Int. J. Human–Computer Studies 98 (2017) 95–108

Contents lists available at ScienceDirect

Int. J. Human–Computer Studies

journal homepage: www.elsevier.com/locate/ijhcs

Making privacy personal: Profiling social network users to inform privacy education and nudging

Pamela J. Wisniewski[a,*], Bart P. Knijnenburg[b], Heather Richter Lipford[c]

[a] The University of Central Florida, College of Engineering and Computer Science, 4000 Central Florida Blvd., Orlando, FL 32816, USA
[b] Clemson University, School of Computing, 215 McAdams Hall, Clemson, SC 29634, USA
[c] The University of North Carolina at Charlotte, Software Information Systems Department, 9201 University City Blvd., Charlotte, NC 28223, USA

ARTICLE INFO

Keywords:
Social Network Sites
Privacy
Feature awareness
Understanding users
Personalization
Mixture Factor Analysis

ABSTRACT

Social Network Sites (SNSs) offer a plethora of privacy controls, but users rarely exploit all of these mechanisms, nor do they do so in the same manner. We demonstrate that SNS users instead adhere to one of a small set of distinct *privacy management strategies* that are partially related to their level of privacy feature awareness. Using advanced Factor Analysis methods on the self-reported privacy behaviors and feature awareness of 308 Facebook users, we extrapolate six distinct privacy management strategies, including: *Privacy Maximizers*, *Selective Sharers*, *Privacy Balancers*, *Self-Censors*, *Time Savers/Consumers*, and *Privacy Minimalists* and six classes of privacy proficiency based on feature awareness, ranging from *Novices* to *Experts*. We then cluster users on these dimensions to form six distinct behavioral profiles of *privacy management strategies* and six awareness profiles for *privacy proficiency*. We further analyze these privacy profiles to suggest opportunities for training and education, interface redesign, and new approaches for personalized privacy recommendations.

1. Introduction

Privacy is a major concern for Social Network Site (SNS) users (Madden, 2012). Interestingly, this concern exists despite the wide range of privacy control mechanisms that SNS users have at their disposal (Karr-Wisniewski et al., 2011; Wisniewski et al., 2016). Although these mechanisms offer users ample control over how they interact and share information with one another online, a number of studies have still identified a "privacy paradox" in users' SNS usage behavior: Many SNS users disclose personal information without adequate privacy-protecting behaviors, despite their stated privacy concerns (Acquisti and Gross, 2006; Barnes, 2006; Liu et al., 2011). In response to this, scholars have suggested several solutions to the privacy paradox, with the prevailing paradigm still being one of "notice and choice" (Cranor, 2012), where users are notified about information sharing privacy implications so that they can make informed privacy decisions. Implementations of this principle have ranged from educating users so that they may take appropriate privacy protection measures to nudging them to implement such measures. However, these approaches have had limited success, often producing little change in users' actual privacy behaviors (Jedrzejczyk et al., 2010; Tsai et al., 2009; Wang et al., 2013a, 2013b). This may in part be due to SNS users' difficulties in managing the plethora of privacy options available to them (Madden, 2012; Madejski et al., 2012; Strater and Lipford, 2008; Wisniewski et al., 2012). Users' efficacy in privacy management is hampered by their bounded rationality (Acquisti and Grossklags, 2008) and limited motivation to control privacy (Compañó and Lusoli, 2010; Gross and Acquisti, 2005). Thus, SNS users may be unable or unwilling to fully understand and exploit the mechanisms available to address their privacy concerns, even when such mechanisms are at their disposal.

This paper presents an empirical analysis of Facebook users' privacy feature awareness and behaviors that may lend insight into why these approaches have had only limited success. Our analysis demonstrates that Facebook users *vary substantially* in how they learn and use different privacy mechanisms. This finding complicates attempts to educate and/or nudge SNS users because it suggests that both education and nudging need to be *personalized* to the end-user. For example, trying to educate novice end-users on advanced privacy features before they have mastered the intermediate privacy features may contribute to their cognitive overload. Similarly, attempting to educate privacy proficient end-users on basic privacy features is as equally inefficient. Furthermore, if SNS users selectively employ certain privacy features intentionally, then nudging them to use other privacy features may contradict their personal privacy choices, thereby limiting their decision autonomy cf., (Smith et al., 2013; Solove, 2012). As an

* Corresponding author.
E-mail addresses: pamwis@ucf.edu (P.J. Wisniewski), bartk@clemson.edu (B.P. Knijnenburg), heather.lipford@uncc.edu (H.R. Lipford).

http://dx.doi.org/10.1016/j.ijhcs.2016.09.006
Received 29 May 2015; Received in revised form 4 May 2016; Accepted 12 September 2016
Available online 14 September 2016
1071-5819/

alternative solution, our analysis uncovers distinct user *profiles* of both privacy-protecting behaviors (i.e. privacy management strategies) and privacy feature awareness (i.e. privacy proficiency levels). These profiles offer an empirical basis for *tailoring* user education and/or nudging efforts to the user. Our results apply specifically to Facebook users, but our work also provides a methodology that can be applied more generally to SNS user profiling and personalization for other social networking platforms as well.

2. Related literature on SNS privacy

2.1. The paradox of control

To help SNS users regulate their privacy boundaries, privacy experts recommend giving users comprehensive control over their privacy (Acquisti and Gross, 2006; Benisch et al., 2011; Brodie et al., 2004; Kolter and Pernul, 2009; Tang et al., 2012; Xu, 2007). However, in order to allow users to manage their privacy with sufficient detail, SNSs like Facebook have to resort to "labyrinthian" privacy controls (Consumer Reports, 2012). As a result, 48% of SNS users report difficulties in managing their SNS privacy settings (Lipford et al., 2008; Madden, 2012). In fact, most Facebook users do not seem to know the implications of their own privacy settings (Liu et al., 2011; Strater and Lipford, 2008) and share content in a manner that is often inconsistent with their own disclosure intentions (Madejski et al., 2012).

Moreover, while users claim to *want* full control over their data (Acquisti and Gross, 2006; Benisch et al., 2011; Brodie et al., 2004; Kolter and Pernul, 2009; Pavlou et al., 2007; Tang et al., 2010; Toch et al., 2010; Wenning and Schunter, 2006; Xu, 2007), they do not actually *exploit* this control (Compañó and Lusoli, 2010). In combination with overly permissive defaults (Bonneau and Preibusch, 2010; Gross and Acquisti, 2005), the lack of either motivation or the knowledge to properly control one's privacy leads to a predominance of oversharing.

2.2. Privacy education and nudging

As we mentioned earlier, "notice and choice" are key principles in information privacy protection that have been met with limited success (Cranor, 2012). Researchers have attempted to improve on aspects of the principles of notice and choice through enhanced privacy education and nudging. For instance, *privacy education* within the SNS context often manifests in the form of notifying users of information sharing practices, through such means as textual notices embedded in privacy authorization dialogues (Knijnenburg and Kobsa, 2013; Wang et al., 2013a), nutrition labels (Kelley et al., 2009), and visual icons (Tsai et al., 2010). A fundamental problem with these approaches is that users must then accurately digest this information and use it to make informed privacy decisions, shifting the onus of privacy protection to the user (Cranor, 2012; Felt et al., 2012). Additionally, a dearth of research exists on educating users on how to properly use the plethora of privacy controls that extend beyond information sharing practices, and—to our best knowledge—none of the existing privacy education approaches take users' existing proficiencies into account.

Another approach to support privacy decisions is *privacy nudging*. Nudges are subtle yet persuasive cues that make people more likely to behave one way or the other (Thaler and Sunstein, 2008). Carefully designed nudges make it easier for people to perform a particular behavior, such as one that preserves privacy without limiting their ability to choose freely. In social media, one prominent type of nudge is to give users feedback regarding the real or potential audience, or the sentiment of a shared piece of information. The effectiveness of this feedback is mixed: users appreciate the information, but it can easily become excessive or annoying, and therefore generally has no significant impact on users' sharing behaviors (Jedrzejczyk et al., 2010; Tsai et al., 2009; Wang et al., 2014b, 2013b).

Default settings are another approach to nudging users' privacy decisions that has only limited success (Wang et al., 2014a; Wang et al., 2011). Defaults (partially) relieve users from the burden of making information disclosure decisions by offering a path of least resistance: Correctly chosen defaults make it easier to choose the right action, or may not even require any action at all. Existing work shows that such defaults influence users' sharing tendency on SNSs but only for users with high privacy concerns (Knijnenburg and Kobsa, 2014). Additionally, inappropriate defaults (i.e., sharing more information than a user feels is necessary), may heighten users' privacy concerns and cause them to disengage from various aspects of sharing through SNSs (Wang et al., 2014a; Wisniewski et al., 2015a, 2015b).

2.3. Privacy profiling as a necessary prerequisite

One reason why education and nudging may have a limited effect on SNS users' privacy protection behaviors is because users have unique strategies and preferences for how they manage their privacy. For example, when it comes to avoiding emotionally charged arguments online, some users prefer to limit strong sentiments in their posts, while others prefer to restrict their audience as a way to avoid self-censorship (Wisniewski, 2012; Wisniewski et al., 2012). If a nudge is contrary to a user's established privacy management strategy (e.g. suggests restricting the audience to someone who already limits their content), then it may be viewed as a hindrance. The optimal hint, default setting, or feedback may be *different* for each particular end-user and, hence, research suggests personalized nudges may be more effective (Almuhimedi et al., 2015; Knijnenburg, 2015). For example, our results could be used to distinguish between features the user has consciously decided not to use (nudges towards these features may annoy the user), features the user is less familiar with but may fit their current strategy (nudges and/or education regarding these features can help solidify users' existing privacy protection strategy), and other features the user does not know about (education on these features could inform the user about alternative strategies that may better fit their privacy desires).

There is ample evidence that people vary extensively in their information disclosure behavior; for instance, Westin et al.'s (Harris et al., 2003, 1997; Westin et al., 1981) categorization of privacy fundamentalists, pragmatists, and unconcerned is one of the most cited works in the privacy literature. However, recent work has questioned the validity of this categorization due to lack of empirical evidence supporting the categorization (Woodruff et al., 2014). Other scholars have argued that privacy categorization should not just consider a difference in degree, but also a difference in kind (Knijnenburg et al., 2013; Woodruff et al., 2014). As such, we create unique user profiles, as first suggested by Spiekermann et al. (2001), to cluster users by their privacy behaviors and awareness of related privacy controls.

In the context of SNSs, a variety of research has examined users' use of various privacy controls, and their relationships with privacy concerns, demographics, or other behaviors and outcomes (for an overview, see De Feyter et al. (2013)). Yet, most of this work has focused specifically on one kind of SNS privacy control—*selective information sharing*. For instance, researchers have examined selective information sharing through friend lists or circles (De Feyter et al., 2013; Kairam et al., 2012; Knijnenburg and Kobsa, 2014; Watson et al., 2012) and the subset of privacy settings that relate specifically to *information disclosure* behaviors (Kairam et al., 2012; Knijnenburg, 2013a; Lampinen et al., 2011; Lipford et al., 2008; Stutzman et al., 2012b, 2011; Tufekci, 2008). In contrast, our work acknowledges that selective information sharing is just one of many strategies SNS users may employ to alleviate privacy tensions (Lampinen et al., 2011; Marwick and boyd, 2014; Tufekci, 2008). Our previous work broadened the scope of interpersonal privacy protection behaviors to the management of relational boundaries (e.g. friending and unfriending),

territorial boundaries (e.g. untagging posts or photos or deleting unwanted content posted by others), network boundaries (e.g. hiding one's friend list from others), and interactional boundaries (e.g. blocking other users or hiding one's online status to avoid unwanted chats) (Karr-Wisniewski et al., 2011; Wisniewski et al., 2016). That work used Altman's broader definition of privacy as "an interpersonal boundary process by which a person or group regulates interaction with others," by altering the degree of openness of the self to others (Altman, 1975). We also apply Altman's definition of privacy in our current work and extend on our prior work by quantitatively measuring specific mechanisms that Facebook users leverage to regulate their privacy boundaries, as well as their level of awareness of these mechanisms. By doing this, we are able to create distinct user profiles based on both privacy management strategies (i.e., behaviors) and privacy proficiency levels (i.e., awareness). These profiles can serve to inform privacy education and nudging practices.

Outside of the context of SNSs, researchers have modeled profiles of user privacy preferences to inform automated or default privacy settings, such as for mobile location sharing (Ravichandran et al., 2009) and Android app permissions (Lin et al., 2014; Liu et al., 2014) on mobile devices. Similarly, this research suggests that such profiles could then be used as a set of default policies provided to users (Wilson et al., 2013) or to predict future privacy decisions. Our research expands upon these efforts by exploring not just specific settings, but a variety of privacy-related behaviors users can take on SNSs, which cannot be captured through privacy settings alone. Our work examines a wider subset of privacy management strategies based on the more nuanced definition of privacy discussed above. We empirically validate that Facebook users form distinct *strategies* around this broader range of SNS privacy behaviors that regulate both informational and interactional privacy boundaries. Moreover, our current work not only examines users' privacy behaviors in the context of SNSs, but also their *awareness* of the various privacy controls that support these behaviors. By linking privacy awareness to behavior, we can better determine to what extent users' privacy strategies consist of consciously selected behaviors and to what extent they are restricted by users' limited knowledge of the available controls.

2.4. Research approach and contribution

The main contribution of this paper is to illustrate the wide variety in SNS users' interpersonal privacy boundary management, both in terms of awareness and behavior, and to subsequently investigate the inherent structure of and relationship between their privacy awareness and behavior. Specifically, through our in-depth, empirical analysis, we:

1. Confirm the *multi-dimensional structure* of Facebook users' privacy behaviors and feature awareness posited by Wisniewski et al. (2012).
2. Show that feature awareness is a significant predictor of Facebook users' privacy behaviors, but also that behaviors are not completely dictated by awareness.
3. Create unique *user profiles* by classifying participants on the established dimensions of privacy behavior (*privacy management strategies*) and feature awareness (*privacy proficiency profiles*).
4. Perform a class-to-class comparison of privacy proficiency profiles with privacy management strategies to show how privacy management strategies align with different privacy proficiency profiles.

Consequently, our paper makes the following key contributions: First, we add to the growing body of work on the privacy of *Facebook users* e.g., (Baumer et al., 2013; Blasiola, 2013; De Wolf et al., 2014; Nemec Zlatolas et al., 2015; Sleeper et al., 2013; Stutzman et al., 2012a; Wang et al., 2014b; Wisniewski et al., 2014), by demonstrating how Facebook users' privacy behaviors and feature awareness comprise a multi-dimensional structure, and how they can be assigned to a limited set of privacy management strategies and privacy proficiency profiles. We make suggestions for a more synergetic design of Facebook's privacy controls that should allow for a more intuitive implementation of these strategies. For *SNS users in general*, we argue that privacy protection behaviors as well as privacy proficiency levels vary widely, making *profiling* a prerequisite for educating or nudging users to take protective privacy measures. To facilitate this, we offer our privacy profiling methodology as a practical framework that can be applied to any SNS. Additionally, our results also contribute to *theory*, as we extend existing critiques (Woodruff et al., 2014) of Westin's privacy classification to include behaviors that address both informational and interactional privacy boundaries. Also, we are the first to provide a separate classification of feature awareness as a way of profiling SNS users by their varying levels of privacy proficiency. Finally, this study empirically links feature awareness to privacy behaviors and helps disentangle to what extent users' privacy management strategies are determined by conscious behaviors versus restricted by their limited knowledge of the available privacy controls.

3. Research framework

We focus on two aspects of SNS privacy in this work: *privacy behaviors* and *feature awareness*. We call the profiles resulting from our analyses of these aspects *privacy management strategies* and *privacy proficiency profiles*, respectively. We define each of these constructs in more detail below, and we study these aspects of SNS privacy in the context of Facebook, the largest SNS with 1.39 billion active, monthly users (Facebook, 2015).

3.1. Privacy behaviors and privacy management strategies

We define *privacy behaviors* as the features and/or settings that Facebook users leverage as a mechanism for managing interpersonal privacy boundaries. These behaviors include managing one's profile, Timeline/Wall, News Feed, and whom one chooses to friend or unfriend. To ground our dimensional structure we draw upon our previous work (Karr-Wisniewski et al., 2011), in which we first performed a domain analysis across five popular SNS websites (including Facebook) of the interface features available for regulating interpersonal privacy, and then qualitatively examined users' usage of these features. A key finding from this prior work was that SNS users manage *different* privacy boundaries in *different* ways; for instance, some users maintained very small networks of friends that enabled them to share more freely, while other users had broad networks that required a higher level of self-censorship (Wisniewski, 2012; Wisniewski et al., 2016). In this paper, we use a data-driven method to empirically uncover a coherent set of *privacy management strategies* from the different observed combinations of privacy behaviors uncovered in our previous work.

3.2. Feature awareness and privacy proficiency profiles

Feature awareness is the degree to which users know about or recognize a particular interface feature or functionality necessary to perform a given task (Findlater and McGrenere, 2010), and ultimately influences a user's ability to achieve desired outcomes (Grossman et al., 2009). Social interactions within SNS environments are fully mediated by the technological interface; therefore, feature awareness plays a crucial role in negotiating privacy boundaries. From a theoretical perspective of privacy regulation, Altman asserted that "environmental awareness and environmental-usage training might help people better use, shape, and reshape their environments" (1975).

Unfortunately, SNS privacy settings and features are often hidden, too complex to understand, or change so quickly that it is hard for users to keep track of them (Karr-Wisniewski et al., 2011; Liu et al., 2011; Madden, 2012; Madejski et al., 2012; Strater and Lipford, 2008). Thus,

we explore not only how various privacy features are used, but also how familiar users are with these features. As with privacy behaviors, we use a data-driven method to empirically uncover a set of *privacy proficiency profiles* that describe characteristic levels of privacy feature awareness across the full set of SNS privacy controls. Furthermore, we empirically examine how users' privacy proficiency influences their privacy management strategies. This allows us to better understand what part of users' privacy strategies may be intentional versus constrained by their limited knowledge of the available privacy mechanisms.

4. Procedure

4.1. Data collection

Data were collected through a web-based survey using Survey Share. Participants had to be over 18 and have an active Facebook account. Recruitment was done through snowball sampling (Babbie, 2004) seeded through a random sample of university email addresses, the first author's personal SNSs, email, and the Craigslist's volunteer's message board. The justification for this approach was to obtain as diverse of a sample as possible and to expedite data collection (Babbie, 2004). Limitations of snowball sampling are addressed later in our discussion. Per the standard IRB procedure of the university, the email addresses were obtained from the registrar's office and included student (both graduate and undergraduate), faculty, and staff email addresses. Participation was incentivized through a drawing of two $200 Amazon gift certificates. Each participant who opted in received one drawing entry. As an incentive to share the survey, participants received one additional entry (up to 25) for each successful referral.

4.2. Operationalization of constructs

Our earlier work, which included a comprehensive domain-oriented feature analysis of 5 SNSs (Karr-Wisniewski et al., 2011), methodically identified a wide range of Facebook privacy settings and features. We leveraged these findings in our current study to provide participants with written directions and a screenshot on how to access various privacy settings and features in their own Facebook account. Fig. 1 shows an example of a screenshot that was embedded in the survey for the privacy options related to managing the content that filters into *one's Facebook News Feed*, which was accompanied by the following instructions:

> "The next set of questions will ask you to report some basic information about how you manage updates in your Facebook News Feed from your friends. To do this: You would have had to click on the drop down arrow at the top, right corner of a post on your News Feed as shown below."

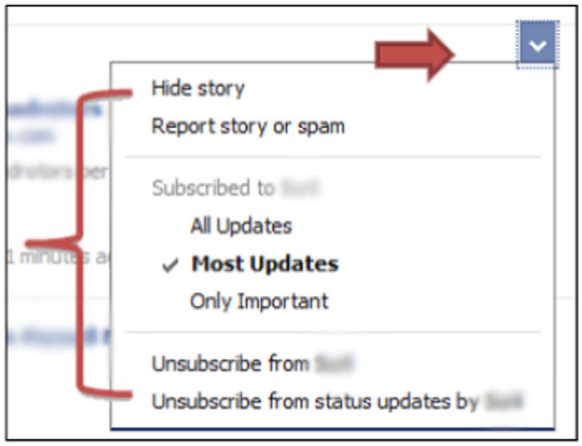

Fig. 1. Privacy options for managing facebook news feed.

Questions were presented in an order that minimized the number of clicks participants needed to access each privacy feature. For each privacy setting or feature, we asked participants about specific actions they had performed in the past. Privacy behaviors that involved a specific setting were measured based on the actual options provided by the Facebook interface (e.g. users answered questions regarding their visibility settings for their "Basic Info" by choosing from "I did not provide this information to Facebook," "Public," "Friends," "Only Me," "Custom," and "Any customized friend list." These responses were coded from 1 least private to *N* most private).

If a privacy feature supported multiple behaviors, we asked a separate question for each behavior. Privacy behaviors that were recurring (e.g. hiding a story on one's News Feed) were measured on a 7-point scale ranging from 1=Never to 7=Always,[1] or by a scale reflecting frequency counts (e.g. we asked users to report how many users they had blocked, ranging from 1=None to 5=More than ten). E.g., for the News Feed (Fig. 1) we asked, "*How often have you done the following to modify posts on your News Feed?*" followed by questions asking users about the frequency with which they had: (1) Hid a story, (2) Reported Story or Spam, (3) Changed friend subscription settings, (4) Unsubscribed from a friend, or (5) Unsubscribed from status updates from a friend. All questions regarding privacy behaviors are displayed in Table 1.

The feature awareness questions are displayed in Table 3. These were measured on a 3-point scale, ranging from "Yes, I definitely recall seeing this item" to "I vaguely recall seeing this item" to "No, I didn't see this item." This scale was adapted from previous literature (Findlater and McGrenere, 2007, 2010). Since we were treating privacy behavior as our dependent variable of interest, we collected data related to this construct prior to asking participants about their level of feature awareness. Note that there are fewer awareness questions than behavior questions because some privacy controls were grouped on the same menu, such as Fig. 1, thereby requiring only a single awareness question.

4.3. Data analysis approach

We adapted our approach from earlier work, cf., Knijnenburg et al.'s (2013a, 2013b), to analyze the privacy behavior and feature awareness items in our dataset. First, using a Confirmatory Factor Analysis (CFA) with a weighted least squares estimator (Kline, 2011; Muthen and Muthen, 2010), we verified the multidimensional structure of privacy behaviors and feature awareness that was suggested by Karr-Wisniewski et al. (2011); Wisniewski (2012). CFA analyzes the covariance between items to create a number of conceptually different dimensions or "factors." We adjusted the resulting factors (i.e. removing items, splitting and combining factors) until we achieved a satisfactory model fit. Second, we tested for a link between the feature awareness and privacy behavior factors using Structural Equation Modeling (SEM) (Kline, 2011). Third, we performed a series of Mixture Factor Analyses (MFAs) with a robust maximum likelihood estimator (Muthen and Muthen, 2010) to cluster participants based on their varying dimensions of privacy behaviors and feature awareness. This analysis resulted in a number of privacy profiles that describe our participants based on their unique *privacy management strategies* (derived from their scores on the privacy behavior factors) and *privacy proficiency levels* (derived from their scores on the feature awareness factors). Finally, we examined the overlap in class membership between these two classifications to determine which privacy management strategies are most prominent for each proficiency level, and vice versa.

[1] In our statistical analysis we treat all variables as ordinal, so specific numbers do not matter.

5. Results

5.1. Descriptive statistics

We collected a total of 314 survey responses. After screening the data for outliers and excessive missing data, a total of 308 participants remained. The sample included 119 males and 189 females, with an average age of 35.74 (standard deviation: 12 years, range: 18–75). About 31% of the participants identified themselves as college students with 81% having at least a two-year degree. The majority (91.6%) of participants reported having a Facebook account for over 2 years, with 19.2% having an active Facebook account over 6 years. These demographics are fairly representative of typical Facebook users. For example, Pew Research has reported that 64% of Facebook users are female with an average age of 38 years, 78% are white, and 69% have at least some college education (Hampton et al., 2011). The differences in our sample from the population of all Facebook users was most likely due to primarily recruiting from a university setting. We found that 66% of the sample were from these direct recruitment efforts, 20% by word-of-mouth from others known by the first author, and only 14% of participants reported being referred by another survey participant (i.e., snowball).

5.2. Examining the multi-dimensionality of privacy behaviors and feature awareness

We measured a total of 36 privacy behaviors and 20 feature awareness items based on features in the Facebook interface. We performed a CFA for both privacy behavior and feature awareness to confirm that the respective items conceptually grouped with the higher-level privacy controls as suggested by Karr-Wisniewski et al. (2011), Wisniewski (2012). In the following sections, we present the results of these CFAs.

5.2.1. Privacy behavior CFA

The dimensional structure and the factor loadings of the privacy behaviors are presented in Table 1, and the correlations between the factors are presented in Table 2. After removing eight items that did not load well on any of the factors, the final 11-factor model shows a good fit[2] ($\chi^2(295)$ 432.59, $p < 0.001$; *CFI*=0.987, *TLI*=0.983; *RMSEA*=0.039, 90% CI: [.031, 0.047]), as well as good convergent and discriminant validity (all AVEs > 0.50, all sqrt(AVE)s > largest correlation with other factors).

The resulting eleven dimensions of Facebook privacy behaviors are: (1) Altering one's News Feed; (2) Moderating one's Timeline/Wall; (3) Reputation management through untagging or asking a friend to take down an unwanted photo or post; (4) Limiting access control or visibility of information shared through one's Timeline/Wall; (5) Blocking people; (6) Blocking apps or event invitations; (7) Restricting chat availability; (8) Selective sharing through customized friend lists; (9) Custom friend list creation and management; (10) Withholding contact information; and (11) Withholding basic information. As shown in Table 2, most of these dimensions are significantly positively correlated with one another, meaning that participants who score high on one dimension are also more likely to score high on the other dimensions. Still, the fact that the factors show good discriminant validity means that they constitute conceptually separate dimensions, nonetheless (e.g. Altering News Feed is conceptually different from Timeline/Wall Moderation).

[2] A good model has a χ^2 that is not statistically different from a saturated model ($p > 0.05$). However, this statistic is regarded as too sensitive, and researchers have proposed other fit indices (Bentler and Bonett, 1980). Hu and Bentler (1999) propose cut-off values for these indices to be: *CFI* > 0.96, *TLI* > 0.95, and *RMSEA* < 0.05, with the upper bound of its 90% CI falling below 0.10.

Table 1
Privacy behavior CFA results.

Factor	Item	Loading
Altering News Feed (NWF) AVE: 0.777	Hid a story from News Feed	0.845
	Changed friend subscription	0.872
	Reported a story or marked as spam	Removed
	Unsubscribed to a friend	0.908
	Unsubscribed to status updates	0.900
Timeline/Wall Moderation (WAL)AVE: 0.638	Deleted content from Timeline/Wall	0.783
	Reported/marked content as spam	0.796
	Hid a story from Timeline/Wall	0.817
Reputation Management (REP)AVE: 0.671	Untagged a photo or post	0.800
	Requested friends to take down posts or photos	0.838
Limiting Access Control (LIM)AVE: 0.734	Tag visibility privacy setting	0.683
	Wall/Timeline post visibility privacy setting	1.012
	Default privacy level	Removed
Blocking People (BLP)AVE: 0.838	Blocked a user	0.892
	Added a user to restricted list	0.938
Blocking Apps/events (BLA) AVE: 0.621	Blocked an event invite	0.746
	Blocked an app invite	0.828
Restricting Chat (CHA)AVE: 0.777	Gone "offline" on Facebook chat	1.013
	Default chat visibility	0.744
Selective Sharing (SEL)AVE: 0.829	Posted a status to a custom friend list	0.867
	Posting a photo to a custom friend list	0.952
Friend Management (FRM) AVE: 0.910	Categorized new friends into friend lists	0.915
	Categorized existing friends into friend lists	0.991
Withholding Contact Info. (CON)AVE: 0.780	Withheld/restricted cell phone number	0.742
	Withheld/restricted other phone number	0.946
	Withheld/restricted IM screen name	0.880
	Withheld/restricted email address	Removed
	Withheld/restricted street address	0.949
Withholding Basic Info. (BAS)AVE: 0.700	Withheld/restricted "Interested In"	0.750
	Withheld/restricted religion	0.878
	Withheld/restricted political views	0.876
	Withheld/restricted birthday	Removed
	Withheld/restricted relationship status	Removed
Concealing Network	Hid Friend list from profile (single item)	Removed
Denying Connection	Hidden a friend request	Removed
	Unfriended (frequency)	Removed

5.2.2. Feature awareness CFA

The factor loadings of the final CFA solution for feature awareness are presented in Table 3, and factor correlations are presented in Table 4. After removing three ill-fitting items, the final 6-factor model shows a good fit ($\chi^2(104)$=153.29, p=0.0012; *CFI*=0.995, *TLI*=0.994; *RMSEA*=0.039, 90% CI: [0.025, 0.052]), as well as good convergent and discriminant validity.

The six dimensions of privacy feature awareness are: (1) Managing profile information, such as basic and contact information; (2) Moderating friends by filtering one's News Feed, moderating one's Timeline/Wall, allowing friend requests to stay in pending status, and unfriending; (3) Limiting access control or visibility of information shared through one's Timeline/Wall; (4) Blocking people, apps, and event invites; (5) Reputation management through untagging photos or posts and requesting that friends take down unwanted photos or posts;

Table 2
Privacy behavior factor correlations.

WAL	0.62***									
REP	0.46***	0.78***								
LIM	0.21***	0.21***	0.26***							
BLP	0.42***	0.41***	0.35***	0.23***						
BLA	0.46***	0.55***	0.54***	–	0.65***					
CHA	0.35***	0.32***	0.32	0.20***	0.26***	0.33***				
SEL	0.44***	0.55***	0.59	0.28***	0.50***	0.47***	0.25***			
FRM	0.45***	0.49***	0.35	0.23***	0.44***	0.40***	0.21**	0.76***		
CON	0.17***	0.30***	0.34	–	0.27***	–	–	0.40***	0.26***	
BAS	0.15*	0.29***	0.27	–	0.25***	–	–	0.27***	0.16*	0.67***
	NFW	**WAL**	**REP**	**LIM**	**BLP**	**BLA**	**CHA**	**SEL**	**FRM**	**CON**

* $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$.

Table 3
Feature awareness CFA results.

Factor	Item	Loading
Managing Profile Information (PRO) AVE: 0.867	User Profile - Basic Information	0.856
	User Profile - Contact Information	1.050
Moderating Friends (MOD) AVE: 0.625	News Feed privacy options menu	0.838
	Wall/Timeline content management	0.826
	Hiding friend requests (as opposed to accepting)	0.780
	Pending friend requests	0.696
	Unfriending	0.805
Limiting Access Control (LIM) AVE: 0.941	Tag visibility privacy setting	0.951
	Wall/Timeline post visibility privacy setting	0.988
Blocking People/Apps/Events (BLO) AVE: 0.839	Blocking a user	0.960
	Adding a user to restricted list	0.903
	Blocking event invites	0.938
	Blocking app invites	0.860
Restricting Chat (CHA)	Changing chat availability/ visibility (single item)	Removed
Reputation Management (REP) AVE: 0.785	Untagging posts or photos	0.936
	Requesting friends to take down posts or photos	0.833
Selective Sharing (SEL) AVE: 0.910	Posting a status to a custom friend list	0.947
	Posting a photo to a custom friend list	0.960
	Managing/creating friend lists	Removed
Concealing Network	Friend list visibility (single item)	Removed

Table 4
Feature awareness factor correlations.

REP	0.75***				
LIM	0.59***	0.61***			
BLO	0.69***	0.62***	0.69***		
SEL	0.69***	0.61***	0.50***	0.59***	
PRO	0.79***	0.67***	0.63***	0.70***	0.57***
	MOD	**REP**	**LIM**	**BLO**	**SEL**

*** $p < 0.001$.

and (6) Selective sharing by managing and creating custom friend lists in order to share photos or posts to specific groups of friends. As shown in Table 4, all of the feature awareness dimensions were significantly correlated with one another, but they still loaded on separate factors as shown in Table 3. Like our results for privacy behavior, this confirms that the dimensions of feature awareness, while related, are conceptually different from each other (e.g. users' awareness of features for Managing Profile Information is conceptually different from their awareness of features for Moderating Friends).

Note also that the dimensions of feature awareness correspond to the physical groupings used within the Facebook interface while the dimensions of privacy behavior *differed* from the physical layout. For example, "basic information" and "contact information" are situated in the same location on Facebook. For feature awareness, these two features merged together in the same dimension (i.e., "Managing Profile Information"). However, the discriminant validity of the CFA confirmed that they represented two *separate* privacy behaviors (i.e., "Withholding Contact Info." and "Withholding Basic Info."). In general, the dimensions of privacy behavior (11 factors) are more granular than those of feature awareness (only 6 factors). This is in part due to how granularly these constructs were measured (i.e. 36 items for privacy behavior and 20 for feature awareness), but it may also suggest that feature awareness may be more closely dictated by interface layout, while actual privacy behaviors are related to the interface layout but vary more based on users' refined privacy preferences. For instance, a Facebook user may be equally aware of how to adjust her privacy settings for basic information and contact information, as these two features are physically grouped together within the Facebook interface and operate in a similar manner. However, she may still exhibit different behaviors regarding these two types of information, given her specific privacy preferences.

5.3. Linking feature awareness and privacy behavior

Next, we tested the relationship between the various dimensions of feature awareness (X) and privacy behavior (Y) by means of a Structural Equation Model (SEM). We decided to retain the items that were previously removed in the SEM to explore how they related to the respective dimensions of feature awareness and privacy behavior.

Table 5
Regressing privacy behaviors on feature awareness.

Awareness (X)	Behavior (Y)	*β*	*p*-Value
Moderating Friends	Altering News Feed	0.60	< 0.001
	Timeline/Wall Moderation	0.56	< 0.001
	Denying Connection: Hiding friend requests[a]	0.32	< 0.001
	Denying Connection: Unfriending[a]	0.54	< 0.001
Reputation Management	Reputation Management	0.64	< 0.001
Limiting Access Control	Limiting Access Control	0.39	< 0.001
Blocking People/Apps/ Events	Blocking People	0.62	< 0.001
	Blocking Apps/Events	0.66	< 0.001
Restricting chat[a]	Restricting chat	0.53	0.001
Selective Sharing	Selective Sharing	0.74	< 0.001
	Friend Management	0.58	< 0.001
	Withholding Contact Info	0.16	0.057
Managing Profile Info	Withholding Basic Info	0.18	0.013
Concealing Network[a]	Concealing Network[a]	0.35	0.001

[a] Items previously removed during the CFAs.

Table 5 shows the significant regression effects of the SEM; this model has a good fit ($\chi^2(1096)=1684.24$, $p < 0.001$; *CFI*=0.968, *TLI*=0.962; *RMSEA*=0.042, 90% CI: [0.038, 0.046]. Most effects are large ($\beta > 0.50$) and in line with our expectations; corresponding dimensions of feature awareness significantly predicted the associated privacy behaviors, suggesting that privacy feature awareness is a prerequisite of subsequent privacy behaviors.

Overall, the results from the SEM confirmed an already obvious relationship between feature awareness and actual use and, thus, serve primarily as an intermediate step in our analysis. However, our SEM results begin to illustrate how the relationship between feature awareness and privacy behavior is not simply one-to-one. For instance, the behavior "Withholding Contact Info" is more influenced by awareness of "Selective Sharing" via lists than by awareness of "Withholding Profile Info." While users are generally aware of this basic privacy option (e.g. sharing contact information publically, with friends only, friends of friends, etc.), awareness of selective sharing plays a larger role in influencing their privacy behaviors related to sharing contact information than the awareness of the feature itself. This may be because Facebook users can use selective sharing as an alternative option for withholding their contact information.

5.4. Classifying facebook users: privacy management strategies and proficiency profiles

Next, we used the confirmed factors from the CFAs to classify users into distinct profiles based on their behaviors and feature awareness. To this end, we ran a series of Mixture Factor Analyses (MFAs) with an increasing number of classes. Mixture Factor Analysis is a type of factor analysis that introduces a classification-based "mixture" of factor means to the factor solution. In other words: rather than allowing the factor scores of participants to vary freely, a classification algorithm assigns each participant to one of K classes, and then calculates mean factor scores for these K classes. The class memberships are chosen in a way that minimizes the residual difference between the "observed" and predicted factor scores per participant. Mixture Factor Analysis does not make substantive arguments about the optimal number of classes, but does provide quality indicators that can be used (with careful deliberation) to select the optimum. These quality indicators are: (1) subsequent models do not fit significantly better (p-value > 0.05), (2) the BIC (Bayesian Information Criterion) is at a minimum, (3) the entropy is highest, and (4) the loglikelihood levels off (Knijnenburg et al., 2013). These metrics may not agree, and decisions should therefore be made primarily based on substantive grounds (e.g. theory; inspection of several solutions) informed by the metrics (Nylund et al., 2007). The resulting MFA classes represent distinct "user profiles" that describe the members of each class.

5.4.1. Privacy behavior MFA: privacy management strategies

Table 6 compares the different MFAs for privacy behavior. No significant improvements are made beyond the trivial 2-class solution. However, this significance test may be underpowered, due to the high dimensionality of the factor analysis part of the model (which results in a means structure with too many free parameters). The BIC, which tests the parsimony of the solution, continues to decrease and is at a minimum for the 6-class solution, which is also where the entropy reaches its maximum value, and where the loglikelihood levels off.

Table 6
Privacy behavior MFA model fit statistics.

Classes	BIC	Entropy	LL	p-Value
1	21998		−10534.652	
2	20829	0.915	−9916.195	< 0.0001
3	20479	0.915	−9706.503	0.1032
4	20324	0.880	−9594.600	0.7248
5	20183	0.905	−9489.752	0.1774
6	20104	0.922	−9415.822	0.4441
7	20163	0.904	−9411.090	0.7039

Since the 2-class solution is theoretically less interesting than the 6-class solution, we adopted the 6-class solution on substantive grounds, backed up by the BIC, entropy and loglikelihood metrics.

Based on our interpretation of the class compositions (see below), we semantically label the six privacy management profiles as follows: *Privacy Minimalists* (22% of participants), *Self-Censors* (11%), *Time Savers/Consumers* (17%), *Privacy Balancers* (36%), *Selective Sharers* (5%), and *Privacy Minimalists* (22%). Fig. 2 uses a stacked bar chart to show how the privacy behavior factors are distributed across these six privacy management strategy profiles. This chart is weighted to account for the total number of users that belong to each class. Limiting access control by setting Timeline/Wall tagging and post visibility to "Friends Only" is the most common behavior while blocking people, apps, and events is the least frequently employed behavior overall. The legend includes the percentage of users who belong to each of the six classes. The largest class is *Privacy Balancers* (36%) followed by *Privacy Minimalists* (22%); the smallest class is *Selective Sharers* (5%).

Figs. 3–5[3] illustrate how the different user privacy management profiles vary based on the behavioral dimensions. Fig. 3 compares *Privacy Maximizers* (10% of participants) with *Selective Sharers* (5%—the minority strategy). The *Privacy Maximizers* tend to report the highest levels of privacy behaviors across the majority of the privacy features, including withholding personal information (something no other users do to such a large extent). In contrast, the *Selective Sharers* leverage more advanced privacy settings: they create and manage customized friend lists, and use these to post content to selective groups of friends (something they do more often than even the *Privacy Maximizers*). They are also more likely to share personal information, such as basic and contact information; this may be related to their selective sharing (e.g. their selective sharing allows them to share more personal information, or their tendency to share more personal information entices them to share more selectively).

In Fig. 4, the *Privacy Balancers* (36%—the largest profile) exhibit moderate levels of privacy management behaviors: lower than *Privacy Maximizers* but higher than *Privacy Minimalists* (see Figs. 3 and 5). In contrast, the *Self-Censors* (11% of participants) use Facebook's privacy features and settings fairly infrequently, but compensate by protecting their privacy through self-censorship, e.g. withholding their basic and contact information.

In Fig. 5, the *Privacy Minimalists* (22% of participants) report the fewest privacy strategies, managing their privacy only using the most common methods, such as limiting their Facebook profile so that they only share with friends by default. The *Time Savers/Consumers* (17% of participants) are similar to the *Privacy Minimalists*, but they additionally use privacy strategies that enable them to passively consume Facebook updates without being bothered by unwanted others. For instance, they often restrict their chat availability so that others cannot initiate chat conversations with them, and alter their News Feeds so that they can more effectively consume updates from their most relevant friends only.

5.4.2. Feature awareness MFA: privacy proficiency profiles

Table 7 compares the MFAs with different numbers of classes for feature awareness. The BIC does not reach a minimum, and the entropy reaches a maximum at 3 classes, which is also where the loglikelihood starts to level off. While the 6-class solution fits the data still marginally better than the 5-class solution, the 7-class solution is clearly not better than the 6-class solution. This means that both the 3-class and 6-class solutions are viable. We adopt the 6-class solution, because it illustrates the different levels of privacy proficiency among

[3] Insightful interactive version of this chart at http://www.usabart.nl/chart/

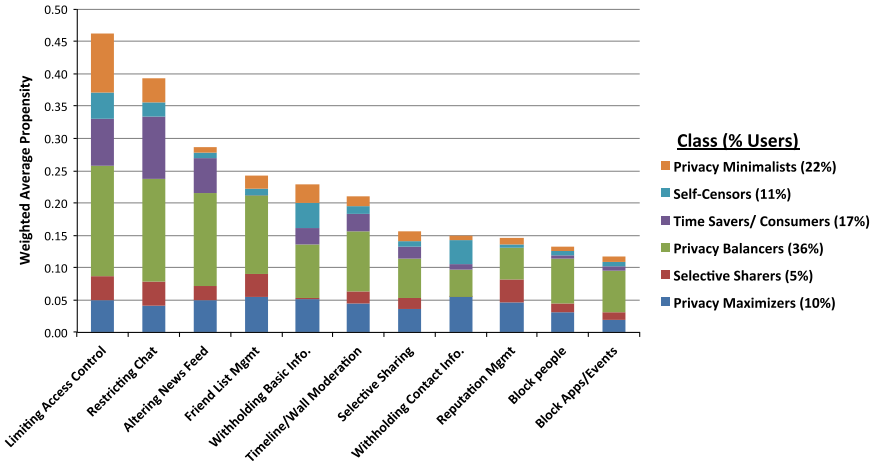

Fig. 2. Privacy management strategies by behavior and user class.

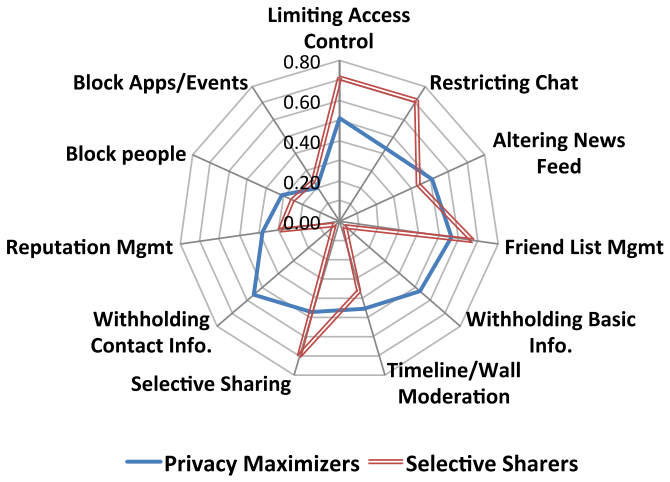

Fig. 3. Privacy Maximizers vs. Selective Sharers.

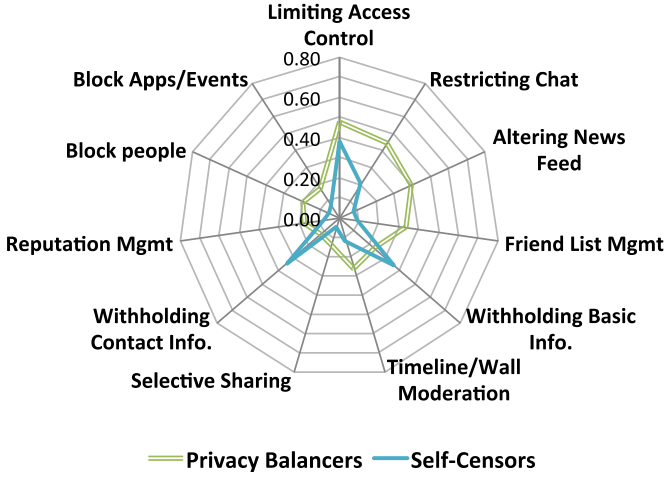

Fig. 4. Privacy Balancers vs. Self-Censors.

our participants in sufficient detail and granularity.

Fig. 6 shows how the awareness factors are distributed over users of different privacy proficiency classes. The y-axis represents the cumulative percentage of users across the six user classes who reported vaguely to definitely recalling each of the privacy features or settings listed on the x-axis. The legend includes the percentage of users who belong to each of the six classes. The privacy feature that is most commonly known across all classes is the ability to manage one's

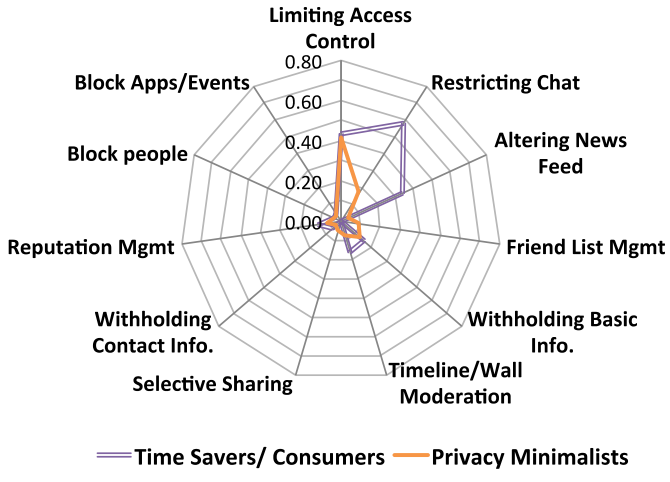

Fig. 5. Time Savers vs. Privacy Minimalists.

Facebook user profile (77%); the privacy feature that is least commonly recognized is selective sharing through the use of customized friend lists (only 30%).

Fig. 7 further illustrates the differences between the six privacy proficiency profiles. Unlike the privacy management profiles, which displayed substantially different patterns of privacy behaviors, the proficiency profiles show similar patterns that differ primarily in degree (such that the profile lines in Fig. 7 are largely concentric). *Experts* (19% of participants) have the highest level of feature awareness, while *Novices* (13% of participants) display very low awareness of the majority of Facebook privacy settings and features. The remaining profiles fill the spectrum of proficiency between the *Experts* and *Novices*. Overall, the proficiency profiles suggest a distinct order in which SNS users tend to learn privacy features: they tend to learn the more basic privacy features (i.e. managing profile info, moderating friends) before they become aware of the more advanced privacy features (i.e. reputation management, selective sharing). The only exception to this rule is *Mostly Novices,* who are more aware of selective sharing features than the arguably less advanced reputation management and blocking features. They are even more likely to be aware of selective sharing features than the generally more proficient users in the *Some Expertize* class. This finding suggests that feature awareness may be *driven* by the users' desired privacy management strategy to selectively share content via friend lists. Thus, this desire may encourage users to seek out the privacy mechanism for accomplishing their specific goals.

Table 7
Feature awareness MFA model fit statistics.

Classes	BIC	Entropy	LL	*p*-Value
1	10131		−4936.792	
2	8804	0.905	−4252.838	0.0004
3	8391	0.919	−4026.395	0.0024
4	8284	0.881	−3953.036	0.1926
5	8228	0.903	−3905.069	0.0239
6	8186	0.905	−3863.676	0.0628
7	8167	0.913	−3834.338	0.2179
8	8154	0.914	−3807.612	0.6659

5.5. Exploring the overlap between privacy proficiency and privacy management strategies

Table 8 shows the overlap between privacy proficiency profiles and privacy management strategy profiles. The numbers in the cells report the *observed* number of users in each combination of classes and (in parentheses) the *expected* number of users given that there would be no relationship between privacy proficiency and privacy management strategy. A "+" indicates that that specific combination of proficiency and management strategy occurs more often than expected (indicating an overlap between the proficiency level and the management strategy) while a "–" indicates that that combination occurs less often than expected (indicating a lack of overlap between the proficiency level and the management strategy). Each cell in the table is also shaded using a heat map gradient (i.e. green for positive differences; red for negative differences) to denote the magnitude of the difference between expected and observed values. Bold cells denote the combinations of classes that are most over/under-represented, and thus show the most or least overlap.

As expected *Privacy Maximizers* are most likely to be *Experts* or *Near-Experts*. However, the relationship is much more nuanced for *Privacy Balancers* who are most often *Experts*, *Near-Experts*, have *Some Expertize*, or alternatively are complete *Novices*. This non-linear trend continues for *Privacy Minimalists* who are most often *Mostly Novices* or *Near-Novices* but not actual *Novices*. Finally, *Selective Sharers* tend to belong to the higher privacy proficiency classes, while *Time Savers* and *Self-Censors* exhibit more intermediate levels of privacy proficiency. This lower level of proficiency may, in part, contribute to their privacy management strategies which do not require as much advanced knowledge about the interface features. Looking at the table inversely, *Experts* are most often *Privacy Maximizers* but *Novices* are more likely to be *Privacy Balancers* than *Privacy Minimalists*, negating the assumption that there is a simple one-to-one, linear relationship between feature awareness and privacy behavior.

6. Discussion

In this paper we set out to characterize SNS users by their privacy proficiency and management strategies. In summary, we have (1) verified the multi-dimensional structure of Facebook users' privacy behaviors and feature awareness; (2) examined the relationships between the dimensions of feature awareness and privacy behavior; (3) classified users based on their unique privacy management strategies and proficiency profiles derived from their scores on the privacy behavior and feature awareness dimensions; and (4) analyzed the overlap between proficiency levels and management strategies. Our findings lead to important insights and implications for design, which we discuss below.

6.1. Theoretical and practical insights

6.1.1. Privacy behaviors and privacy management strategies

Understanding the underlying dimensionality of privacy behaviors and interpreting these privacy profiles enables a number of theoretical and practical contributions. First, we will relate our findings back to Westin's theoretical categorization of privacy fundamentalists, pragmatists, and unconcerned (Harris et al., 2003, 1997; Westin et al., 1981). Unlike Westin's coarse categorization, our classification of Facebook users by their multi-dimensional privacy management strategies was empirically derived from self-reported data of Facebook users. This approach allowed us to gain more detailed insights as to our participants' privacy behaviors and overall privacy management strategies. Our work also highlights privacy behaviors that are most common and most infrequent across all of our participants. For example, our results show that Facebook users alter their News Feed privacy settings more frequently than moderating the posts to their Timeline/Wall (see Fig. 2). We also observed that a fair share of users tend to create and manage friend lists, but that they are actually less likely to use these lists to selectively share content with subsets of Facebook friends.

More importantly, our users did not simply employ *more* or *fewer* privacy behaviors; instead, the privacy management strategies show distinctly *different* behavioral patterns. For example, *Selective Sharers* (Fig. 3) frequently leverage friend list management and selective sharing, but do not withhold their basic information and contact information, while *Self-Censors* (Fig. 4) choose to withhold such information, and rarely create custom friend lists or leverage the

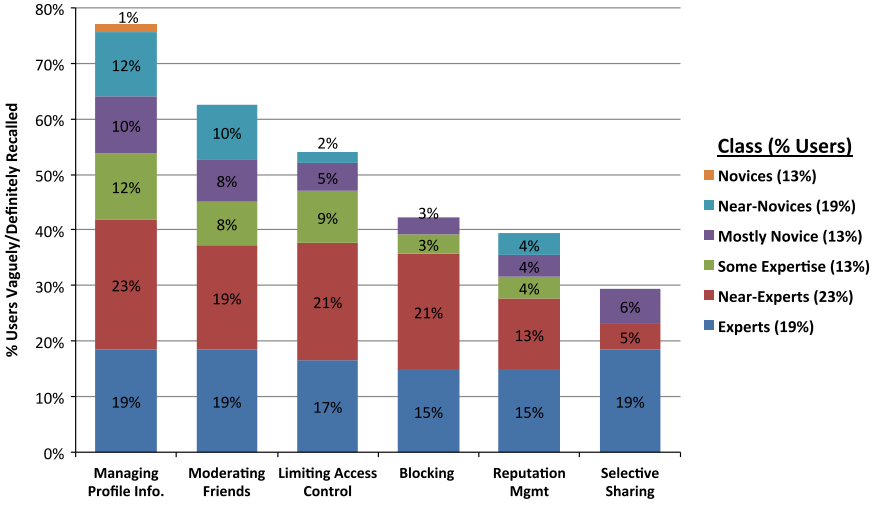

Fig. 6. Privacy proficiency profiles by feature and user class.

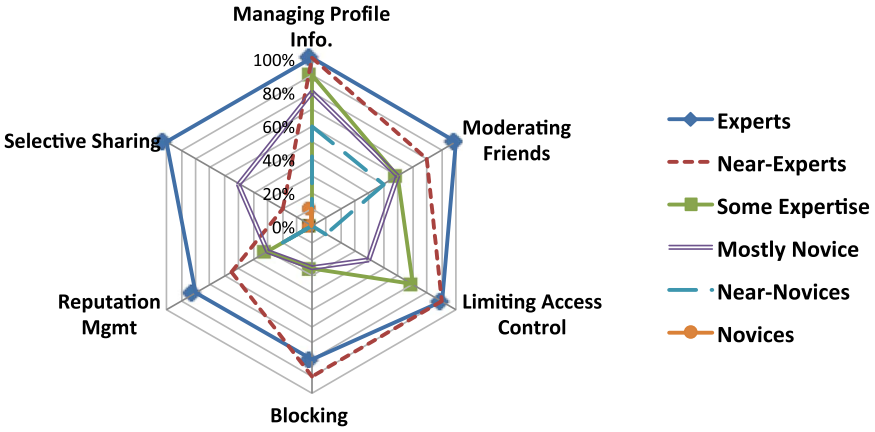

Fig. 7. Privacy proficiency profiles.

Table 8
Class-to-class membership table showing discrepancies between privacy proficiency level and management strategy class memberships.

	Privacy Maximizers	Selective Sharers	Privacy Balancers	Time Savers	Self-Censors	Privacy Minimalists
Experts	**13 (5.6) +**	6 (3) +	**28 (20.4) +**	**4 (9.4) –**	**1 (6.1) –**	**5 (12.6) –**
Near-Experts	**11 (6.9) +**	**8 (3.7) +**	**31 (25.4) +**	**7 (11.8) –**	4 (7.6) –	**10 (15.7) –**
Some Expertise	1 (4) –	0 (2.1) –	17 (14.6) +	9 (6.8) +	4 (4.4) –	10 (9.1) +
Mostly Novice	1 (3.8) –	0 (2) –	**1 (13.9) –**	4 (6.5) –	**12 (4.2) +**	**21 (8.6) +**
Near-Novices	**1 (5.8) –**	0 (3.1) –	**1 (21.4) –**	**22 (9.9) +**	7 (6.4) +	**19 (13.2) +**
Novices	3 (3.9) –	2 (2.1) –	**22 (14.3) +**	5 (6.6) –	5 (4.3) +	3 (8.8) –

Note: Values represent actual representation in each cluster versus (expected). + indicates larger class-to-class membership than expected; – indicates smaller than expected. Color gradient corresponds to the magnitude of this discrepancy (Red is smaller than expected; Green is larger than expected)

ability to selectively share information within their networks. This finding is significant because it is both consistent with Altman's (1975) original theories on privacy boundary regulation, which suggest that different individuals employ different mechanisms in different combinations to optimize their social interactions with others, and it also empirically confirms the observations we made previously from our qualitative interview studies (Karr-Wisniewski et al., 2011; Wisniewski, 2012).

6.1.2. Feature awareness and privacy proficiency profiles

Another theoretical contribution is that we empirically examined two different aspects of end user privacy, both behavior and awareness, to understand how they related to one another. Our results show first and foremost that few users understand and use *all* of Facebook's privacy features, so users typically learn and use a *subset* of these features, resulting in unique user privacy management profiles. We identified six unique classes of SNS user privacy proficiency based on a spectrum of awareness regarding Facebook privacy interface controls. The pattern identified in these classes suggests that privacy proficiency is somewhat additive; users seem to learn the basic privacy features first and the more advanced features later. Feature awareness is shown to be a significant predictor (cf. Table 5) of corresponding privacy behaviors (e.g. knowing how to block another user is a major contributing factor for actually doing it). This means that SNS users require some level of privacy proficiency in order to enact the privacy strategies that match their end goals.

However, our analysis of the overlap between privacy proficiency and privacy management strategies (cf. Table 8) shows that while privacy proficiency seems to be a prerequisite for becoming a *Privacy Maximizer*, more proficient users do not always exhibit more protective strategies: most (near) experts are in fact *Privacy Balancers*, and *Privacy Minimalists* are not complete *Novices*, indicating that employing fewer protective strategies may be an informed decision of these users. Conversely, *Novices* are not likely to be *Privacy Minimalists*, which means that even at the lowest level of privacy proficiency, novice Facebook users are capable of developing some intermediate privacy management strategies.

Also insightful is the mixed awareness classification for *Privacy Balancers*: they are either (*Near-*)*Experts* or complete *Novices*. Likely, the class of *Privacy Balancers* contains both *informed balancers* (who carefully select what privacy mechanisms to exploit) and *uninformed balancers* (who simply make do with the limited mechanisms they are aware of). This distinction between uninformed and informed users, combined with their privacy management strategy classification, can be useful information for deciding whether a particular user should be educated, nudged, or even left alone.

6.1.3. Moving beyond disclosure privacy

We leveraged Altman's (1975) conceptualization of privacy as a boundary regulation process that optimizes one's social interactions with others, not just serving to regulate private versus public information flows. This broadened the scope of the types of privacy features

and settings we examined in our analysis and dictated our approach, which required participants to self-report on their privacy behaviors and awareness. If we had only collected privacy settings as they were available through the Facebook API, this would have severely limited the scope of our analysis. Framing SNS privacy as the decision to disclose or withhold personal information at the content-level over-simplifies the complexity of the decision-making process users go through when regulating their interpersonal privacy boundaries. In contrast, we found that both SNS privacy behaviors and feature awareness are multidimensional in nature, and that withholding information is by far not the most popular privacy protection behavior (see Fig. 2). Users prefer to limit friends' access to the information instead. The "privacy paradox" may thus simply be an artifact of the field's narrow focus on disclosure behavior: our results show that Facebook users employ a wide range of behaviors to protect their interpersonal privacy boundaries, despite disclosing a large amount of information on the network.

6.2. Implications for design

6.2.1. Capitalizing on privacy synergies

Our CFAs found that the physical grouping of privacy features in Facebook's user interface drives the dimensionality of both privacy behaviors and feature awareness. This suggests that creating *privacy synergies* (i.e. conceptually grouping privacy settings and features by the privacy functionality that they support) should be a crucial element of design, because the physical grouping of privacy features has a strong influence on both behavior and awareness. For instance, our findings uncovered that users often create customized friend lists and group friends into these lists, but that it is less common for them to actually *use* these lists to selectively share content. Contrary to our expectations, these two privacy behaviors did not load on the same factor. Why would users go through the process of creating customized friend lists and categorizing friends if not to leverage this as a privacy management strategy? It is possible that friend list management supports other purposes; however, it is also possible that the link between these two behaviors is disjointed because they are not physically grouped within Facebook's user interface. Connecting these two features more strongly in the interface may then result in more effective privacy management strategies.

6.2.2. Managing awareness

Our results also show that there are certain privacy mechanisms that users are mostly aware of, but that very few users actually exploit: Features to block friends, apps, and events, for example. It may be that our participants did not use apps or that these other features are used but not needed on a daily basis. Past research has found that blocking friends, for instance, tends to be a more drastic form of boundary setting that is rarely used (Karr-Wisniewski et al., 2011; Wisniewski et al., 2016). Another option is that perhaps these mechanisms do not meet users' needs, in which case they could be redesigned, or Facebook could deemphasize them and instead increase users' awareness of subtler privacy management strategies. Other mechanisms, such as selective sharing, score low on both awareness and behavior. Yet, our SEM results show a very strong link between awareness and behavior for this mechanism, indicating that almost all users who know about this feature actually use it. This feature is thus an excellent candidate for Facebook to educate its users about privacy; emphasizing this feature could turn more users into *Selective Sharers*.

6.2.3. Personalized privacy education

Facebook has recently introduced a "Privacy Dinosaur" that gives users timely tips on how to manage their privacy settings. To be effective, such tips need to relate to features that fit users' privacy proficiency: tips about features that the user already knows may serve as a helpful reminder (Almuhimedi et al., 2015), but alternatively, could be considered annoying by users (Jedrzejczyk et al., 2010; Tsai et al., 2009; Wang et al., 2014b, 2013b). Similarly, these tips need to match users' personal privacy management strategies: tips about features that the user does not want to employ are equally useless. In order to most effectively educate users about privacy, the advice of the Privacy Dinosaur thus needs to be *personalized*, i.e., tailored to users' privacy proficiency and management strategies (Knijnenburg, 2013b).

The profiles uncovered in this paper can inform such personalized privacy education. For example, a *Selective Sharer* who is also a *Near Expert* should not receive tips about withholding personal information as she most likely already knows this feature but chooses not to employ it. She should also not receive any tips regarding limiting access control, because while she is likely to use this feature, she is also likely to already know about it. Rather, Facebook could give this user tips on about how to optimally share certain updates with custom friend lists (a feature that is used frequently among *Selective Sharers*, but not universally known among *Near Experts*).

In sum, rather than teaching all users about the *same* privacy features, personalized privacy education empowers social network users to employ the privacy mechanisms *they want*; something that has been shown to increase social connectedness and social capital (cf., Wisniewski et al., 2015a, 2015b). Our results can help select the features best suited for education, i.e., the features that fit the user's strategy, but are outside their current proficiency profile.

6.2.4. Personalized nudges

We believe that our results can be used to design more personalized nudges based on users' proficiency and familiarity profiles. For example, although our results show that users' privacy management strategies are partially driven by their proficiency level, there are many situations where users may be consciously deciding to not use certain privacy features (cf. note that most *Experts* are in fact *Privacy Balancers*). We argue that such consciously avoided privacy features should *not* be used in nudges (or do so with great care) because using them would likely cause annoyance, which is considered to be one of the biggest barriers towards the effective deployment of privacy nudges (Jedrzejczyk et al., 2010; Tsai et al., 2009; Wang et al., 2014b, 2013b). Another reason to avoid nudging such features is the recent call to make sure that nudges take users' desires into account, lest they move from "soft paternalism" towards plain old-fashioned paternalism (Smith et al., 2013; Solove, 2012).

The types of features that *should* be used in nudges are the ones that the user are less familiar with, but that *do* align with their current privacy management strategies. The privacy profiles presented in this paper represent coherent sets of behaviors that many users employ. If we can identify a certain user as having of a specific strategy, but if this user is unaware (by virtue of their proficiency profile) of certain features of that strategy, then we can nudge them to use these features, based on the knowledge that many other users tend to use this feature as a coherent part of that same strategy. Thus, using these features would be in line with the user's privacy goals, and therefore, provide decision support without reducing consumer autonomy (Smith et al., 2013), and it enhances SNS user experience by helping them meet their unique privacy needs (Wisniewski et al., 2015a, 2015b).

6.2.5. Prescriptive privacy education and nudges

One type of feature that we have not yet covered in this discussion is the set of features that a user does not know about but would be incongruent with their current privacy strategy. It is unclear whether this type of feature fits the user's desire for privacy or not. Without the knowledge of a users' privacy desires, this type of feature could still be used—with extreme care—to inform a more prescriptive approach to privacy education and nudging. One could, for instance, nudge users (by means of a combination of education and persuasion) toward a subset of these features to suggest an *alternative* privacy management strategy. For example, it is possible that *Self-Censors* (who are

predominantly *Mostly Novices*) withhold information as a *coping strategy* (Wisniewski et al., 2012) due to their lack of awareness of more sophisticated privacy features. Suggesting these users adopt friend list management and selective sharing may encourage them to become *Selective Sharers* or *Privacy Balancers*. An ethical consideration here is, of course, to ensure that any potential behavior modifications benefit users, as opposed to (only) benefiting the SNS at users' expense. While this is beyond the scope of the current paper, we encourage privacy researchers and practitioners to be aware of the fine lines between education, persuasion, and downright manipulation of end user behaviors (cf., Wilson et al., 2013). A good way to prevent nefarious practices would be to explicitly measure users' privacy *desires* (cf., Wisniewski, 2012; Wisniewski and Lipford, 2013) and use this to inform such prescriptive privacy nudging/education practices.

6.3. Limitations and future research

There are a number of limitations of our study that can be used to inform the design of future research. First, our recruitment strategy combined a sample frame (email addresses from the university's registrar) with snowball sampling (Babbie, 2004). While many studies implicitly employ snowball recruitment strategies by recruiting participants through shared social media posts (Bhutta, 2012), we explicitly chose this approach because we wanted to increase the diversity within our sample and to extend the generalizability of our results (Babbie, 2004) beyond our local university setting. We felt that leveraging participants' existing social structures was congruent with the population from which we were sampling – (i.e. Facebook users). From our post-hoc assessment only a minority of participants were recruited using the snowball sampling approach. While this lessens the potential bias in our sample, we believe it would be prudent for future research to use more widely accepted probability sampling techniques (Biernacki and Waldorf, 1981).

Second, our research relied on Facebook users' self-reported privacy behaviors and feature awareness. Other researchers have used a more behavioral approach by unobtrusively capturing privacy settings over time (Wang et al., 2014b, 2013b). However, this type of analysis was not feasible for this study. First, Facebook's API only provides privacy-related information at the content-level ("Graph API Privacy Node - Documentation - Facebook for Developers," n.d.). For instance, the privacy preferences of a particular post, picture, or an app. Therefore, we would not have been able to capture participants' more global privacy preferences. Second, we were interested in privacy behaviors that extended beyond information privacy settings that could simply not be captured without asking the participants to self-report on their behavior. For example, the frequency of unfriending, hiding a post from one's News Feed, and hiding a story from one's Timeline or Wall are privacy behaviors supported by various Facebook features but not tied explicitly to any privacy settings. Future studies would benefit if they could find a way to feasibly study these broader and more nuanced privacy behaviors in an unobtrusive and objective way. However, our work strongly motivates this type of future analysis because we were able to use Bayesian techniques to draw significant insights from a relatively small sample of Facebook users based on their self-reported behaviors. Combining the potential of big data with our novel approach of profiling privacy management strategies and proficiency levels may prove to be an extremely worthwhile endeavor.

Finally, we modeled the relations between feature awareness and privacy behaviors as causal paths from awareness to behavior: being more aware of a certain mechanism causes users to use it. Alternatively, one could argue that users intentionally seek out and learn the features they intend to use, or more likely, that both effects occur in a complex feedback loop of discovery, usage and internalization. Future studies may employ longitudinal techniques or controlled experiments to better understand causal relationships. While our work provides a number of new insights regarding SNS users' privacy management strategies, it also raises new questions. For example, *why* do users develop certain privacy management strategies? Are they motivated by privacy concerns, their social needs, or other goals of using Facebook? How do these strategies change and evolve over time? Do these strategies influence their interactions with their Facebook friends? Investigating how privacy management profiles relate to a variety of other factors will provide a deeper understanding and further opportunities for design, user education, and personalization. Specifically, we acknowledge that measuring users' privacy *desires* could further inform nudging/education of unknown features that do not fit the user's current privacy management strategy.

Finally, although the different management strategies protect users' privacy to varying extents (e.g. the privacy of *Minimalists* is arguably less protected than the privacy of *Maximizers*), we have refrained from relating privacy management strategies to users' subjective privacy concerns. As subjective concerns vary considerably from person to person (Madden, 2014), users' optimal level of protection may or may not coincide with their privacy management strategy. In future work, we are interested in exploring which of the different strategies results in more optimal or sub-optimal levels of privacy protection from the user's perspective.

7. Conclusion

In this paper, we have made the case for broadening the scope of SNS privacy research to better acknowledge the complex, multi-dimensional nature of end users' varying privacy behaviors and levels of privacy feature awareness, encompassing both informational and interactional aspects of privacy. We demonstrate how SNS users can be classified by their unique privacy management strategies and privacy proficiency levels so that efforts to educate and personalize SNS privacy can be tailored and optimized for subsets of users. By delineating between informed and uninformed users, we offer a solution for disentangling users' privacy intentions and preferences from their bounded rationality. We also make suggestions for a more synergetic design of Facebook's privacy controls, and—beyond Facebook—offer our privacy profiling methodology as a practical framework for future research into exciting new approaches to address privacy design, user education, and personalization.

References

Acquisti, A., Grossklags, J., 2008. What Can Behavioral Economics Teach Us About Privacy? Digital Privacy: Theory, Technologies, and Practices. pp. 363–377.

Acquisti, A., Gross, R., 2006. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook, Privacy Enhancing Technologies. Springer, Berlin / Heidelberg.

Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., Cranor, L.F., Agarwal, Y., 2015. Your location has been shared 5398 times!: A field study on mobile app privacy nudging. In: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, CHI'15. ACM, New York, NY, USA, pp. 787–796. ⟨http://dx.doi.org/10.1145/2702123.2702210⟩.

Altman, I., 1975. The Environment and Social Behavior. Brooks/Cole Pub. Co., Monterey, CA.

API Graph Privacy Node - Documentation - Facebook for Developers [WWW Document], n.d. Facebook Developers. URL ⟨https://developers.facebook.com/docs/graph-api/reference/privacy/⟩ (accessed 4.25.16).

Babbie, E., 2004. The Practice of Social Research 10th ed.. Wadsworth Publishing Company, Belmont, CA.

Barnes, S.B., 2006. A privacy paradox: social networking in the United States. First Monday 11. http://dx.doi.org/10.5210/fm.v11i9.1394.

Baumer, E., Adams, P., Khovanskaya, V., Liao, T., Smith, M., Sosik, V.S., Williams, K., 2013. Limiting, leaving, and (re)lapsing: an exploratoration of facebook non-use practices and experiences. In: Presented at the Conference on Human Factors in Computing Systems.

Benisch, M., Kelley, P.G., Sadeh, N., Cranor, L.F., 2011. Capturing location-privacy preferences: quantifying accuracy and user-burden tradeoffs. Pers. Ubiquitous Comput. 15, 679–694. http://dx.doi.org/10.1007/s00779-010-0346-0.

Bentler, P.M., Bonett, D.G., 1980. Significance tests and goodness of fit in the analysis of covariance structures. Psychol. Bull. 88, 588–606.

Bhutta, C.B., 2012. Not by the book facebook as a sampling frame. Sociol. Methods Res.

41, 57–88. http://dx.doi.org/10.1177/0049124112440795.
Biernacki, P., Waldorf, D., 1981. Snowball sampling: problems and techniques of chain referral sampling. Sociol. Methods Res. 10, 141–163. http://dx.doi.org/10.1177/004912418101000205.
Blasiola, S., 2013. What friends are for: how network ties enable invasive third party applications on facebook. In: Presented at the Measuring Networked Privacy Workshop at CSCW.
Bonneau, J., Preibusch, S., 2010. The privacy jungle: on the market for data protection in social networks. In: Moore, T., Pym, D., Ioannidis, C. (Eds.), Economics of Information Security and Privacy. Springer US, New York, NY, 121–167.
Brodie, C., Karat, C.M., Karat, J., 2004. Creating an E-commerce environment where consumers are willing to share personal information. Des. Personal. User Exp. eCommer., 185–206.
Compañó, R., Lusoli, W., 2010. The policy maker's anguish: regulating personal data behavior between paradoxes and dilemmas. In: Moore, T., Pym, D., Ioannidis, C. (Eds.), Economics of Information Security and Privacy. Springer US, New York, NY, 169–185.
Consumer Reports, 2012. Facebook and Your Privacy: Who Sees the Data You Share on the Biggest Social Network? [WWW Document]. Consumer Reports.
Cranor, L.F., 2012. Necessary but not sufficient: standardized mechanisms for privacy notice and choice. J. Telecommun. High Technol. Law 10, 273.
De Feyter, T., De Couck, M., Stough, T., Vigna, C., Du Bois, C., 2013. Facebook: a literature review. New Media Soc. 15, 982–1002.
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. http://dx.doi.org/10.1016/j.chb.2014.03.010.
Facebook, 2015. Newsroom [WWW Document]. URL ⟨http://newsroom.fb.com/company-info/⟩ (accessed 3.7.15).
Felt, A.P., Ha, E., Egelman, S., Haney, A., Chin, E., Wagner, D., 2012. Android permissions: user attention, comprehension, and behavior. In: Proceedings of the Eighth Symposium on Usable Privacy and Security, SOUPS'12. ACM, New York, NY, USA. pp. 3:1–3:14. ⟨http://dx.doi.org/10.1145/2335356.2335360⟩.
Findlater, L., McGrenere, J., 2007. Evaluating reduced-functionality interfaces according to feature findability and awareness. Presented at the Proceedings of the 11th IFIP TC 13 international conference on Human-computer interaction, Springer-Verlag, 1777071, pp. 592–605
Findlater, L., McGrenere, J., 2010. Beyond performance: feature awareness in personalized interfaces. Int. J. Hum.-Comput. Stud. 68, 121–137. http://dx.doi.org/10.1016/j.ijhcs.2009.10.002.
Grossman, T., Fitzmaurice, G., Attar, R., 2009. A survey of software learnability: metrics, methodologies and guidelines. In: Presented at the Proceedings of the 27th international conference on Human factors in computing systems, ACM, 1518803, pp. 649–658. ⟨http://dx.doi.org/10.1145/1518701.1518803⟩.
Gross, R., Acquisti, A., 2005. Information revelation and privacy in online social networks. In: Presented at the Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, ACM, pp. 71–80.
Hampton, K., Sessions Goulet, L., Rainie, L., Purcell, K., 2011. Social Networking Sites and Our Lives [WWW Document]. URL ⟨http://www.pewinternet.org/files/old-media/Files/Reports/2011/PIP%20-%20Social%20networking%20sites%20and%20our%20lives.pdf⟩, (accessed 4.25.16).
Harris, L., Associates, Westin, A.F., 1997. Commerce, Communications, and Privacy Online: A National Survey of Computer Users.
Harris, L., Westin, A.F., Associates, 2003. Consumer Privacy Attitudes: A Major Shift Since 2000 and Why (No. 10), Privacy and American Business Newsletter. Harris Interactive, Inc.
Hu, L., Bentler, P.M., 1999. Cutoff criteria for fit indexes in covariance structure analysis: conventional criteria versus new alternatives. Struct. Equ. Model.: Multidiscip. J. 6, 1–55. http://dx.doi.org/10.1080/10705519909540118.
Jedrzejczyk, L., Price, B.A., Bandara, A.K., Nuseibeh, B., 2010. On the impact of real-time feedback on users' behaviour in mobile location-sharing applications. In: Presented at the Proceedings of the Sixth Symposium on Usable Privacy and Security - SOUPS'10, Redmond, Washington, p. 1. ⟨http://dx.doi.org/10.1145/1837110.1837129⟩.
Kairam, S., Brzozowski, M., Huffaker, D., Chi, E., 2012. Talking in circles: selective sharing in google+. In: Presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM Press, Austin, TX. pp. 1065–1074. ⟨http://dx.doi.org/10.1145/2207676.2208552⟩.
Karr-Wisniewski, P., Wilson, D., Richter-Lipford, H., 2011. A new social order: mechanisms for social network site boundary regulation, in: AMCIS 2011 Proceedings, AMCIS '11. p. 9
Kelley, P.G., Bresee, J., Cranor, L.F., Reeder, R.W., 2009. A "nutrition label" for privacy. In: Proceedings of the 5th Symposium on Usable Privacy and Security, SOUPS'09. ACM, New York, NY, USA. pp. 4:1–4:12. ⟨http://dx.doi.org/10.1145/1572532.1572538⟩.
Kline, R.B., 2011. Principles and Practice of Structural Equation Modeling Third. ed.. The Guilford Press, New York.
Knijnenburg, B.P., 2015. A User-Tailored Approach to Privacy Decision Support (Ph.D. Thesis). University of California, Irvine, Irvine, CA.
Knijnenburg, B.P., Kobsa, A., Jin, H., 2013. Dimensionality of information disclosure behavior. Int. J. Hum.-Comput. Stud. 71, 1144–1162. http://dx.doi.org/10.1016/j.ijhcs.2013.06.003.
Knijnenburg, B.P., 2013a. On The Dimensionality of Information Disclosure Behavior in Social Networks Presented at the Measuring Networked Privacy Workshop at CSCW.
Knijnenburg, B.P, 2013b. Simplifying privacy decisions: towards interactive and adaptive solutions. In: Presented at the Proceedings of the Recsys 2013 Workshop on Human Decision Making in Recommender Systems (Decisions@ RecSys'13), Hong Kong, China, pp. 40–41
Knijnenburg, B.P., Kobsa, A., 2014. Increasing disclosure without reducing satisfaction: finding the best privacy settings user interface for social networks. In: Presented at the ICIS 2014.
Knijnenburg, B.P., Kobsa, A., 2013. Making decisions about privacy: information disclosure in context-aware recommender systems. ACM Trans. Interact. Intell. Syst 3, 1–23. http://dx.doi.org/10.1145/2499670.
Kolter, J., Pernul, G., 2009. Generating user-understandable privacy preferences. In: Presented at the 2009 International Conference on Availability, Reliability and Security, Fukuoka, Japan, pp. 299–306. ⟨http://dx.doi.org/10.1109/ARES.2009.89⟩.
Lampinen, A., Lehtinen, V., Lehmuskallio, A., Tamminen, S., 2011. We're in it together: interpersonal management of disclosure in social network services. In: ACM (Ed.), Presented at the Proceedings of the Annual Conference on Human Factors in Computing Systems.
Lin, J., Sadeh, N., Hong, J.I., 2014. Modeling users' mobile app privacy preferences: restoring usability in a sea of permission settings. In: Presented at the Symposium on Usable Privacy and Security, Palo Alto, CA.
Lipford, H.R., Besmer, A., Watson, J., 2008. Understanding privacy settings in facebook with an audience view. In: Presented at the Usability, Psychology, and Security 2008 (UPSEC 2008).
Liu, B., Lin, J., Sadeh, N., 2014. Reconciling mobile app privacy and usability on smartphones: could user privacy profiles help? In: Proceedings of the 23rd International Conference on World Wide Web, WWW'14. ACM, New York, NY, USA, pp. 201–212. ⟨http://dx.doi.org/10.1145/2566486.2568035⟩.
Liu, Y., Gummadi, K.P., Krishnamurthy, B., Mislove, A., 2011. Analyzing Facebook privacy settings: user expectations vs. reality. In: Presented at the Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference. ACM, Berlin, Germany. pp. 61–70. ⟨http://dx.doi.org/10.1145/2068816.2068823⟩.
Madden, M., 2014. Public perceptions of privacy and security in the post-snowden era. Pew Research Center's Internet & American Life Project.
Madden, M., 2012. Privacy management on social media sites. Pew Research Internet Project.
Madejski, M., Johnson, M., Bellovin, S.M., 2012. A study of privacy settings errors in an online social network. In: Presented at the 2012 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), Lugano, Switzerland. pp. 340–345. ⟨http://dx.doi.org/10.1109/PerComW.2012.6197507⟩.
Marwick, A.E., boyd, d, 2014. Networked privacy: how teenagers negotiate context in social media. New Media Soc. 16, 1051–1067.
Muthen, L.K., Muthen, B.O., 2010. Mplus Statistical Analysis with Latent Variables User's Guide.
Nemec Zlatolas, L., Welzer, T., Heričko, M., Hölbl, M., 2015. Privacy antecedents for SNS self-disclosure: the case of Facebook. Comput. Hum. Behav. 45, 158–167. http://dx.doi.org/10.1016/j.chb.2014.12.012.
Nylund, K.L., Asparouhov, T., Muthén, B.O., 2007. Deciding on the number of classes in latent class analysis and growth mixture modeling: a Monte Carlo simulation study. Struct. Equ. Model.: Multidiscip. J. 14, 535–569. http://dx.doi.org/10.1080/10705510701575396.
Pavlou, P.A., Liang, H., Xue, Y., 2007. Understanding and mitigating uncertainty in online exchange relationships: a principal- agent perspective. MIS Q. 31, 105–136.
Ravichandran, R., Benisch, M., Kelley, P.G., Sadeh, N.M., 2009. Capturing Social Networking Privacy Preferences, in: Proceedings of the 9th International Symposium on Privacy Enhancing Technologies, PETS '09. Springer-Verlag, Berlin, Heidelberg, pp. 1–18. ⟨http://dx.doi.org/10.1007/978-3-642-03168-7_1⟩.
Sleeper, M., Balebako, R., Das, S., McConahy, A.L., Wiese, J., Cranor, L.F., 2013. The post that wasn't: exploring self-censorship on facebook. In: Presented at the Proceedings of the 2013 conference on Computer supported cooperative work, ACM, 2441865, pp. 793–802. ⟨http://dx.doi.org/10.1145/2441776.2441865⟩.
Smith, N.C., Goldstein, D.G., Johnson, E.J., 2013. Choice without awareness: ethical and policy implications of defaults. J. Public Policy Mark. 32, 159–172. http://dx.doi.org/10.1509/jppm.10.114.
Solove, D.J., 2012. Privacy Self-Management and the Consent Dilemma (SSRN Scholarly Paper No. ID 2171018). Social Science Research Network, Rochester, NY.
Spiekermann, S., Grossklags, J., Berendt, B., 2001. E-privacy in 2nd generation e-commerce: privacy preferences versus actual behavior. In: Proceedings of the 3rd ACM Conference on Electronic Commerce, EC'01. ACM, New York, NY, USA, pp. 38–47. ⟨http://dx.doi.org/10.1145/501158.501163⟩.
Strater, K., Lipford, H.R., 2008. Strategies and struggles with privacy in an online social networking community. In: Presented at the Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction - Volume 1, British Computer Society, 1531530. pp. 111–119.
Stutzman, F., Capra, R., Thompson, J., 2011. Factors mediating disclosure in social network sites. Comput. Hum. Behav. 27, 590–598. http://dx.doi.org/10.1016/j.chb.2010.10.017.
Stutzman, F., Gross, R., Acquisti, A., 2012a. Silent listeners: the evolution of privacy and disclosure on facebook. J. Priv. Confid. 4, 7–41.
Stutzman, F., Vitak, J., Ellison, N.B., Gray, R., Lampe, C., 2012b. Privacy in interaction: exploring disclosure and social capital in facebook. In: Presented at the Proceedings of the Sixth International AAAI Conference on Weblogs and Social Media.
Tang, K., Hong, J., Siewiorek, D., 2012. The implications of offering more disclosure choices for social location sharing. In: Presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM Press, Austin, TX. pp. 391–394. ⟨http://dx.doi.org/10.1145/2207676.2207730⟩.
Tang, K., Lin, J., Hong, J., Siewiorek, D., Sadeh, N., 2010. Rethinking location sharing: exploring the implications of social-driven vs. purpose-driven location sharing. In:

Ubicomp'10. Presented at the Proceedings UbiComp 2010. ACM Press, New York, NY, USA. pp. 85–94. ⟨http://dx.doi.org/10.1145/1864349.1864363⟩.
Thaler, R.H., Sunstein, C., 2008. Nudge: Improving Decisions About Health, Wealth, and Happiness. Yale University Press, New Haven, NJ & London, U.K.
Toch, E., Cranshaw, J., Drielsma, P.H., Tsai, J.Y., Kelley, P.G., Springfield, J., Cranor, L., Hong, J., Sadeh, N., 2010. Empirical models of privacy in location sharing. In: Presented at the Proceedings of the 12th ACM International Conference on Ubiquitous Computing. ACM Press, Copenhagen, Denmark. pp. 129–138. ⟨http://dx.doi.org/10.1145/1864349.1864364⟩.
Tsai, J.Y., Kelley, P., Drielsma, P., Cranor, L.F., Hong, J., Sadeh, N., 2009. Who's viewed you?: the impact of feedback in a mobile location-sharing application. Presented at the Proceedings of the 27th International Conference on Human Factors in Computing Systems. ACM, Boston, MA, USA. pp. 2003–2012. ⟨http://dx.doi.org/10.1145/1518701.1519005⟩.
Tsai, J.Y., Egelman, S., Cranor, L., Acquisti, A., 2010. The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. Information Systems Research. doi:10.1287/isre.1090.0260
Tufekci, Z., 2008. Can you see me now? Audience and disclosure regulation in online social network sites. Bull. Sci. Technol. Soc. 28, 20–36.
Wang, N., Grossklags, J., Xu, H., 2013a. An online experiment of privacy authorization dialogues for social applications. In: Presented at the Proceedings of the 2013 Conference on Computer Supported Cooperative Work, ACM. pp. 261–272.
Wang, N., Wisniewski, P., Xu, H., Grossklags, J., 2014a. Designing the default privacy settings for facebook applications. In: Presented at the Proceedings of the Companion Publication of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing, ACM, 2556495, pp. 249–252. ⟨http://dx.doi.org/10.1145/2556420.2556495⟩.
Wang, N., Xu, H., Grossklags, J., 2011. Third-party apps on facebook: privacy and the illusion of control. In: Presented at the CHIMIT 2011, ACM Press.
Wang, Y., Leon, P.G., Acquisti, A., Cranor, L.F., Forget, A., Sadeh, N., 2014b. A field trial of privacy nudges for facebook. In: Presented at the Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems, ACM, Toronto, Canada, pp. 2367–2376. ⟨http://dx.doi.org/10.1145/2556288.2557413⟩.
Wang, Y., Leon, P.G., Scott, K., Chen, X., Acquisti, A., Cranor, L.F., 2013b. Privacy nudges for social media: an exploratory Facebook study. Presented at the Proceedings of the 22nd international conference on World Wide Web companion, International World Wide Web Conferences Steering Committee, 2488038. pp. 763–770
Watson, J., Besmer, A., Lipford, H.R., 2012. +Your circles: sharing behavior on Google+. In: Presented at the Proceedings of the 8th Symposium on Usable Privacy and Security, ACM, Pittsburgh, PA. ⟨http://dx.doi.org/10.1145/2335356.2335373⟩.
Wenning, R., Schunter, M., 2006. The Platform for Privacy Preferences 1.1 (P3P1.1) Specification. W3C Working Group Note.
Westin, A.F., Harris, L., associates, 1981. The Dimensions of Privacy: A National Opinion Research Survey of Attitudes Toward Privacy. Garland Publishing, New York.
Wilson, S., Cranshaw, J., Sadeh, N., Acquisti, A., Cranor, L.F., Springfield, J., Jeong, S.Y., Balasubramanian, A., 2013. Privacy Manipulation and Acclimation in a Location Sharing Application. In: Presented at the Ubicomp 2013. pp. 549–558.
Wisniewski, P., 2012. Understanding and Designing for Interactional Privacy Needs within Social Networking Sites (Dissertation). University of North Carolina at Charlotte, Charlotte, NC.
Wisniewski, P., Islam, A.K.M., Lipford, H.R., Wilson, D., 2016. Framing and measuring multi-dimensional interpersonal privacy preferences of social networking site users. Communications of the Association for Information Systems. 38.
Wisniewski, P., Islam, N., Knijnenburg, B., Patil, S., 2015a. Give social network users the privacy they want. In: Presented at the the 2015 ACM Conference on Computer Supported Cooperative Work (CSCW 2015).
Wisniewski, P., Knijnenburg, B.P., Lipford, H.R., 2014. Profiling facebook users' privacy behaviors. In: Presented at the the Workshop on Privacy Personas and Segmentation at the Symposium On Usable Privacy and Security (SOUPS 2014).
Wisniewski, P., Lipford, H.R., 2013. Between nuance and rigor: contextualizing and measuring SNS desired privacy level. In: Presented at the 2013 ACM Conference on Computer Supported Cooperative Work.
Wisniewski, P., Lipford, H., Wilson, D., 2012. Fighting for my space: coping mechanisms for SNS boundary regulation. In: Presented at the ACM Conference on Human Factors in Computing Systems.
Wisniewski, P., Xu, H., Lipford, H., Bello-Ogunu, E., 2015b. Facebook apps and tagging: the trade-off between personal privacy and engaging with friends. J. Assoc. Inf. Sci. Technol.. http://dx.doi.org/10.1002/asi.23299.
Woodruff, A., Pihur, V., Consolvo, S., Schmidt, L., Brandimarte, L., Acquisti, A., 2014. Would a privacy fundamentalist sell their DNA for $1000... if nothing bad happened as a result? The Westin categories, behavioral intentions, and consequences. In: Presented at the Symposium on Usable Privacy and Security (SOUPS).
Xu, H., 2007. The effects of self-construal and perceived control on privacy concerns. In: Presented at the ICIS 2007 Proceedings, p. paper 125.

Pamela Wisniewski is an Assistant Professor in the College of Engineering and Computer Science at the University of Central Florida. Her research interests are situated in Human-Computer Interaction and lie at the intersection of social computing and privacy. Her goal is to frame privacy as a means to not only protect end users, but more importantly, to enrich online social interactions that individuals share with others. Her work has won best paper (top 1%) and best paper honorable mentions (top 5%) at premier conferences in her field.

Bart P. Knijnenburg is an Assistant Professor in Human-Centered Computing at Clemson University. His work focuses on privacy decision-making and adaptive systems. He received a Bachelor degree in Innovation Sciences and a Master degree in Human-Technology Interaction from Eindhoven University of Technology, The Netherlands, a Master degree in Human-Computer Interaction from Carnegie Mellon University, and a Ph.D. in Informatics from the University of California, Irvine.

Heather Richter Lipford is an Associate Professor in the Department of Software and Information Systems at the University of North Carolina at Charlotte. Her research interests are in Human Computer Interaction, with a focus in usable privacy and security, secure programming, and social computing. At UNC Charlotte, Dr. Lipford is a member of the HCI Lab, the Cyber Defense and Network Assurability Center, and the Cognitive Science Academy. She received a Bachelor of Science degree from Michigan State University in 1995, and a Ph.D. from the College of Computing at the Georgia Institute of Technology in 2005.