of human-computer system
Interaction design
User interface
Software engineering
Computer science
Psychology

ABSTRACT

People's posting behaviors in social networks was perceived as ambiguous, with concerns misaligned with people's public postings. To address this gap, we suggest a model that offers new insights into the relationship between perceptions and actual behaviors. We define a quantitative marker for agility, the frequency in which people update their audience selection when posting information in online social networks, and evaluate the factors that contribute to the variability of agility between different users. We analyzed the posting behavior of Facebook 181 participants, as well as their answers to open and close questions. We find that frequent changes in privacy settings are correlated with high social privacy and with institutional privacy concerns, whereas social concerns were found to be more prominent. Agility was negatively correlated with low public sharing. Our findings show that users use privacy settings to effectively mitigate privacy concerns and desires for creating and strengthening social connections. We discuss how agility can be used to design and to evaluate new user interfaces for managing privacy in social settings.

1. Introduction

Online Social Networks (OSNs) are consistently growing, with 2.3 billion users on Facebook alone, with 74% of respondents reporting they are visiting Facebook sites daily (Smith and Anderson, 2018). Despite OSNs being commonly used (Smith and Anderson, 2018; Tsay-Vogel et al., 2018; Perrin, 2015), users are still very concerned about possible implications of using OSNs, and specifically about implications relating to their privacy and online disclosure. An indirect indication for these significant concerns can be deduced from the raise of privacy-preserving methodologies in OSNs (Praveena and Smys, 2016). Furthermore, privacy concerns increase, and the negative relationship between privacy concerns and self-disclosure weakened across time (Tsay-Vogel et al., 2018).

The behavior of OSNs users has undergone dramatic changes in recent years. Users can now control the information they share with their peers to a large extent (and to a lesser extent, the information they share with service providers.) Privacy norms have shifted over time towards a more restrictive access (Stutzman et al., 2013; Stutzman and Hartzog, 2012), with a higher reliance on privacy settings and on other boundary-regulation mechanisms (Altman, 1975). The literature around privacy behaviors had looked at measures of self-disclosure (Cheung et al., 2015; Saeri et al., 2014; Wisniewski et al., 2014; Hargittai and Marwick, 2016; Dienlin and Metzger, 2016; Gruzd & Hernández-García, 2018) and the effects of a variety of perceptions and attitudes on information disclosure, for example, the perceived risk in sharing (James et al., 2017). Perceptions and attitudes have been extensively examined, including privacy attitudes (Malhotra et al., 2004; Preibusch, 2013; Tan et al., 2012), trust (Wilson and Valacich, 2012), and privacy management controls and architecture (Li et al., 2015). However, navigating sharing on social networks becomes more complicated, for example, because of context collapse, in which people from different social relationships will see the same information about a single person (Skeels and Grudin, 2009). Users need to make nuanced decisions on who they share their information with and in which context. Existing constructs and research

[*] Corresponding author.
E-mail address: hadasch@ac.sce.ac.il (H. Schwartz-Chassidim).

https://doi.org/10.1016/j.heliyon.2020.e03298
Received 20 September 2019; Received in revised form 28 December 2019; Accepted 22 January 2020

methods do not adequately capture and understand how and why people change and update their privacy settings.

In this study, we explore users' behavior with regard to the way they actively share, and not only the amount of shared information or the intention to share. Our approach offers a quantitative multi-dimensional view of people's information sharing behaviors based on Facebook server logs and perceptions in OSNs. Following Altman's Boundary Regulation Theory (Altman, 1975), we adopt a view of privacy as an ongoing dynamic, feedback-oriented process in which individuals continually manage their boundaries to optimize their disclosure goals, balancing between openness and closeness. Therefore, we capture the dynamics of privacy behavior and measure Agility using existing variables (e.g., bridging, bonding, trust etc'.) as well as openness and publicness.

Our study contributes to the existing literature in two ways. First, it provides a model for selectivity in sharing information in OSNs instead of other forms of information disclosure behaviors. Second, our model offers new insights into the relationship between perceptions and actual behaviors. Our model can be useful to scholars, designers, policymakers, and users who can use our privacy marker to understand users' online privacy behavior better and to improve the profile settings and the users' interaction in OSNs.

2. Background

2.1. Privacy in online social networks

Users have growing concerns regarding their privacy in OSNs (Tsay-Vogel et al., 2018; Hodkinson, 2017; Dey et al., 2012). These concerns in OSNs can be divided into institutional and social concerns (Raynes-Goldie, 2010; Ayalon and Toch, 2019). Institutional concerns regard issues that involve concerns from companies and governments, and their possible data usage of personal information (Malhotra et al., 2004; Min and Kim, 2014), for example, the potential use of data for advertisements (Poikela and Toch, 2017). Social concerns regard private information access by other people, as the users' family, friends, and colleagues (Dong et al., 2015; De Wolf et al., 2014; Wisniewski et al., 2012). In OSNs, there is growing evidence that social concerns have a more significant effect on users' behavior than institutional interests (Raynes-Goldie, 2010; Krasnova et al., 2009).

With the growing use of OSNs, and the diverse set of social circles that they encompass, it is harder for users to manage their privacy in different contexts. For example, users who have both their college friends and their close family on the same social network might find it challenging to share their weekend drinking photos. This phenomenon is known as the *Context Collapse*, describing the increasing difficulty of managing privacy with growing social contexts (Skeels and Grudin, 2009; Jeong and Kim, 2017). At the same time, OSNs like Facebook deviate users from their preferred settings by using defaults as a nudge (Hirschprung et al., 2017). Users use technological mechanisms, such as access restrictions Litt and Hargittai, 2016, un-tagging, and deletion (Karr-Wisniewski et al., 2011), as well as more complex strategies, such as division of the platform, obfuscation, and inclusive identities, to manage multiple social contexts (Lampinen et al., 2011; Stutzman and Hartzog, 2012).

2.2. The gap between privacy perceptions and privacy behaviors

The discrepancy between attitudes towards privacy, which tend to reflect concerns and fears, and the actual privacy behaviors which tend to more self-disclosure is commonly referred to as the "Privacy Paradox" in OSNs (Acquisti and Gross, 2006; Barth and De Jong, 2017). Overall, privacy concerns are considered a weak predictor of information disclosure behavior (Acquisti and Gross, 2006; Taddei and Contena, 2013; Hughes-Roberts, 2013; Min and Kim, 2014; Jordaan and Van Heerden, 2017; Kokolakis, 2017; Chen and Chen, 2015). Debatin et al. (2009) used social gratifications to explain the relations between the perceived threats to privacy and the disclosure of information. In another study, the privacy paradox was explained by small incentives, costs or misdirection that can lead people to disclose their personal data more than they declared before (Athey et al., 2017). Several studies have pointed to the perceived social capital, the benefits derived from the social network, as a way to explain why users would be willing to forget some or all of their privacy (Johnston et al., 2013; Utz, 2015; Ellison and Vitak, 2015; Quinn, 2016).

It should be noted that although the Privacy Paradox has been extensively studied in the context of OSNs, there is still inconsistency of privacy attitudes and privacy behavior. The complexity involved in managing self-disclosure in OSNs (Litt and Hargittai, 2016; Li et al., 2018), should focus our attention on how privacy attitudes are related to the actual way sharing mechanisms are used (Kokolakis, 2017). Managing privacy boundaries requires a dialectical process of settings management and coordination, as people take into account both the benefits and risks that come from sharing information (James et al., 2015). It can be the case, for example, that while the overall amount of information users post remains the same, they are more selective in the way they share the information with others. Current measures for information sharing do not adequately capture this discrepancy.

2.3. Understanding privacy behaviors

A variety of studies examined users' use of sharing controls, and their relationships with demographics, privacy attitudes, norms and other properties. Wisniewski et al. (2014) and Lambert (2016) enumerated the variety of privacy behaviors exhibited by users, suggesting six distinct profiles that express users' privacy perceptions and reported strategies. Ellison and Vitak (2015) showed a positive correlation between Facebook users' use of advanced privacy settings, such as selective sharing, and higher levels of perceived social capital. Similarly, other studies have also stressed the ability of users to selectively share their content (Kairam et al., 2012; Watson et al., 2012). The ability of users to control information sharing was found to be one of the strongest predictors to self-reported usage intensity on Facebook (Jordaan and Van Heerden, 2017). This finding highlights the importance of the control in privacy behaviors, but it also raises a question: what are the factors that drive the the control of personal information in OSNs, and what are the factors that are contribute to users' and the need for suitable privacy management mechanisms.

To understand the factors related to the actual use of privacy controls, we first need to bridge the conceptual gap in measuring privacy behaviors that go beyond the disclosure of information. The aforementioned papers (Watson et al., 2012; Wisniewski et al., 2014; Chen and Chen, 2015) explored the visibility of the information, by asking whether participants have employed selective sharing, regardless of the disclosure as a continuous and longitudinal process. However, there are still no measures that adequately address the selectivity of information sharing. To address contemporary behaviors correctly, we need measures that capture selective sharing and switching between multiple audiences to mitigate context collapse and multiple social groups in OSNs.

Surveys are the most commonly-used tool for capturing privacy behavior (Ellison et al., 2007; Chen and Chen, 2015; Dienlin and Trepte, 2015; James et al., 2015; Wisniewski et al., 2015), but they suffer from several important limitations. First, as the privacy paradox predicts, people consistently report perceptions and behaviors that are more privacy oriented than their actual behavior (Utz and Krämer, 2009; Chalklen and Anderson, 2017). The wording of privacy questionnaires has a significant impact on the participants' answers, especially when asking about online privacy (Braunstein et al., 2011). Media reports that focus on privacy risks might influence users (Teutsch and Niemann, 2015). These findings strengthen the need to apply observational metrics to examine the real users' behaviors on OSNs, and to capture actual, rather than stated, user behaviors. Only a handful of works, as Acquisti and Gross (2006), relied on multi-dimensional results that include both surveys and quantitative observational methods, a combination that can align perceptions and behaviors. Multi-dimensional model may assist to assess the impact of perceptions on actual behavior and will contribute to the ongoing discussion around the privacy paradox.

3. Research model and hypotheses

To bridge the gap in understanding selective sharing behavior, we were inspired by Altman's boundary regulation theory, and define *Agility*, a marker that indicates how users manage the boundary with multiple social circles. Agility captures the level of adaptive privacy behavior by quantifying the frequency in which users change the posts' intended audience. When measured through extended periods, agility captures how adaptive a user's behavior is and the extent to which the user adapts to multiple scenarios. This measure reflects the fluctuation in privacy settings with respect to actual posts by the user. The number of configuration changes is counted, regardless of the change source: if it was applied by changing the default privacy or the members of a particular post audience. Because Facebook automatically retains the sharing settings from the last published post as the default for the next one, the marker reflects the user's willingness to divert from the previous configuration. As agility captures the diversity of individual behavior, we have applied Shannon entropy to the measure, similar to the ways in which it was applied to fields such as social group equality (Matei et al., 2015).

We define the agility of user x as the entropy of privacy settings and calculated as the *ln* function of the number of configuration changes among a total of N posts, where p_i^x expresses the chosen configuration of post i normalized by the number of posts N:

$$agility(user_x) = \frac{1}{N}\ln\left(1+\sum_{i=1}^{n-1} C_i^x\right)$$

$$C_i^x = \begin{cases} 1 & \left(p_i^x = \text{default}\right) \vee \left(p_i^x = p_{i-1}^x\right) \\ 0 & else \end{cases} \tag{1}$$

The agility marker returns 0 for a user who uses a single configuration throughout the entire time-frame and a higher value for a user who uses multiple configurations. Based on the definition of agility, we build on the model by Ellison et al. (2007) and examined the relationship between agility and other factors that are based on the users' perceptions. Due to the exploratory nature of our study, and the use of real behavioral data, we have deliberately chosen a flat model, in which we evaluate the relationship between each of the independent variables on agility.

3.1. Privacy behaviors

To align our model with previous models of information disclosure, we define two other measures. Measuring the volume of information which is open to the public is used as the main measure for information disclosure in social networks in several papers (Stutzman et al., 2013; Dienlin and Trepte, 2015; Saeri et al., 2014). To analyze the relation of information disclosure with agility, we define *Publicness* as a measure that quantifies the amount of information a user shares with the general public. The analysis includes personal details (e.g., family and relationships, workplace, home town), identifiable profile picture, other pictures, Facebook ‘likes’, and posts. Each of the information fields was assigned a binary value of 1 if exposed by the user and 0 if not. To measure the publicness of posted photos, we used a scale of 3 values based on the potential ability to identify the person in the picture: ‘0’ no photo, ‘1’ non-identifiable, and ‘2’ identifiable. If more identifying information is revealed the score increases. The publicness of user x is calculated as the sum of the scores in all categories divided by k, the maximum achievable score (which is 19 in our case.) We define $S(Pr_i^x)$ as the score for Pr – profile item i of user x:

$$Publicness(user_x) = \frac{1}{k}\sum_{i=1}^{k} S\left(Pr_i^x\right) \tag{2}$$

To illustrate how publicness is calculated, if a user exposes 13 of the possible 19 categories of information, the total score of public information is $\frac{13}{19} = 0.68$. Previous studies have shown that limiting profile visibility is positively correlated with the perceived ability to manage privacy (Chen and Chen, 2015). As we hypothesize that agility will be positively related to literacy, and that which is based on similar constructs to efficacy (De Wolf et al., 2014), we hypothesize that:

Hypothesis 1. Agility is negatively correlated with Publicness.

The third marker, *Openness*, captures how opened or closed the boundary of communication of an individual user is, measuring how wide the audience of the user's posts is. A higher openness value means that the user tends to share posts with larger audiences. The value is calculated as a weighted sum of the proportion of the different types of posts. We define five categories of audience types, and rank them according to the size of the audience for a posts i by user x, such that $cat(p_i^x)$ receives values as follows: 1 – Only me, 2 – Custom, 3 – Friends-only, 4 – Friends-of-friends, 5 – Public.

$$openness(user_x) = \frac{1}{n_x}\sum_{i=1}^{n} cat\left(p_i^x\right) \tag{3}$$

where n_x is the total number of posts by user x. For example, if a user shares 2 posts with “friends-only” and 4 posts with the whole public, the calculation will be as following: $\frac{(2*3+4*5)}{6} = 4\frac{1}{3}$.

Because OSN users have a varied group of relations, we expect that:

Hypothesis 2. Agility is negatively correlated with Openness.

3.2. Privacy attitudes

Studies have shown that users' privacy concerns in OSNs fall into two categories: social and institutional, whereas participants were more concerned with social privacy (Raynes-Goldie, 2010). Organizational concerns included concerns resulted from possible usage of information by the service provider and by other institutions, such as marketing, human resource, government agencies. Social concerns included concerns related to possible damages caused by other users, including taking advantage of the published information. Therefore, we have measured institutional privacy concerns based on a survey by Malhotra et al. (2004) and perceived social privacy concerns with (Stutzman, 2006). We also measured perceived privacy control and perceived privacy risk (Dinev et al., 2013), as well as perceived trust in Facebook as a company and trust in the users’ social network (Acquisti and Gross, 2006). Accordingly, we hypothesize that:

Hypothesis 3. High privacy concerns (both social and institutional) will be positively correlated with agility, whereas trust and control will be negatively correlated.

3.3. Technological literacy

Research indicates that a lack of computing skills might affect the user's ability to manage her privacy in OSNs (De Wolf et al., 2014). This relation extends to digital privacy literacy, as Malhotra et al. (2004) have shown that the ability of users to understand and manage their privacy is an important factor in Internet users' privacy approaches (Malhotra et al., 2004). Individuals with higher Internet skills are more likely to share content online and to adopt newer social media services (Hargittai and Litt, 2011). Therefore, we hypothesize that:

Hypothesis 4. High levels of digital literacy will be positively related to agility.

3.4. Social capital

Several studies have shown that social capital (Coleman, 1988) is related to a multitude of social network activities, such as creating and maintaining relationships (Ellison et al., 2007) and managing privacy (Quinn, 2016; Utz, 2015). Williams (2006) developed and validated measures for two types of social capital in OSNs: bridging social capital that refers to the benefits gained through connections with weak ties, and bonding capital that is accumulated when strongly tied individuals from a similar background provide support for one another. As higher agility reflects sharing to multitudes of social groups, we hypothesize that:

Hypothesis 5. Agility is positively correlated with bridging and bonding social capital.

4. Method

The study's method is based on correlating collected data regarding sharing behavior on Facebook with a survey data of the same users. We have developed a Facebook application which extracted data that included information about posts that were published by the participant at a three-month period including number of Facebook "likes", number of comments, date of publication, the post type (status, link, video, photo, geographical check-in) and its sharing settings (e.g., public, friends-of-friends, friends, custom, only me.) Overall, 11,141 posts were analyzed, dating to a period three-months prior to the beginning of the survey. The study was reviewed and authorized by Tel- Aviv University ethics review board. Data were collected in an anatomized and secured fashion, without collecting personally-identifiable information such as name, Facebook ID, email, or the content of the posts. Furthermore, participants were informed about the usage of their data and were asked to provide authorization first in our system and another time at the Facebook application.

4.1. Participants

Participants were adult Facebook users (over 18 years of age) recruited via Amazon Mechanical Turk (MTurk), a crowdsourcing service that is commonly used in privacy researches (Kelley, 2010) and also considered to represent a diverse population sample in terms of age, gender and education (Kang et al., 2014; Paolacci and Chandler, 2014; Burnham et al., 2018; McCredie and Morey, 2018).

To control for the quality of the responses, we have followed best practices to control the quality of the MTurk participation and the answers to the questionnaire (Kelley, 2010), including choosing only workers with high qualification scores, using a reading comprehension test, and scanning for inconsistent answers. Also, we have provided an additional bonus of $0.25 for participants who provide a high-quality and authentic explanation regarding their sharing decision-making. Participants were scanned for minimal age, Facebook membership with active behavior (i.e., at least one post in the last month), and at least 100 Facebook friends to ensure measurable privacy behavior. The survey took an average of nine minutes to complete. Following the insights of Braunstein et al. (2011) and Acquisti and Grossklags (2005), the instructions did not explicitly use the term "privacy" in order to avoid priming the participants' for privacy awareness. In the test of inconsistent answers we phrased two additional questions that were opposite to two of the original questions. Following the inconsistency test we excluded 10 participants from this study, leaving 181 valid participants.

The study's population included 110 females and 71 males (181 in total), with an average age of 35 ± 14 years. Forty participants were between the ages of 18 and 24 (22%), 84 participants were between the ages of 25 and 34 (46%), 45 participants were between the ages of 35 and 54 (25%) and 12 participants were 55 or older (6.6%).

4.2. Factors

Agility, calculated for each participant individually, as defined in section 3.1, served as the dependent variable. The independent variables included openness and publicness, which were calculated for each participant based on Facebook actual usage (see sections 3.2 and 3.3.) In addition, a survey was used to gather the participants' perceptions. We measured bridging and bonding social capital (Williams, 2006), and demographics. Based on the contemporary literature, we classified the perception variables into two groups: institutional and social privacy (Raynes-Goldie, 2010; Confessore, 2018). The first consists of concerns, control, and risk and the second consists of access. Publicness, trust and identity can be associated with both social and institutional dimensions. The complete questionnaire, consisting of 56 items, is shown in Table 1. Unless otherwise noted, scale items were measured on a seven-point Likert type scale (1 = Strongly Disagree, 7 = Strongly Agree.) The analysis was controlled for gender and for the participants' age.

To reduce the survey's complexity, the items were grouped together using Principle Component Analysis (PCA) (Hair et al., 2006). The complete set of variables that were analyzed by PCA appears in Table 2. The independent variables were the PCA factors that represent the items of the questionnaire and several measures of Facebook user properties (e.g., number of posts, number of friends) Agility data did not follow a normal distribution (see Figure 1), and describe a temporal count process, so we chose to analyze it using GLM with the Poisson link function of Cameron and Trivedi (2013). Both publicness and openness were found to be normally distributed. Finally, we conducted qualitative analysis of open-ended questions about privacy management, and categorized the explanations the participants provided regarding their privacy strategies.

5. Results

The distribution of each marker for all of the 181 participants is presented in Figure 1. Approximately 50% of posts in our sample were open to friends-only, 12% were open to the public and the rest are open to custom groups. These results were in line with several studies based on surveys (Hampton et al., 2012) or on large-scale observational analyses (Stutzman et al., 2013). Approximately 50% of users used more than one privacy sharing option in the observed three-month period; 25% of the posts are shared with more restricted methods than friends only by excluding specific people or including specific groups. Approximately 30% of the participants used these mechanisms, indicating the relative success of fine-grained privacy settings.

5.1. Modeling agility

Agility is unevenly distributed, with 48.3% of the participants having an agility value of 0, which means that they were using a single privacy sharing setting (the most common is friends only.) Therefore, we see that little more than 50% of users employ some sort of selectivity by sharing different posts with different groups. The agility of the rest of the users are spread in a long-tail distribution, with 27% of the users switching privacy settings of 0.2 of their posts, and additional 15% of the users change the privacy settings of up to 0.4 of their posts. The openness values indicate the popularity of the friends-only privacy setting (openness = 3); approximately 45% of posts are published using this configuration. Publicness is approximately normally distributed: the left side of the graph, which represents users who publish in a less public manner, is 28%; 52% present more identifying information (grade between 0.3 and 0.) None of the participants revealed the maximum number of public items.

To analyze the factors related to agility, three Generalized Linear Models (GLM) regressions were created, using the set of aforementioned PCA factors that express demographics, OSN literacy, social capital scales, privacy perceptions and Facebook usage. Identity and computer

Table 1. The full questionnaire, consisting of 11 topics.

Topics	Questions
a. OSN Literacy	a.1 I feel confident changing a Facebook post's privacy settings.
	a.2 I am aware of the option to limit the shared information with special audience.
	a.3 I feel confident limiting the people who can search for me or contact me on Facebook.
	a.4 I feel confident deleting old Facebook posts.
	a.5 I feel confident limiting the publicity of certain profile information on Facebook.
	a.6 I am aware of to whom I share a content online.
	a.7 When sharing information online I am making adjustments so the content will fit the potential audience.
b. Computer Literacy	b.1 I feel confident solving most computer problems.
	b.2 I use the computer for many of my needs (work, searching, purchasing, etc.).
c. Risk (Dinev et al., 2013)	c.1 In general, it would be risky to give personal information to Web sites.
	c.2 There would be high potential for privacy loss associated with giving personal information to Web sites.
	c.3 Providing Web sites with my personal information would involve many un- expected problems
d. Perceived privacy concern (Malhotra et al., 2004)	d.1 I am concerned that companies are collecting too much information about me
	d.2 Companies should not use personal information for any purpose unless it was authorized by individuals who provided the information.
	d.3 Companies should never sell the personal information to other companies.
	d.4 Online companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information.
e. Trust Perceived (Acquisti & Gross, 2006)	e.1 Facebook as a company.
	e.2 Your own friends on Facebook.
	e.3 Friends of your friends on the Facebook.
	e.4 A Facebook user which is not connected to you or to your friends.
f. Perceived control (Dinev et al., 2013)	f.1 I think I have control over what personal information is released by these websites.
	f.2 I believe I have control over how personal information is used by these web-sites
	f.3 I believe I have control over what personal information is collected by Web-sites
	f.4 I believe I can control my personal information provided to these Web sites.
g. Identity (Stutzman, 2006)	g.1 It is important to me to protect my identity information.
	g.2 I am concerned with the consequences of sharing identity information.
h. Access (Stutzman, 2006)	h.1 I am OK with friends accessing my Facebook profile.
	h.2 I am OK with family accessing my Facebook profile.
	h.3 I am OK with classmates accessing my Facebook profile.
	h.4 I am OK with strangers accessing my Facebook profile.
i. Bonding social capital (Williams, 2006)	i.1 There are several people online I trust to help solve my problems.
	i.2 There is someone online I can turn to for advice about making important decisions.
	i.3 When I feel lonely, there are several people online I can talk to
	i.4 If I needed an emergency loan of $500, I know someone online I can turn to.
	i.5 The people I interact with online would put their reputation on the line for me.
	i.6 The people I interact with online would be good job references for me.
	i.7 The people I interact with online would share their last dollar with me.
	i.8 The people I interact with online would help me fight an injustice.
j. Bridging social capital (Williams, 2006)	j.1 Interacting with people online makes me interested in things that happen out-side of my town.
	j.2 Interacting with people online makes me want to try new things.
	j.3 Interacting with people online makes me interested in what people unlike me are thinking.
	j.4 Talking with people online makes me curious about other places in the world.
	j.5 Interacting with people online makes me feel like part of a larger community.
	j.6 Interacting with people online makes me feel connected to the bigger picture.
	j.7 Interacting with people online reminds me that everyone in the world is connected.
	j.8 I am willing to spend time to support general online community activities.
	j.9 Interacting with people online gives me new people to talk to.
	j.10 Online, I come in contact with new people all the time.
k.Demographic information	k.1 In which country do you currently reside?
	k.2 What is your gender?
	k.3 What is your age?
	k.4 Which of the following best describes your highest achieved education level?
	k.5 How long have you 10been using Facebook?
	k.6 On average, how often do you use Facebook?
	k.7 On average, how often do you update your profile in Facebook?
	k.8 On average, how often do you post information on Facebook

Table 2. The results of the principle component analysis (PCA). Each set of items is explained by either one or two components.

Factors	Eigen-value	Vari-ance	KMO	Sphericity or Factor Loading
a.1) OSN Literacy (PC1)	3.14	44.8	2	$\chi^2 = 351:65; p < 0:001$
Change privacy settings				0.579
Aware to limit shared info				0.772
Limit people who can search				0.836
Delete old posts				0.704
Publicity of certain profile				0.879
a.2) OSN Literacy (PC2)	1.100	15.7		
making adjustments				0.881
aware to whom I share				0.601
b) Risk	2.347	78.245	0.728	$\chi^2 = 252:77, p <:001$
Personal info to OSN				0.904
Potential to privacy loss				0.883
Unexpected problems				0.866
c) Concern	2.98	59.58	0.772	$\chi^2 = 380:157; p <:001$
Sharing a lot of info. about myself				0.649
Companies collecting info				0.752
Companies should not use info				0.817
Companies should never sell info				0.849
Companies should never share info				0.778
d) Trust	1.419	47.31	0.530	$\chi^2 = 26:98, p <:001$
Facebook as a company				0.496
Your friends				0.736
Friends of your Friends				0.795
e) Control	2.418	80.597	0.69	$\chi^2 = 331:485; p <:001$
Personal info				0.919
What is provided				0.934
How personal info used				0.937
f.1) Access (PC1)	1.806	45.139	0.545	$\chi^2 = 101:971; p <:001$
I am OK with friends accessing my Facebook profile				0.835
I am OK with family accessing my Facebook profile				0.78
f.2) Access (PC2)	1.110	27.742		
I am OK with classmates accessing my Facebook profile				0.672
I am OK with strangers accessing my Facebook profile				0.947
g.1) Bonding (PC1)	4.350	54.369	0.878	$\chi^2 = 669:688; p <:001$
I trust to help solve my problems				0.829
I can turn to for advice				0.864
I feel comfortable talking to about intimate personal problems				0.770
would help me fight an injustice				0.757
g.2) Bonding (PC2)	1.05	13.057		
I needed an emergency loan of $500				0.832
would put their reputation on the line for me			0.836	
would be good job references for me				0.686
would share their last dollar with me				0.829
h.1) Bridging (PC1)	5.435	54.353	0.5	$\chi^2 = 247:976; p <:001$
makes me interested in things that happen out-side of my town				0.737
makes me want to try new things				0.762
makes me interested in what people unlike me are thinking				0.785
makes me curious about other places in the world				0.826
makes me feel like part of a larger community				0.833
makes me feel connected to the bigger picture				0.826
reminds me that everyone in the world is connected				0.612
h.2) Bridging (PC2)	1.511	15.117		
spend time to support general online community				-0.852
gives me new people to talk				-0.967
I come in contact with new people				-0.967

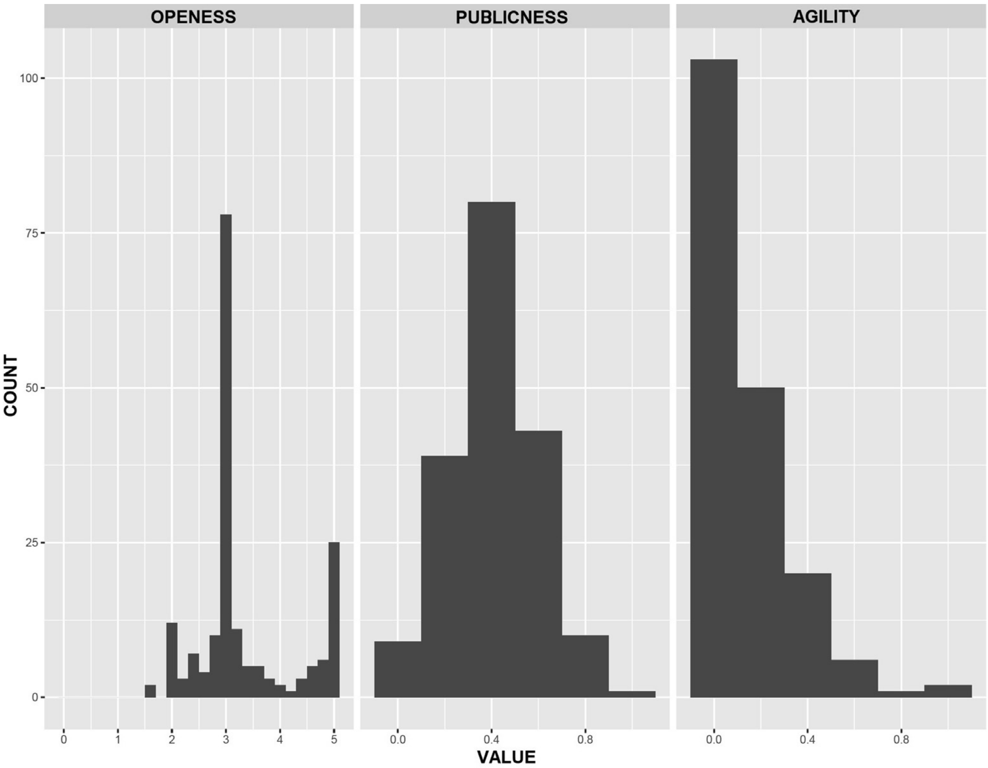

Figure 1. The distribution of each of the three markers, Openness, Publicness, and Agility across all 181 participants.

literacy had only two questions, thus they were used as mean values. Trust showed low adequacy to the factor with $KMO = 0.53$ and low factor loading (< 0.5), therefore the individual items were included as raw variables that refer to social and institutional privacy. We demonstrate an evolving model that is composed of the three main stages and show the contribution of each facet: (I) demographics, (II) privacy concerns and digital literacy and (III) Facebook usage and sociability. As long as the R^2 or adjusted R^2 is greater than the previous stage threshold (e.g., $0.1 < 0.23 < 0.7$), we continued with the process of adding predictors to the model (Harrell, 2015). The full list of significant relations is depicted in Table 3. The GLM model for Agility includes a set of dummy variables to model categorical predictor variables.

Agility is significantly tied to the variables of disclosure of information, social and institutional privacy, literacy and social capital measures ($\chi^2(28) = 1148.8, p < 0.001$ with an r^2 of 0.34.) Publicness was found as the most significant predictor ($\chi^2(1) = 16.27$, $p < 0.001$), negatively correlated to agility. Users with higher publicness tend to be less agile, thus confirming Hypothesis 1. Openness was the second most significant variable that is related to a decrease Agility (χ^2 $(1) = 129.9, p < 0.001$). Users who are more open tend to be less agile, supporting Hypothesis 2.

The findings show that both social and institutional privacy affected the agility, with stronger effect of social privacy variables. The familiarity with people that access Facebook and trusting Facebook users that are friends of friends are negatively associated with Agility ($\chi^2(1) = 36.0$, $p < 0.05$ and $\chi^2(1) = 5.33$, $p < 0.05$ correspondingly). This supports Hypothesis 3. From institutional privacy perspective, trusting Facebook as a company was not found to be significant, and only privacy concerns was found to be significant, such that users with higher privacy concerns have higher agility ($\chi^2 2(1) = 9.09$, $p < 0.05$.) Concerns regarding the consequences of sharing Identity information significantly decreases Agility. Hypothesis 4, which assumes an effect of digital literacy on agility, was only weakly confirmed. Higher agility was associated with higher computer literacy ($\chi^2(1) = 4.45$, $p < 0.05$) but not with OSN literacy. The intensity of Facebook use was found to have only a weak relatuib on Agility, with a higher number of posts slightly related to lower Agility (χ^2 $(1) = 277.2, p < 0.001$). The number of friends was not found to be significant.

Bonding social capital factors were significant variables in the model. Participants with higher bonding social capital perceptions were generally more agile ($\chi^2(1) = 12.65$, $p < 0.001$ PC1.) The effect of bridging was not significant. These results point to the association between adaptive privacy behavior and strong-tie socialization on Facebook. Therefore, Hypothesis 5 is supported for bonding, but not for bridging.

To compare agility to other privacy behavior measures, we build a similar model for publicness and openness. The model for publicness shows a significant but modest fit ($F(19, 160) = 2.435, p < 0.001$), with an r^2 of 0.22 and an adjusted r^2 of 0.14 (controlled for age, education, and number of Facebook friends.) Bridging social capital has a significant effect on publicness, demonstrating a relationship between constructing connections with weak-tie relations and strangers and the higher exposure of personal profile information. Publicness was also found to be significantly affected by lower levels of concern regarding access to personal information. These findings is inline with the results of De Wolf et al. (2014), Litt (2013). The linear model for openness was significant but rather weak ($F(19, 161) = 1.048$, $p < 0.001$) with an r^2 of 0.11 and an adjusted r^2 of 0.06. Participants with lower levels of access concerns are more open overall. The relations between openness and awareness of sharing information, including the extent of content adjustment, were reversed such that participants who were more open had lower OSN literacy. Publicness and openness are significantly correlated, with a weak-to-medium effect size ($r = 0.2$.) We conclude that the boundary regulation within Facebook friends is less meaningful than that with the general public.

5.2. Qualitative analysis

In the last question of the survey, we have asked participants to explain their decisions when choosing their audience when posting on Facebook, with the objective of understanding the reasons behind different types of privacy strategies. The answers were qualitatively

Table 3. Regression model evolution of the three markers. Agility models refer to the generalized linear regression with Poisson link function. Cells contain standardized coefficients, and values of significant predictor variables and in the bracket the partial correlation value. Significant variables were significant at $p < 0.01$ were marked with ** and at $p < 0.05$ with *. Marginally significant was marked with # at $p < 0.1$

Agility

	Demographics	Demo+ Privacy + Literacy	Full model
Intercept	1.99 (0.09)**	2.58 (0.5)**	3.80 (0.52)**
Age (18–24)	0.47 (0.09)**	0.34 (0.09)**	0.09 (0.1) n.s.
Age (25–34)	0.19 (0.08)*	0.16 (0.08)*	0.03 (0.08) n.s.
Gender (female)	-0.9 (0.06)	-0.5 (0.07)**	0.03 (0.08) n.s.
Education (Up to 12 years)	-1.02 (0.42)	-0.8 (0.42)*	-0.43 (0.4) n.s.
Education (High-school)	-0.22 (0.15) n.s.	-0.15 (0.16) n.s.	-0.27 (0.1)n.s.
Education (College)	-0.25 (0.1)	-0.05 (0.1) n.s.	0.05 (0.12) n.s.
Education (Bachelor)	0.07 (0.09) n.s.	0.15 (0.1) n.s.	-0.11 (0.1) n.s.
Risk PC1	-	-0.04 (0.01)	0.002 (0.01) n.s.
Trust Facebook as company	-	-0.03 (0.02) n.s.	-0.01 (0.03) n.s.
Trust Own friends	-	-0.06 (0.03)	0.035 (0.04) n.s.
Trust Friends of friends	-	-0.13 (0.04)	-0.1 (0.03)
Privacy concern PC1	-	0.03 (0.01)**	0.04 (0.01)**
Access PC1	-	-0.3 (0.08)	-0.22 (0.03)
Access PC2	-	0.17 (0.02)**	0.35 (0.05)**
Identity	-	-0.02 (0.03)n.s.	-0.08 (0.04)
Control PC1	-	-0.03 (0.01)	-0.02 (0.01)#
Computer literacy	-	0.07 (0.04) n.s.	0.10 (0.05)*
OSN literacy PC1	-	0.02 (0.01)#	0.01 (0.01) n.s.
OSN literacy PC2	-	0.02 (0.02)n.s.	0.02 (0.02) n.s.
Bridging PC1	-	-	-0.003 (0.008) n.s.
Bridging PC2	-	-	0.01 (0.01) n.s.
Bonding PC1	-	-	0.04 (0.01) **
Bonding PC2	-	-	0.01 (0.001) n.s.
Number of friends	-	-	-2.10^5 (9.52^5) n.s.
Number of posts	-	-	-0.02 (0.001) **
Publicness	-	-	-0.95 (0.22) **
openness	-	-	-0.56 (0.03) *
Pseudo R^2	0.1	0.23	0.7

analyzed by two independent raters to develop categories; they displayed high inter-rater reliability (pairwise Kappa of $0.719, p < 0.0001$.) After several iterations we have reached four final categories included four distinctive strategies: “Context-based” (40%), “Friends” (33.5%), “Self-censorship” (19%), and “Unconcerned” (7.5%.)

Approximately 40% of participants provided reasons that were related to the interaction of the post's context with various audiences, which we defined as the context-based strategy. Some participants rely on Facebook's built-in mechanisms (*“I share most with my friends. If I am posting a joke or something that may be taken the wrong way by a few people I hide it from them. I rarely post public updates.”*) Other participants deferred to other boundary regulation mechanisms such as multiple networks or multiple media channels: *“If I have something private to say to a small group of people, I rely on Skype or email…”*. These results are correlative with the distribution of the agility marker (Figure 1), in which about 53% have used more than one privacy setting.

The context-based strategy was particularly useful when social contexts are complicated: “I always choose custom and exclude at least the same two people who I do not like. Also I often exclude my mother.” or “If it's something I wouldn't want my ex-husband to know about then it's a custom post; otherwise, it's a Friends only post.” Other participants choose their audience based on the content: “…as not to offend some people that I care about with my posts about politics, marijuana, or peppered with cursing.” The need to distinguish between personal and business use of Facebook was mentioned by several participants: “I use social media for marketing as well as for keeping up with friends and family, so those people are designated in groups as well.”

Approximately 19% of the participants described some sort of self-censorship mechanism. For example, a user stated: *“If I'm uncomfortable with my friend's list seeing it, then I don't post it”*. Another user stated, *“I don't make anything custom because I feel that if you need to hide something from certain people, you should not be posting it in the first place.”* Of the 36 participants in the self-censorship group, 26 participants had an agility of 1 (a single setting used throughout the three-month period), 9 participants had a variety of 2 and one participant had a variety of 3. These results show that participants who use a single privacy setting might compensate with additional selectivity in the published content ($\lambda^2 = 8.43, p < 0.01$.) Finally, A total of 7.5% of the participants used the Friends strategy, relying on the choice of friends as the main mechanism for privacy regulation: *“I generally always choose friends. Anyone who wants to know about me needs to know me”*.

The qualitative results are well aligned with the quantitative ones. The categories are able to predict the agility with a fit of $R^2 = 0.31$. The relations between the reported strategy management and privacy concerns and sociability were significant but lower (0.18 and 0.14, respectively.) The relationship with the intensity of use (number of posts and number of friends) was not significant. Following these results, we deduce that the variables that explain the user's privacy management strategies are related to agility and social benefits rather than to the amount of published information.

These findings demonstrate that most of the participants reported that they use existing tools and mechanisms to attain the required privacy level by selecting the audience and content for different situations. A small minority of participants reported they use self-censorship and sometimes refrain from publishing instead of relying on “built-in” mechanisms. People's decisions are frequently guided based on the nature of the relationships, attempting to match the extent of closeness and familiarity to the published content.

6. Discussion and conclusions

This work measures and analyzes a particular aspect of privacy behavior: the selectivity of the audience Facebook users choose for their posts. Our findings tie observed selective information disclosure behavior to motivations and attitudes and showed that agility is influenced by approaches towards socialization and towards privacy. Our analysis points to the importance of measuring selective information sharing. We see that the relation between privacy concerns and agility is stronger than its relation to publicness and to openness. Therefore, we conclude that measuring privacy only as of the disclosure of information to the public (e.g., in Stutzman et al. (2013); Dienlin and Trepte (2015); Saeri et al. (2014); Chen and Chen (2015)), does not adequately address the full spectrum of privacy behaviors. We show how agility functions as a privacy management strategy that is reflected by an ongoing activity in which individuals continually manage their privacy boundaries in different and changing contexts. We first show that the intensity of this activity is negatively correlated with the proposed markers publicness and openness and with high privacy concerns and sociability measures.

To some extent, our findings provide an explanation to some aspects of the privacy paradox in online social networks today. Concerns are mitigated by selective sharing, the practice of using Facebook's sharing controls to effectively control the audience for the published information. We argue that the contradiction with previous observational evidence (Acquisti and Gross, 2006; Debatin et al., 2009; Krasnova et al., 2010; Stutzman et al., 2012; Acquisti et al., 2015; Jordaan and Van Heerden, 2017) can be explained by the use of different methodological approaches and by the way in which privacy behavior and perceptions are theoretically framed and phrased. The following are the main contributions of the study. High privacy concerns can be channeled with higher selectivity rather than with lower public exposure.

Our results show that social privacy concerns have stronger relationship to privacy behavior than institutional privacy concerns. These results support survey-based results that measured the relationship between various types of privacy concerns and people's attitude Ayalon and Toch (2019). Concerns about access by other social groups to data (e.g., friends, family, coworkers) which reflects social privacy concerns (Stutzman et al., 2011), were found to be a significantly stronger predictor than the effect of the way companies treat personal information (Malhotra et al., 2004).

Agility provides a way to empirically characterize users' privacy strategies. In contrast to studies that were based on self-reflected reports Wisniewski et al. (2014), Dong et al. (2015), the actual behavioral data reveals a smaller set of strategies. The first strategy, which we name “nesting”, is characterized by high openness and low agility. Nesting is manifested primarily by low variance in privacy settings. On the other hand, by analysing the textual feedback, we see that nesters frequently employ self-censorship. Nesters might decide to refrain from publishing some information, thus limiting their ability to access the resources of the social network can support their preferences. In the second strategy, which we name “roaming”, users rely on Facebook's privacy management mechanisms to selectively distribute information. Roamers frequently change their privacy settings, posting different types of information to different audiences. Roamers reach a larger number of people with information they want to share while restricting sensitive information to a smaller group of users reflected by bonding.

Analyzing agility allows us to draw relationships between sociability and privacy behavior. Our results tie Boundary Regulation Theory (Altman, 1975) and Social Capital Theory (Ellison et al., 2011), by describing detailed relations between approaches toward social capital affects and different aspects of privacy behavior. We see that bonding social capital has a stronger relationship with roaming behavior, leading us to conclude that roamers gain a higher level of both privacy and sociability. Selective sharing allows the user to gain higher bonding social capital by presenting a tailored identity to different groups of people. However, self-censorship, which characterizes nesters, reduces bonding social capital as a result of reduced interaction with strong-tie relations. Furthermore, roamers were found to have a significantly higher level of technical skills when managing OSN features, including privacy settings, which partially explains the differences between the two groups. We find this result encouraging, as it points to the potential of privacy education to increase both privacy and social capital. In simpler terms, educating users about privacy or adapting the design of user interface on OSNs to the users'. privacy preferences may make the entire social network more valuable to users while simultaneously increasing the level of privacy.

Our findings have some methodological implications. First, it highlights the importance of using actual privacy behaviors rather than self-reported surveys. Self-reported behavior might be biased in different ways, which is especially important in light of growing evidence that points to methodological problems when using surveys to learn about privacy (Hughes-Roberts, 2013; Braunstein et al., 2011; Brenner and DeLamater, 2016). Similarly to Dienlin and Trepte (2015) and Hughes-Roberts (2013), our findings show that the definition of privacy attitudes has a significant effect on the correlation with behavior. Different phrasing of attitudinal questions can lead different researchers to completely different conclusions. We therefore argue for incorporating behavioral observations, extracted from Facebook server, as a way to validate and objectively explore the real needs and preferences of users.

When considering the applicability of our findings, the reader should take into account several limitations of our study. First, as the sample is based on Amazon MTurk workers, our sample is not representative of the general population. For example, females were over represented in our sample, and the population is more privacy-aware than the general U.S. population (Kang et al., 2014). However, we partially control for these biases by showing that privacy setting distribution is similar to larger representative surveys (Hampton et al., 2012) and other large-scale observational studies (Stutzman and Kramer-Duffield, 2010; Stutzman et al., 2013). In addition, the results of our comprehensive approach can be even more significant if users are less skilled and the gap between their perceptions and their behavior could be explained by the lack of strategies implementation. Another limitation is the size of our sample. While our analysis produced a significantly statistical model, larger sample sizes might reveal more variations within the results and may lead to a more fine-grained analysis of privacy strategies. Finally, our findings are associational in nature, and causality can only be supported by accepting the theoretical assumptions that ties planned behavior to privacy behavior (Saeri et al., 2014).

The context of this work was OSNs, particularly Facebook. However, by applying the normalization methods we suggest, the markers can be relevant to systems that allow peers to specify fine-grained sharing policies in a network environment. Also, the markers can be extended to systems such as location-sharing applications, multi-party supply-chains, and enterprise information systems. Designers, administrators and researchers of information sharing networks can use the boundary regulation markers to analyse the privacy norms of users, to predict the impact of privacy mechanisms including increasing the users' awareness to institutional privacy, and to assess how privacy behavior changes over time.

In this study, we define and analyze social network sharing agility – a marker for the selectivity in sharing posts on Facebook. We interpret Boundary Regulation Theory (Altman, 1975) to produce quantitative and empirical analysis that measure how people change their information boundary within an OSN. We then compare the new marker with more traditional measures of privacy behavior, including Publicness and Openness, to model the uses and factors that drive selectivity. Our findings support the hypothesis that employing audience selectivity to mitigate privacy concerns, which may be a possible explanation in resolving the privacy paradox in online social networks. Secondly, that attitudes towards social capital govern the strategies users choose regarding their privacy. These strategies are diverse, leading towards different socialization objectives, ranging from bonding with close friends to discovering new relations.

Declarations

Author contribution statement

Hadas Schwartz-Chassidim: Conceived and designed the experiments; Performed the experiments; Analyzed and interpreted the data; Contributed reagents, materials, analysis tools or data; Wrote the paper.

Oshrat Ayalon: Conceived and designed the experiments; Analyzed and interpreted the data; Contributed reagents, materials, analysis tools or data; Wrote the paper.

Tamir Mendel: Performed the experiments; Contributed reagents, materials, analysis tools or data; Wrote the paper.

Ron Hirschprung: Analyzed and interpreted the data; Contributed reagents, materials, analysis tools or data; Wrote the paper.

Eran Toch: Conceived and designed the experiments; Contributed reagents, materials, analysis tools or data; Wrote the paper.

Funding statement

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Competing interest statement

The authors declare no conflict of interest.

Additional information

No additional information is available for this paper.

References

Acquisti, A., Gross, R., 2006. Imagined communities: awareness, information sharing, and privacy on the Facebook. In: International workshop on privacy enhancing technologies, pp. 36–58.

Acquisti, A., Grossklags, J., 2005. Privacy and rationality in individual decision making. IEEE Secur. Priv. 2, 24–30.

Acquisti, A., Brandimarte, L., Loewenstein, G., 2015. Privacy and human behavior in the age of information. Science 347, 509–514.

Altman, I., 1975. The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding.

Athey, S., Catalini, C., Tucker, C., 2017. The digital privacy paradox: small money, small costs, small talk. In: Tech. Rep. National Bureau of Economic Research.

Ayalon, O., Toch, E., 2019. Evaluating users' perceptions about a system's privacy: differentiating social and institutional aspects. In: Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019).

Barth, S., De Jong, M.D., 2017. The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. Telematics Inf. 34, 1038–1058.

Braunstein, A., Granka, L., Staddon, J., 2011. Indirect content privacy surveys: measuring privacy without asking about it. In: Proceedings of the Seventh Symposium on Usable Privacy and Security, p. 15.

Brenner, P.S., DeLamater, J., 2016. Lies, damned lies, and survey self-reports? Identity as a cause of measurement bias. Soc. Psychol. Q. 79, 333–354.

Burnham, M.J., Le, Y.K., Piedmont, R.L., 2018. Who is Mturk? Personal characteristics and sample consistency of these online workers. Ment. Health Relig. Cult. 1–11.

Cameron, A.C., Trivedi, P.K., 2013. In: Regression Analysis of Count Data, 53. Cambridge university press.

Chalklen, C., Anderson, H., 2017. Mothering on Facebook: exploring the privacy/openness paradox. Soc. Media+ Soc. 3, 2056305117707187.

Chen, H.-T., Chen, W., 2015. Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection. Cyberpsychol., Behav. Soc. Netw. 18, 13–19.

Cheung, C., Lee, Z.W., Chan, T.K., 2015. Self-disclosure in social networking sites: the role of perceived cost, perceived benefits and social influence. Internet Res. 25, 279–299.

Coleman, J.S., 1988. Social capital in the creation of human capital. Am. J. Sociol. S95–S120.

Confessore, N., 2018. Cambridge Analytica and Facebook: the Scandal and the Fallout So Far Kernel Description. Retrieved from. http://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

De Wolf, R., Willaert, K., Pierson, J., 2014. Managing privacy boundaries together: exploring individual and group privacy management strategies in Facebook. Comput. Hum. Behav. 35, 444–454.

Debatin, B., Lovejoy, J.P., Horn, A.-K., Hughes, B.N., 2009. Facebook and online privacy: attitudes, behaviors, and unintended consequences. J. Computer-Mediated Commun. 15, 83–108.

Dey, R., Jelveh, Z., Ross, K., 2012. Facebook users have become much more private: a large-scale study. In: Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference, pp. 346–352.

Dienlin, T., Metzger, M.J., 2016. An extended privacy calculus model for SNSs: analyzing self-disclosure and self-withdrawal in a representative US sample. J. Computer-Mediated Commun. 21, 368–383.

Dienlin, T., Trepte, S., 2015. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. Eur. J. Soc. Psychol. 45, 285–297.

Dinev, T., Xu, H., Smith, J.H., Hart, P., 2013. Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. Eur. J. Inf. Syst. 22, 295–316.

Dong, C., Jin, H., Knijnenburg, B.P., 2015. Predicting Privacy Behavior on Online Social Networks. ICWSM, pp. 91–100.

Ellison, N.B., Vitak, J., 2015. Social network site affordances and their relationship to social capital processes. Handb. Psychol. Commun. Technol. 32, 205.

Ellison, N.B., Steinfield, C., Lampe, C., 2007. The benefits of Facebook "friends:" Social capital and college students' use of online social network sites. J. Computer-Mediated Commun. 12, 1143–1168.

Ellison, N.B., Vitak, J., Steinfield, C., Gray, R., Lampe, C., 2011. Negotiating privacy concerns and social capital needs in a social media environment. In: Privacy Online. Springer, pp. 19–32.

Gruzd, A., Hernández-García, Á., 2018. Privacy concerns and self-disclosure in private and public uses of social media. Cyberpsychol., Behav. Soc. Netw. 21, 418–428.

Hair, J.F., Black, W.C., Babin, B.J., Anderson, R.E., Tatham, R.L., 2006. In: Multivariate Data Analysis, 6. Pearson Prentice Hall Upper, Saddle River, NJ.

Hampton, K.N., Goulet, L.S., Marlow, C., Rainie, L., 2012. Why Most Facebook Users Get More than They Give. Pew Internet Am. Life Project 3.

Hargittai, E., Litt, E., 2011. The tweet smell of celebrity success: explaining variation in Twitter adoption among a diverse group of young adults. New Media Soc. 13, 824–842.

Hargittai, E., Marwick, A., 2016. "What can I really do?" Explaining the privacy paradox with online apathy. Int. J. Commun. 10, 21.

Harrell Jr., F.E., 2015. Regression Modeling Strategies: with Applications to Linear Models, Logistic and Ordinal Regression, and Survival Analysis. Springer.

Hirschprung, R., Toch, E., Schwartz-Chassidim, H., Mendel, T., Maimon, O., 2017. Analyzing and optimizing access control choice architectures in online social networks. ACM Trans. Intell. Syst. Technol. (TIST) 8, 57.

Hodkinson, P., 2017. Bedrooms and beyond: youth, identity and privacy on social network sites. New Media Soc. 19, 272–288.

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

James, T.L., Wallace, L., Warkentin, M., Kim, B.C., Collignon, S.E., 2017. Exposing others' information on online social networks (OSNs): perceived shared risk, its determinants, and its influence on OSN privacy control use. Inf. Manag. 54, 851–865.

James, T.L., Warkentin, M., Collignon, S.E., 2015. A dual privacy decision model for online social networks. Inf. Manag. 52, 893–908.

Jeong, Y., Kim, Y., 2017. Privacy concerns on social networking sites: interplay among posting types, content, and audiences. Comput. Hum. Behav. 69, 302–310.

Johnston, K., Tanner, M., Lalla, N., Kawalski, D., 2013. Social capital: the benefit of Facebook `friends. Behav. Inf. Technol. 32, 24–36.

Jordaan, Y., Van Heerden, G., 2017. Online privacy-related predictors of Facebook usage intensity. Comput. Hum. Behav. 70, 90–96.

Kairam, S., Brzozowski, M., Huffaker, D., Chi, E., 2012. Talking in circles: selective sharing in google+. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 1065–1074.

Kang, R., Brown, S., Dabbish, L., Kiesler, S., 2014. Privacy attitudes of mechanical turk workers and the us public. In: Symposium on Usable Privacy and Security (SOUPS).

Karr-Wisniewski, P., Wilson, D., Richter-Lipford, H., 2011. A new social order: mechanisms for social network site boundary regulation. In: Americas Conference on Information Systems, AMCIS.

Kelley, P.G., 2010. Conducting usable privacy & security studies with amazon's mechanical turk. In: Symposium on Usable Privacy and Security (SOUPS)(Redmond, WA).

Kokolakis, S., 2017. Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon. Comput. Secur. 64, 122–134.

Krasnova, H., Günther, O., Spiekermann, S., Koroleva, K., 2009. Privacy concerns and identity in online social networks. Identity Inf. Soc. 2, 39–63.

Krasnova, H., Spiekermann, S., Koroleva, K., Hildebrand, T., 2010. Online social networks: why we disclose. J. Inf. Technol. 25, 109–125.

Lambert, A., 2016. Intimacy and social capital on Facebook: beyond the psychological perspective. New Media Soc. 18, 2559–2575.

Lampinen, A., Lehtinen, V., Lehmuskallio, A., Tamminen, S., 2011. We're in it together: interpersonal management of disclosure in social network services. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 3217–3226.

Li, Y., Gui, X., Chen, Y., Xu, H., Kobsa, A., 2018. When SNS privacy settings become granular: investigating users' choices, rationales, and influences on their social experience. In: Proceedings of the ACM on Human-Computer Interaction, 2, p. 108.

Li, Y., Li, Y., Yan, Q., Deng, R.H., 2015. Privacy leakage analysis in online social networks. Comput. Secur. 49, 239–254.

Litt, E., 2013. Understanding social network site users' privacy tool use. Comput. Hum. Behav. 29, 1649–1656.

Litt, E., Hargittai, E., 2016. "Just cast the net, and hopefully the right fish swim into it": audience management on social network sites. In: Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing, pp. 1488–1500.

Malhotra, N.K., Kim, S.S., Agarwal, J., 2004. Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. Inf. Syst. Res. 15, 336–355.

Matei, S.A., Bruno, R., Morris, P.L., 2015. Visible effort: visualizing and measuring group structuration through social entropy. In: Transparency in Social Media. Springer, pp. 109–123.

McCredie, M.N., Morey, L.C., 2018. Who Are the Turkers? A Characterization of MTurk Workers Using the Personality Assessment Inventory. Assessment, 1073191118760709.

Min, J., Kim, B., 2014. How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit and cost. J. Assoc. Inf. Sci. Technol.

Paolacci, G., Chandler, J., 2014. Inside the turk understanding mechanical turk as a participant pool. Curr. Dir. Psychol. Sci. 23, 184–188.

Perrin, A., 2015. Social Media Usage: 2005-2015.

Poikela, M., Toch, E., 2017. Understanding the valuation of location privacy: a crowdsourcing-based approach. In: Proceedings of the 50th Hawaii International Conference on System Sciences.

Praveena, A., Smys, S., 2016. Anonymization in social networks: a survey on the issues of data privacy in social network sites. J. Int. J. Eng. Comput. Sci. 5, 15912–15918.

Preibusch, S., 2013. Guide to measuring privacy concern: review of survey and observational instruments. Int. J. Hum. Comput. Stud.

Quinn, K., 2016. Why we share: a uses and gratifications approach to privacy regulation in social media use. J. Broadcast. Electron. Media 60, 61–86.

Raynes-Goldie, K., 2010. Aliases, Creeping, and wall Cleaning: Understanding Privacy in the Age of Facebook, 15. First Monday.

Saeri, A.K., Ogilvie, C., La Macchia, S.T., Smith, J.R., Louis, W.R., 2014. Predicting Facebook users' online privacy protection: risk, trust, norm focus theory, and the theory of planned behavior. J. Soc. Psychol. 154, 352–369.

Skeels, M.M., Grudin, J., 2009. When social networks cross boundaries: a case study of workplace use of facebook and linkedin. In: Proceedings of the ACM 2009 International Conference on Supporting Group Work, pp. 95–104.

Smith, A., Anderson, M., 2018. Social media Use in 2018, 1. Pew Research Center.

Stutzman, F., 2006. An evaluation of identity-sharing behavior in social network communities. J. Int. Digit. Media Arts Assoc. 3, 10–18.

Stutzman, F., Capra, R., Thompson, J., 2011. Factors mediating disclosure in social network sites. Comput. Hum. Behav. 27, 590–598.

Stutzman, F., Gross, R., Acquisti, A., 2013. Silent listeners: the evolution of privacy and disclosure on Facebook. J. Priv. Confidentiality 4, 2.

Stutzman, F., Hartzog, W., 2012. Boundary regulation in social media. In: Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work, New York, NY, USA, pp. 769–778.

Stutzman, F., Kramer-Duffield, J., 2010. Friends only: examining a privacy-enhancing behavior in facebook. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, pp. 1553–1562.

Stutzman, F., Vitak, J., Ellison, N.B., Gray, R., Lampe, C., 2012. Privacy in interaction: exploring disclosure and social capital in facebook. ICWSM.

Taddei, S., Contena, B., 2013. Privacy, trust and control: which relationships with online self-disclosure? Comput. Hum. Behav. 29, 821–826.

Tan, X., Qin, L., Kim, Y., Hsu, J., 2012. Impact of privacy concern in social networking web sites. Internet Res. 22, 211–233.

Teutsch, D., Niemann, J., 2015. Social network sites as a threat to users' self-determination and security: a framing analysis of German newspapers. J. Int. Commun. 1–20.

Tsay-Vogel, M., Shanahan, J., Signorielli, N., 2018. Social media cultivating perceptions of privacy: a 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. New Media Soc. 20, 141–161.

Utz, S., 2015. The function of self-disclosure on social network sites: not only intimate, but also positive and entertaining self-disclosures increase the feeling of connection. Comput. Hum. Behav. 45, 1–10.

Utz, S., Krämer, N., 2009. The privacy paradox on social network sites revisited: the role of individual characteristics and group norms. Cyberpsychology: J. Psychosoc. Res. Cyberspace 3, 2.

Watson, J., Besmer, A., Lipford, H.R., 2012. Your circles: sharing behavior on Google. In: Proceedings of the Eighth Symposium on Usable Privacy and Security, p. 12.

Williams, D., 2006. On and off the Net: scales for social capital in an online era. J. Computer-Mediated Commun. 11, 593–628.

Wilson, D., Valacich, J.S., 2012. Unpacking the Privacy Paradox: Irrational Decision-Making within the Privacy Calculus.

Wisniewski, P., Islam, A.K., Knijnenburg, B.P., Patil, S., 2015. Give social network users the privacy they want. In: Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing, pp. 1427–1441.

Wisniewski, P., Knijnenburg, B.P., Richter Lipford, H., 2014. Profiling Facebook Users' Privacy Behaviors. In: SOUPS2014 Workshop on Privacy Personas and Segmentation.

Wisniewski, P., Lipford, H., Wilson, D., 2012. Fighting for my space: coping mechanisms for SNS boundary regulation. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 609–618.