Mapping User Preference to Privacy Default Settings

JASON WATSON, University of North Alabama
HEATHER RICHTER LIPFORD, University of North Carolina at Charlotte
ANDREW BESMER, Winthrop University

Managing the privacy of online information can be a complex task often involving the configuration of a variety of settings. For example, Facebook users determine which audiences have access to their profile information and posts, how friends can interact with them through tagging, and how others can search for them—and many more privacy tasks. In most cases, the default privacy settings are permissive and appear to be designed to promote information sharing rather than privacy. Managing privacy online can be complex and often users do not change defaults or use granular privacy settings. In this article, we investigate whether default privacy settings on social network sites could be more customized to the preferences of users. We survey users' privacy attitudes and sharing preferences for common SNS profile items. From these data, we explore using audience characterizations of profile items to quantify fit scores that indicate how well default privacy settings represent user privacy preferences. We then explore the fit of various schemes, including examining whether privacy attitude segmentation can be used to improve default settings. Our results suggest that using audience characterizations from community data to create default privacy settings can better match users' desired privacy settings.

Categories and Subject Descriptors: H.5.m [**Information Interfaces and Presentation (e.g. HCI)**]: Miscellaneous

General Terms: Human Factors, Security

Additional Key Words and Phrases: Privacy, default policies, social network sites, access control

ACM Reference Format:
Jason Watson, Heather Richter Lipford, and Andrew Besmer. 2015. Mapping user preference to privacy default settings. ACM Trans. Comput.-Hum. Interact. 22, 6, Article 32 (November 2015), 20 pages.
DOI: http://dx.doi.org/10.1145/2811257

1. INTRODUCTION

People are connecting and sharing large amounts of personal information through social media sites, cloud and health services, and other online applications. Users often manage their interactions and information disclosures on these sites using a variety of privacy settings. For example, the use of privacy settings on Facebook has been extensively studied. Researchers have found that users have many friends and desire to selectively share with multiple audiences [Boyd and Ellison 2007]. However, users struggle to manage their privacy settings as they are quite complex and change frequently. As a result, users can share information more broadly than intended, even among people they have friended [Johnson et al. 2012], resulting in embarrassment or regret [Wang et al. 2011]. Rather than adjust confusing privacy settings, users may resort to various coping mechanisms such as censoring their disclosures [Wisniewski et al. 2012].

Authors' addresses: J. Watson, University of North Alabama, One Harrison Plaza, Florence, AL, 35632; email: jwatson5@una.edu; H. R. Lipford, University of North Carolina at Charlotte, 9201 University City Blvd., Charlotte, NC, 28223; email: heather.lipford@uncc.edu; A. Besmer, 701 Oakland Ave., Rock Hill, SC, 29733; email: besmera@winthrop.edu.

DOI: http://dx.doi.org/10.1145/2811257

Previous research has explored various methods for improving the understanding of complex privacy settings [Reeder et al. 2007; Besmer and Lipford 2009; Egelman et al. 2011; Watson et al. 2012]. However, there remains a large burden for managing these settings. Users would need to spend a large amount of time to initially configure a desired privacy policy, even when presented with usable configuration mechanisms. Beyond improving the interface mechanisms, another approach is to reduce configuration effort by generating default privacy settings that better represent user privacy preferences.

In the past, default privacy settings on sites such as Facebook have generally been open and permissive [Govani and Pashley 2005; Gross et al. 2005]. More recently, social network sites like Facebook have changed the default posting settings to include friends and family only. For most online systems like these, the default privacy settings are created by the developers, and are likely to emphasize the site's values for information sharing. Thus, permissive default settings may promote social interaction but may require more user burden to manage for those with greater privacy desires. While users are able to customize these settings, many do not, at least until a privacy violation occurs [Strater and Lipford 2008]. Surveys of end-users have shown an increase in the awareness and modification of Facebook privacy settings over the years, yet many users still do not seem to be familiar with the extent of the privacy settings on Facebook or take the time to configure all possible settings [Johnson et al. 2012; Madejski et al. 2012; Wisniewski 2012]. Our research seeks to reduce the gap between default privacy settings and user preference—to help reduce the burden of having to modify a large number of privacy settings and to increase the privacy of those who do not customize defaults. There is limited research on personalizing or inferring privacy settings from other users or past decisions [Fang and LeFevre 2010; Mo et al. 2010; Mugan et al. 2011]. We expand upon this research by exploring default policies based not only on users' setting preferences but also on attitudes towards disclosures to alternate audiences.

We present a study that gathers privacy profile preferences from 184 Facebook users. Participants were asked about audience preferences for all of the 29 profile items and reactions to alternate audience changes for those items. Using this information, we generated an optimal default policy for a training set of participants and examine how that policy compares against three others: a completely restrictive policy, the preferred audience chosen by most participants, and the permissive Facebook default settings.[1] Last, we explore using three different privacy segmentation models, for example, Westin/Harris, to determine if multiple canonical policies could be used to further improve default settings. The use of segmentation models did not improve policy fit within our data. Our results highlight the complexity of privacy attitudes and indicate that user privacy preferences of profile items and disclosure can be used to create default privacy settings that better represent user preferences.

The contributions of this article are twofold. First, the data we gather from our survey provides characterization of user preferences for a variety of settings on Facebook, including users' discomfort with settings that do not match their preferences. Second, we demonstrate how that information can be used to evaluate the fit of policies against user preferences and to calculate a policy from a community of existing users. Our results show that even with a fairly simple method and a small training set, we can generate defaults based on existing users that will be closer to what users desire than current defaults.

[1]Prior to May 2014 changes see: http://www.cnn.com/2014/05/22/tech/social-media/facebook-privacy/.

2. BACKGROUND

Any set of controls has a starting point—the default configuration that the user then modifies as desired. Customizing these settings takes user effort, and users often accept the defaults rather than perform the work of modifying them to meet their needs [Acquisti and Gross 2006; Madejski et al. 2012; Mondal et al. 2014]. Thus, the default settings can have a large impact on the resulting privacy for users [Johnson et al. 2012; Strater and Lipford 2008]. Organizations and developers that create applications must make a decision on a default privacy configuration that may or may not account for user privacy needs and desires.

A variety of research has examined how to automatically determine or recommend personalized privacy settings. One strand of research has investigated whether measured privacy attitudes correlate to privacy settings, and thus predict settings or privacy-related behaviors. A number of privacy indexes—ranked answers from a set of privacy questions combined together as a score or classification—have been proposed. These scores can then be used to group, or segment, people into categories. The most commonly cited index is the Westin and Harris privacy segmentation model [Kumaraguru and Cranor 2005]. Westin and Harris segment privacy attitudes into three categories: Fundamentalists, Pragmatists, and Unconcerned. In a 2003 survey, Westin and Harris report only 10% of the U.S. population as privacy unconcerned—people who have no real concerns about how other people use information about them [Kumaraguru and Cranor 2005]. Other indexes include Buchanan et al. [2007], Dinev and Hart [2004], and Stutzman [2006], which each measure privacy along multiple dimensions. However, few studies have shown that such attitudes predict or correlate to behavior. We explore using both the Westin/Harris and Buchanan indexes to segment our participants in this article.

Another approach is to learn canonical policies from existing users, to determine the default settings for new users. For example, in the location privacy domain, work with the Loccacino and PeopleFinder systems seeks to reduce configuration burden for dynamic and complex location privacy settings through user feedback and utilizing machine learning to generate default policies [Ravichandran et al. 2009; Sadeh et al. 2009; Toch et al. 2010; Mugan et al. 2011]. The challenge explored by such work is to determine which policy or persona a new user should have to define default sharing settings. In Loccacino, users can explicitly choose a "privacy profile" for adoption as an initial policy. These results suggest providing users with these canonical options can significantly reduce configuration burden by providing default settings that better represent the user's privacy preference. We explore similar questions in this article, in the social media domain.

Others have examined using machine learning or other algorithms to automatically determine settings based on a user's previous settings or behaviors. For example, Sinha et al. [2013] gather information about users' previous Facebook posts to predict better default policies for future posts. Similarly, Shehab et al. [2010], Shehab and Touati [2012], and Mo et al. [2010] suggest using machine learning to automatically configure complex privacy settings for friends based upon configuration for an initial set of friends. These methods may help users as they make similar decisions about new content over time but do not help with initial defaults for items or content that are relatively static.

Prior work on characterizing privacy includes work by Liu and Terzi [2010] who presented a framework for computing privacy scores using profile item sensitivity and the user's social network level. They test two models (Item Response Theory [Baker and Kim 2004] and naïve) for computing privacy scores from user privacy settings. Also related to our research, Fang and LeFevre [2010] use a privacy wizard to gather

user disclosure preference to provide better default privacy settings. Maximilien et al. [2009] proposed using a Privacy-as-a-Service framework to combine profile characteristics of sensitivity and visibility to form a privacy index that can be used to evaluate privacy risks that can be accessed using an API. Similarly, Minukus and Memon [2014] examined characterizing privacy settings into a single score that can be used to aid users in configuration of the privacy policy or compare two given policies. They proposed both a naïve and weighted method, which took into account both sensitivity and visibility.

However, the underlying assumption for these previous models—based on the calculation of the characterization scores—was that profile items disclosed to a more public audience would increase privacy risk and items disclosed to more private audiences added little to no additional privacy risk. Yet people who post information on SNSs desire to share, and restricting too much information is at odds with the purpose of the social network site and the desire of its users. Thus, similar to Minkus and Memon, Liu and Terzi, and Fang and LaFevre, we compute a score to characterize a user's privacy preference. However, our characterization score makes no assumptions about how each piece of data should impact the score. In other words, making data more public does not lower the score, because a user may desire that data to be public. Instead, our characterization scores utilize both the sensitivity of the item and the degree to which that item fits a stated user desire. Additionally, all prior work we are aware of in the area of characterizing privacy defines sensitivity using a single audience preference. Our work uses alternate audience privacy preferences to determine privacy sensitivity. Thus, our characterizations are flexible enough to adjust to changing privacy attitudes as users become more private or more public.

3. METHODOLOGY OVERVIEW

The goal of our research is to examine the fit of existing default privacy policies and the potential to improve upon those defaults using privacy characterization scores. We utilized Facebook for this study, as it is a widely used social network site with a large variety of privacy settings. We first gathered data about users' profile privacy preferences with a survey, asking users what their preferred setting was for 29 Facebook profile items, as well as their attitudes toward the alternate setting options. This approach allows us to not only characterize the participants' desired policies but also their potential reactions to policies that do not represent their best preference. We decided not to query participants' actual Facebook privacy settings, as users may not have taken the time or effort to configure their privacy preferences on the site for a variety of reasons. Thus, despite the limitations of a self-report survey, we felt that this would be the most accurate method of gathering participants' privacy preferences. The details of the survey and the descriptive results are presented in Section 4.

With our survey data, it was possible to compute scores that represent how well a given applied policy would fit the user's stated desires. The details of how we calculated these scores are presented in Section 5. Using the scores as a basis for comparison, we randomly divided our sample into training and test sets to do a between-subjects comparison of different privacy setting policies. We examined four different default policies: two static policies and two that were calculated based on the reported preferences of the training sample of participants. We calculated a fit score for each participant in the test set and compared the scores for the four policies.

Finally, we performed two additional explorations of our calculated optimal policy. First, we explored the results of differing training set sizes on the calculation of the optimal policy. Finally, we explored differences with and without segmentation using

three different privacy attitude measures from our survey. These results are presented in Section 6.

4. SURVEY

We designed a web-based questionnaire to gather Facebook privacy information from people in the United States. The participants were recruited using Amazon's Mechanical Turk system. Each participant or *Turker* can view a list of available Human Intelligence Tasks (HITs) and choose to participate for a monetary incentive, in our case a $2.00 incentive for an estimated 30-minute survey. The HIT was designed to only allow participants registered to Amazon.com with a valid United States address. We also restricted the HIT to *Turkers* with an overall HIT approval rate greater than 95%.

When a *Turker* accepted the HIT, she was first shown an IRB-approved informed consent message that described the study and purpose.[2] If the participant consented, she received the questionnaire. The questionnaire was divided into three logical components: a short demographics section, Facebook usage and general privacy attitude questions and specific questions about privacy preference for 29 profile items. We chose 29 profile items from those available on Facebook, but many of these items are also available as profile items on other social network sites.

The general usage and attitude questions were used to later segment participants' into preference categories. We first used the three-question Westin/Harris segmentation index [Kumaraguru and Cranor 2005]. We also used a 16-question index developed by Buchanan et al. [2007] to measure privacy concern. Finally, we surmised that perhaps general usage of Facebook may be related to privacy attitudes. Thus, we also included the Facebook Intensity (FBI) Index designed to measure usage, frequency, and emotional connectedness along with how the site integrates into people's daily activities [Ellison et al. 2007].

We presented the privacy attitude questions before gathering the profile item privacy preferences. This introduced a privacy bias common in privacy studies [Braunstein et al. 2011]; however, it was our intention to gather a conscientiously reported privacy preference. Still, our results likely present more restrictive default privacy preferences than users may truly desire when interacting on a social site.

The privacy profile questions were each displayed one per page in three stages, as shown in Figure 1. We displayed this dialog for each of the 29 profile items; however, this figure represents a single profile item as an example. Participants were first shown only the question labeled A about disclosure preference—whether the participant would be willing to share the profile item on Facebook. The participant then selected a preferred sharing audience from four available options ranging from most restrictive to most permissive, "Only Me," "Friends," "Friends of Friends", and "Everyone," as shown in Stage B. If the participant selected "No," in Stage A, she would be asked the remaining questions about the profile item using hypothetical verbiage such as: "If you did share your *[item]* on Facebook, which group would you be likely to share it with?" The responses to the hypothetical questions in cases of nondisclosure were discarded during analysis. The purpose for asking the additional hypothetical questions was to prevent participants from answering "No" in an effort to avoid answering additional questions. The third stage, Stage C, then queried the participant about their attitude if the profile item was somehow disclosed to the other three alternative audiences. These alternative options used sliders to gather an interval value from 0 (representing "Very Undesirable") to 100 (representing "Would Not Care"). A more common label of "Very Undesirable" and "Very Desirable" was not used because the desired choice was already

[2]UNC Charlotte IRB protocol 13-11-31.

Fig. 1. Example showing three stages of a question about profile item privacy preference.

selected and at best they would be indifferent to their ideal setting not being chosen. Thus, we chose these labels to represent the strength of discomfort from alternatives that did not represent the optimal chosen audience. We settled on these labels after pilot testing.

In addition to the 29 actual profile items, we included two fake profile items as an instructional manipulation check [Oppenheimer et al. 2009]. These questions asked participants if they would be willing to share their Social Security Number (after the 12th profile item question) and their Debit/Credit Card Information (after the 27th profile item question) on Facebook. We considered any affirmative response to Social Security Number as invalid and removed the participant's data from analysis. For Debit/Credit Card information, we accepted a "Yes" response to disclosure because some people legitimately give that information to Facebook for application purchases. However, if they chose to disclose with a preferred audience other than "Only Me," we considered the response invalid and removed the participants from any further analysis.

For each page in the survey, we recorded the timestamp at the time the question(s) was/were first displayed. Thus, the time between timestamps was recorded as the amount of time in milliseconds the participant interacted with the question.

4.1. Results

During January 2014, we recruited 200 survey participants using Amazon's Mechanical Turk system. Of the 200 results, we excluded six ($n = 6$) participants with outlier responses to the instructional manipulation checks. We normalized the timing results for the remaining participants and trimmed any participant below the 2.5 percentile and above the 97.5 percentile. This excluded responses for any participant who may have not spent enough time to read the questions or that spent excessive time on the survey as to not represent the average participant. An additional ($n = 10$) cases were removed as a result of timing anomalies leaving a total of ($n = 184$) accepted cases for analysis.

Participant age ranged from 19 to 66 with $\bar{x} = 31.4$ and $Md = 29$. More ($n = 104$) participants were male than female ($n = 80$). Education levels varied between no High School diploma to Master's degrees with: ($n = 4$) having no High School diploma, ($n = 51$) graduating High School or having some college, ($n = 33$) having vocational training or Associate's degree, ($n = 57$) with Bachelor's degrees and ($n = 11$) with Master's or other professional degrees.

Facebook Intensity Index: We asked eight questions as part of the FBI scale [Ellison et al. 2007] to measure Facebook usage and how emotionally connected people feel to Facebook. The scale uses six Likert questions about Facebook connectedness and two additional questions about social network usage—total number of Facebook friends and average time per day over the previous week. The total friends and average uses are assigned normalized ranks between 1 and 10, and the FBI score is calculated by averaging the reported ranks for all questions with a higher score ($max = 6.25$) representing a stronger connection and integration in the user's daily life. Participants' scores in this study ranged from 1.25 to 5.75, with $\bar{x} = 3.58$, $s = 1.0$ and $Md = 3.5$ resulting in average usage and a moderate distribution range.

Westin/Harris Segmentation: Privacy attitude assessment from the Westin/Harris survey was somewhat typical with a larger than expected number of participants segmented as "Fundamentalist" ($n = 82, 44.5\%$). Other participants were classified as "Pragmatists" ($n = 86, 46.7\%$) and "Unconcerned" ($n = 16, 8.7\%$). Most Westin/Harris results have resulted in: ∼25% "Fundamentalist," ∼60% "Pragmatists," and ∼15% "Unconcerned."[3]

Buchanan Index: The Buchanan et al. [2007] index consisted of the combined ranks of 16 Likert questions about general privacy concerns Scores range from 16 to 80, with 80 being very strongly concerned about privacy matters. Buchanan et al. make no attempt to segment based on their index, but higher scores would correspond with "Fundamentalist" and lower scores would represent the "Unconcerned" group. Results from this scale included a wide range from 26 to 80, with $\bar{x} = 52.4$, $s = 12.1$ and $Md = 51$ indicating a moderate distribution range of scores.

Participants' reported disclosures of profile items are shown in Figure 2 ordered by willingness to disclose on Facebook. For most profile items, approximately two thirds of participants were willing to share the item on Facebook. The more sensitive profile items (phone numbers, email and street address) were reported to be shared by around one quarter of participants. Items such as religion and political alignment along with previous location information were reportedly disclosed by about half of the participants. Life changes such as family and relationship information, home and living information, and places lived also were disclosed by slightly more than half of the participants. More participants were willing to disclose the photos they post than

[3]http://www.harrisinteractive.com/vault/Harris-Interactive-Poll-Research-Most-People-Are-Privacy-Pragmatists-Who-While-Conc-2003-03.pdf.

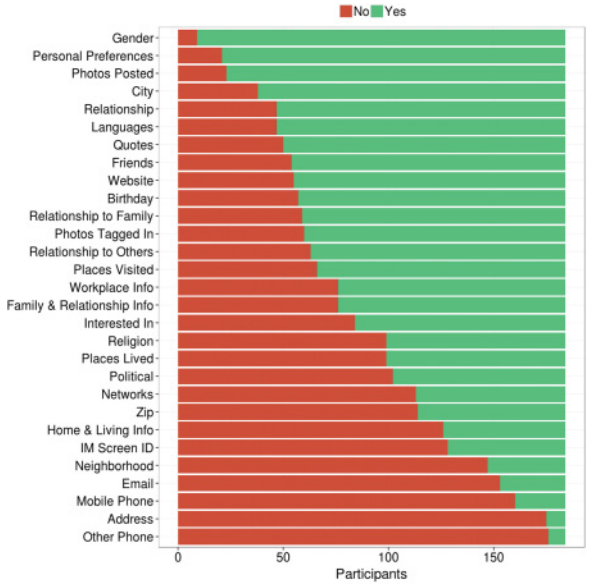

Fig. 2. Disclosure choice for all participants.

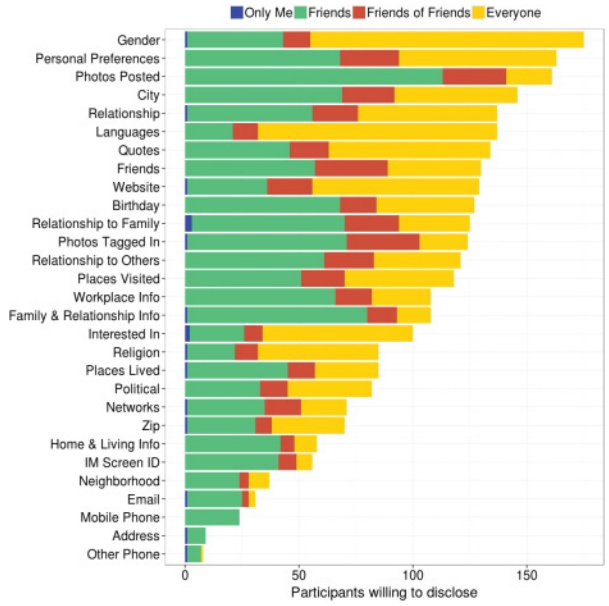

Fig. 3. Preferred audience choice for all participants willing to disclose.

disclose photos they had been tagged in, possibly indicating a perceived difference in control over the disclosure.

Of the participants willing to disclose, the preferred audience responses are indicated in Figure 3. These results indicate most participants were more inclined to share profile information with their friends only, with the ratio between friends only and other audiences increasing with the more sensitive profile items. Of those willing to disclose the

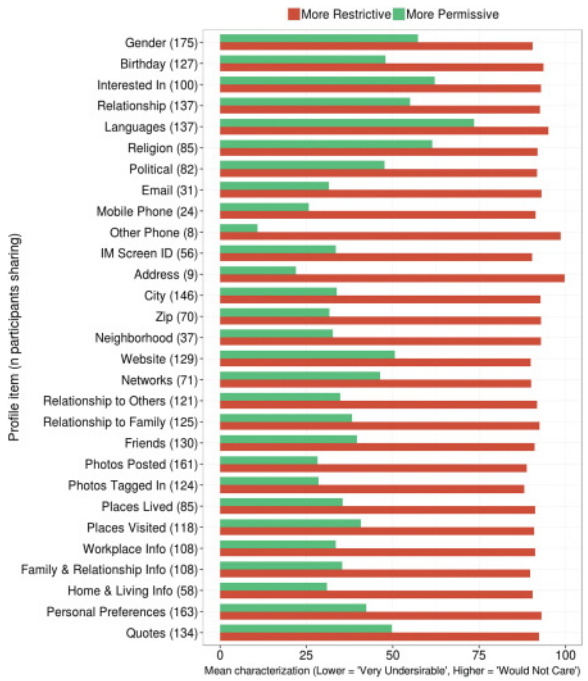

Fig. 4. Reactions for changes to alternate audiences.

more sensitive information (phone numbers and addresses) on Facebook, only in rare cases—such as religion and political preference—was the preferred audience more permissive than friends. However, for less sensitive profile items such as gender, personal preferences and posted photos, participants reported varying audience preferences.

In addition to simply asking what the desired setting would be, we asked questions to attempt to better characterize that profile item. Participants used a slider to respond with an interval value between 0 and 100 to characterize how undesirable it would be if they discovered the item was disclosed to the remaining audience choices. The average of these characterizations for profile items that participants were willing to disclose are shown in Figure 4. We divided the reported values for choices that were more restrictive and more permissive relative to the audience selected as the preferred choice. For more-restrictive audiences, participants would be reacting to the potential that people they wanted to view a profile item would not be able to. For more-permissive audiences, participants are expressing potential reaction to over-sharing with more users being able to access the information than desired. Participants reported neutral reactions to any audience that was more restrictive for all profile items. More-permissive audiences were reported as moderately undesirable in most cases.

The items in Figure 4 are listed in the order presented to the participant in the survey. Some reported values for the seemingly less-sensitive profile items toward the end of the survey were lower and could represent a bias concern from previous profile items that were more sensitive.

5. COMPARING POLICIES

In order to compare policies, we randomly divided the sample into a larger training set of participants and used the remaining participants as a test set. The training set data were used to determine the default choice for each profile item characterized

as the most acceptable for all users in the training set. These choices were combined to form an optimal policy to predict acceptable settings for the sample participant responses in the test set. We calculated optimal privacy settings similar to the naïve polytomous privacy scores used by Liu and Terzi [2010]. They used probabilities to calculate profile item sensitivity. However, in our study, we gathered self-reported user reaction to each possible alternative audience choice, which is an indication of users' views on item sensitivity. Thus, the probabilities were replaced with actual audience characterizations recorded from user responses and represented as a utility score for each option. An optimal policy was thus calculated by combining all participants' utility scores in the training set using the following method:

For each profile item $p \in P$ in an online social network profile,

$$P = \{name, birthday, \ldots, quotes\},$$

the participant chose an audience preference d from a set

$$D = \{only\ me,\ friends,\ friends\ of\ friends,\ everyone\}.$$

The chosen preference was assigned a full utility x of 100. The alternative audience options $d \in D$ from the participant's answers using the sliders shown in Figure 1 became the utility values X_d (between 0 and 100, with 100 being "Would Not Care") for each alternative. Adding X_d for each of the four profile audience options across all participants in the training set represented the collective utility for the options. The largest of the collective utility values became the optimal audience decision o_p for that profile item such that

$$o_p = max\left(\forall d \in D, \sum_{i=1}^{n} X_{di}\right).$$

All of the optimal decisions represented an optimal policy

$$O_p = o_p \mid p \in P.$$

In this study, we compared four different policies. The Optimal policy based on the training community was considered the first treatment. The training or community set was also used to calculate the second treatment condition by simply iterating through all training participants and using the mode of audience choices for each profile item. The third treatment policy was a highly Restrictive policy and consisted of the "Only Me" audience for each profile item. Finally, the actual Facebook default policy was the fourth treatment for the within-subjects variance analysis, as described later.[4]

5.1. Calculating Policy Fit

The dependent variable for our policy comparison was a fit score generated by assessing how well each treatment policy fit each participant's audience choice or utility for alternative audiences. For example, using the estimated values of the choices in Figure 1, this participant chose to disclose the "Gender" profile item to the audience "Friend of Friends" and assigned utilities for "Only Me" (90), "Friends" (75), and "Everyone" (10). Suppose the treatment policy choices were: Optimal ("Friends"), Mode ("Everyone"), Restrictive ("Only Me"), and Facebook ("Everyone"), then the assigned fit score for this participant would be Optimal (75), Mode (10), Restrictive (90), and Facebook (10). Thus, for this participant and profile item, the Restrictive treatment default policy was the better fit. The individual fit scores for all items were combined

[4]As of January 2014, using a new Facebook account and recording each default privacy setting.

to represent an overall fit score for the entire policy and the highest value is the best fit for that participant's privacy setting defaults. Overall policy fit scores had possible values from 0 (no disclosure or disclosure with no correct policy choices combined with undesirable characterization) to 2,900 (disclosure for all 29 items and correct policy choices or neutral characterizations for all items). For comparisons, we divided the total fit score by the number of shared items resulting in a number between 0 and 100.

During the questionnaire, we asked the participants who chose not to disclose a profile item to consider the audience and alternatives if they were to disclose. For the fit score, we discarded any profile item the participant chose not to disclose and the overall fit score was a combination of only the profile items that would be disclosed on Facebook. For example, if a participant responded they would never share their "Address" on Facebook, that item was ignored when the overall fit was calculated. While we could potentially utilize the hypothetical answers to the audience characterizations, those tended to be quite restrictive, as users often did not desire to share that information with anyone.

The participant fit scores were not normally distributed for any treatment condition. The overall fit scores were evaluated using a Friedman's test on the four related treatments. We hypothesized that the median fit scores for the treatment models would be significantly different:

$$H_0 : \theta_{Opt} = \theta_{Res} = \theta_{Mode} = \theta_{Face}$$
$$H_1 : \theta_{Opt} \neq \theta_{Res} \neq \theta_{Mode} \neq \theta_{Face}.$$

For pairwise post-hoc analysis between groups, we conducted Wilcoxon signed-rank tests with a Bonferroni correction applied, resulting in a significance level at $p < 0.008$. Effect sizes were calculated for each post-hoc pairwise analysis result using Cohen's r [Cohen 1960, 1988].

The survey described in Section 4 provided data that enabled us to test how well different policies fit to the reported user preference. In order to compare policies, we randomly divided the sample into a larger training set of participants and used the remaining participants as a test set. We then created the four policies mentioned earlier to test how well each policy fit as a default policy for the participants in the test set. For the Optimal and Mode policies, we used the training set of participants to derive a choice for each profile item. The Optimal policy used the participants' answers from profile item questions about audiences reactions to generate settings for profile items; the algorithm is described later. The Mode policy represented the most popular audience decision for all participants in the training set. Our data were collected after privacy-related questions, and we determined that the optimal preferences might represent a somewhat restrictive policy, so we chose to include the most restrictive policy choice to compare with the Mode and Optimal policies. We also included another policy for comparison that represented the actual Facebook default settings (from early 2014) to represent a real-world permissive default setting policy. The Restrictive and Facebook policies disregarded the training set and used the same set of randomly selected test participants for consistent comparison with all models.

5.2. Results

Policy Settings: Table I lists the policies that were calculated and compared. While the Restrictive policy obviously differs vastly from the others, the Mode and Optimal policies also differ for many items. Interestingly, the Optimal policy is "Friends" for all profile items except for three items even though the Mode is more permissive. This is likely because our participants' reported stronger negative reactions to over disclosure

Table I. Privacy Settings for Each Test Model

Item	Facebook	Mode	Optimal	Restrictive
Gender	EO	EO	Fr	OM
Birthday	FoF	Fr	Fr	OM
Interested In	EO	EO	Fr	OM
Relationship	EO	Fr	Fr	OM
Languages	EO	EO	Fr	OM
Religion	FoF	EO	Fr	OM
Political	FoF	EO	Fr	OM
Email	Fr	Fr	OM	OM
Mobile Phone	Fr	Fr	Fr	OM
Other Phone	Fr	Fr	OM	OM
IM Screen ID	Fr	Fr	Fr	OM
Address	Fr	Fr	OM	OM
City	Fr	Fr	Fr	OM
Zip	Fr	Fr	Fr	OM
Neighborhood	Fr	Fr	Fr	OM
Website	EO	EO	Fr	OM
Networks	EO	Fr	Fr	OM
Relationship to Others	EO	Fr	Fr	OM
Relationship to Family	EO	Fr	Fr	OM
Friends	EO	Fr	Fr	OM
Photos Posted	EO	Fr	Fr	OM
Photos Tagged In	EO	Fr	Fr	OM
Places Lived	EO	Fr	Fr	OM
Places Visited	EO	Fr	Fr	OM
Workplace Info	EO	Fr	Fr	OM
Family & Relationship Info	EO	Fr	Fr	OM
Home & Living Info	EO	Fr	Fr	OM
Personal Preferences	Fr	Fr	Fr	OM
Quotes	EO	EO	Fr	OM

Note: Only Me (OM), Friends (Fr), Friends of Friends (FoF), Everyone (EO).

than to under disclosure, resulting in the trained policy erring toward restricting items. We discuss the implications of this later.

Fit Variance: The training set was only used to calculate the Optimal and Mode policies; however, the same test set of participants was used to derive fit scores for all models. To determine the size of the test set, we estimated a Cohen's d medium effect size ($d = 0.49$). Compensating for multiple post-hoc comparisons, we estimated a test sample size of ($n = 51$) in order to achieve at least 0.80 statistical power [Cohen 1988]. Thus, although gathering a larger sample was feasible, we decided to only gather the sample size estimated by the power analysis to avoid overstating statistical significance between groups with inflated sample sizes. The sample size estimation was evaluated before data collection and, therefore, based on parametric tests. After the data were collected and we discovered the fit scores violated a normal distribution assumption, we used nonparametric statistical tests to analyze variance. However, Tanizaki [1997] showed in a series of Monte Carlo experiments that Wilcoxon nonparametric tests have similar or more power than t-tests when the underlying distribution is not normal.

We conducted a Friedman test to compare differences between the fit score medians of the four treatments: Optimal ($Md = 99.39$), Mode ($Md = 89.75$), Restrictive

Table II. Comparison of Model Fit Score Variance Effect Sizes

Model		Optimal	Mode	Restrictive	Facebook
	Md	**Effect Size** (Cohen's *d*)			
Optimal	99.39				
Mode	89.75	**0.5847*****			
Restrictive	96.08	**0.4115*****	0.0826		
Facebook	73.43	**0.7973*****	**0.7895*****	**0.6025*****	

Note: ***Significant at $p < 0.001$.

($Md = 96.08$), and Facebook ($Md = 73.43$). The test was significant $\chi^2(3, n = 51) = 56.98, p < 0.001$, and the Kindall's coefficient of concordance ($W = 0.558$) indicated a strong variance between treatments and resulted in rejecting the null hypothesis $H_0 : \theta_{Opt} = \theta_{Res} = \theta_{Mode} = \theta_{Face}$.

To further examine differences between groups, we conducted six post-hoc pairwise comparisons using Wilcoxon tests with a Bonferroni adjustment ($p < 0.008$). Pairwise comparison results are displayed in Table II. The Optimal median was significantly greater than all three other conditions, Mode ($p < 0.001, r = 0.58$), Restrictive ($p = 0.003, r = 0.41$), and Facebook ($p < 0.001, r = 0.80$). Mode and Restrictive medians were not significantly different ($p = 0.6, r = 0.08$). Both Mode ($p < 0.001, r = 0.79$) and Restrictive ($p < 0.001, r = 0.60$) medians were significantly larger than the Facebook treatment. Thus, we found statistically significant differences between the policies, with the Optimal policy representing the larger fit scores and Facebook's current policy being the lowest fit. Interestingly, despite being very different policies, the Mode and Restrictive fit scores were not significantly different.

6. ADDITIONAL EXPLORATION

The statistical analysis only evaluated the models at a fit training set size ($n = 133$). Thus, it was not clear how the training set size affects the variance between the different model fit scores. With evidence of significant variance at ($n = 133$), we wanted to evaluate what the minimum training set size might be to produce higher fit scores with the Optimal model. We also wanted to determine if the training set size affected fit scores with the other static models. To capture this, we ran the fit algorithm for every training set size from ($n = 4$) to ($n = 133$). The results of this analysis are shown in Figure 5. In each case represented in Figure 5, the participants were randomly split into the varying group sizes. Data item values represent the mean fit score for all participants in the test group.

Not surprisingly, the fit scores for the Optimal model have more variation with a smaller number of participants in the training set. However, as the number of training participants reached about 40, the Optimal model produced slightly higher and more consistent scores with less variation than the other models. Restrictive policy fits were close but more often slightly higher than the Mode mean fits. Facebook model mean fits were vastly lower compared to the differences between the other three models. Mode mean fits were inconsistent across the entire range of training sets, and Facebook and Restrictive became less consistent with a smaller test size, likely representing larger fit score variance across participants with those models. With a surprisingly small training set size ($n > 40$), the Optimal model scores appeared to corroborate the statistical analysis results for the post-hoc pairwise comparisons made earlier with a fixed training set size of ($n = 133$). Thus, the number of test set participants derived from the power calculation would not likely change the results of the statistical analysis provided the test set size was larger. The Facebook and Restrictive static policies were moderately consistent for all training set sizes.

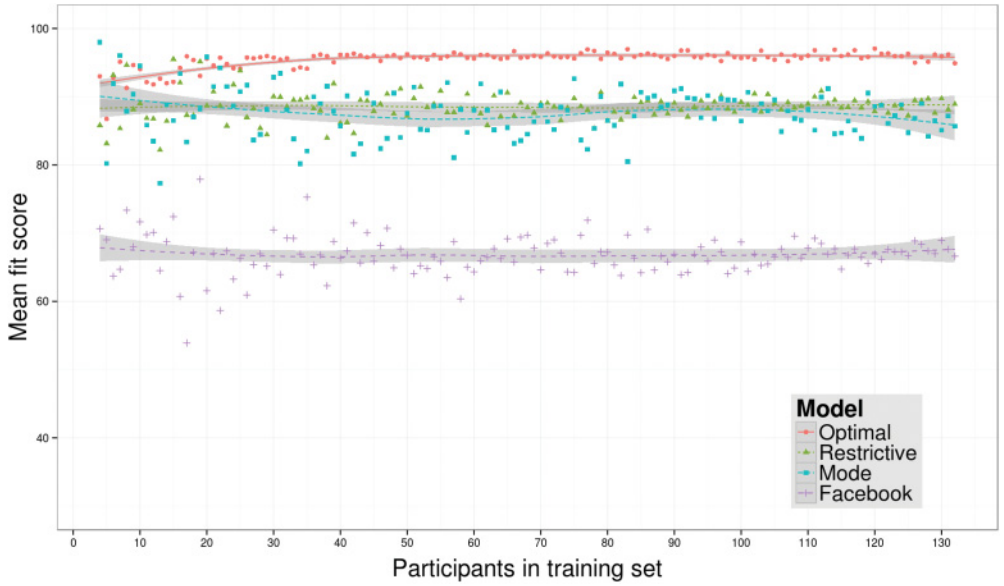

Fig. 5. Model comparison of mean fit scores for varying training set sizes.

6.1. Segmentation

Optimal policy fit scores were high and fairly consistent with enough data available in the training set; however, we wanted to explore if this could be improved by using a set of canonical policies based on different segmentation models. To further evaluate using privacy segmentation, we created additional policies using training data with sample sets segmented by privacy attitude and Facebook usage. During the survey, we asked questions from three different scales or indexes. For each of the segmentation methods, the training and test sets were segmented using the responses to the respective questions. The Westin/Harris responses were evaluated for each participant and segmented into categories (Pragmatist, Fundamentalist, and Unconcerned) based on agreement or disagreement. We calculated index scores for the FBI scale and the Buchanan index. For these indexes, the privacy attitude or behavior was characterized by the value of index scores. To segment participants with these scales, we also divided the participants into three groups (Low, Average, and High), with the "Average" being from -1 standard deviation from the mean to $+1$ standard deviation from the mean. The "Low" and "High" groups were the participants with scores beyond the single standard deviation from the means.

We segmented both the training and test sets using the same criteria. The training set was used to calculate an optimal policy for each segment using the method in Section 5.1. To calculate the fit score for the segmentation policies, we applied the optimal policy representative of the test participant's segment.

For evaluation purposes, we also included the nonsegmented trained policy used in the statistical variance analysis to compare with the three different optimal segmentation models. This policy became a control to evaluate the differences, if any, between the segmentation models. We used the same secondary analysis described previously with varying training set sizes to produce fit scores for the control and segmentation policy fits.

Figure 6 shows the mean fit scores for all test participants for training set sizes from ($n = 4$) to ($n = 133$). To evaluate the effects of the segmentation, we included an

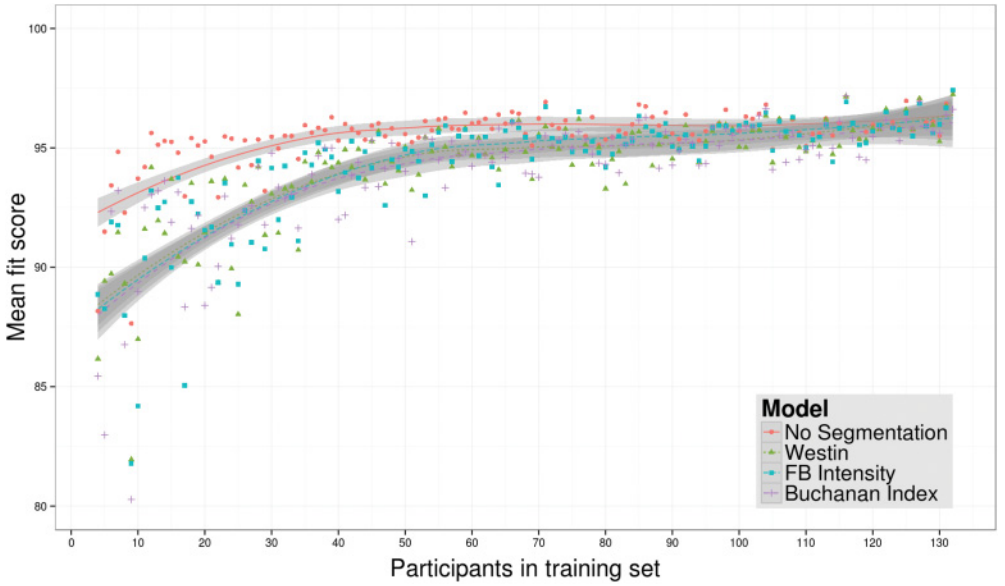

Fig. 6. Segmentation model comparison of mean fit scores for varying training set sizes.

optimal fit model with no participant segmentation for the training or test participants. All segmentation models performed equally well. The y-axis in Figure 6 was adjusted from 80 to 100 to highlight small differences between the nonsegmented optimal model and the models that used segmentation. Segmentation model fit scores were slightly lower with small training sets but began to mirror the nonsegmented optimal model with >90 participants. This difference in mean scores likely represented the effect of dividing the training and test sets into segments, which did not perform well until the segments were sufficiently large. In reviewing the resulting policies, segmented policies were often very similar as long as there was sufficient data in the segment. These results indicate no improvement in fit scores for any segmentation method.

7. LIMITATIONS

Privacy attitude is difficult to define and measure and this study suffers from limitations associated with this challenge. Participants reported privacy attitudes in a context that lacked any of the incentives for social interaction, which may introduce a bias toward more restrictive privacy preferences. For example, participants reported neutral reactions to more-restrictive audiences, but restricting information to "Only Me" is rarely useful and would likely be less desirable than was reported by participants in this study. Our survey may have also introduced some ordering effects. The question order is reflected in Figure 4. The characterization values for more-permissive audiences seemed generally lower after asking about some of the more-sensitive profile items such as phone numbers and address. Responses to more-private profile items could have inadvertently caused participants to respond more conservatively to less-sensitive profile items asked later in the questionnaire.

Participants in this study responded with a reaction to a change in audience with an interval slider from 0 to 100, with 0 being "Very Undesirable" and 100 being "Would Not Care." The chosen audience was also assigned a value of 100. This did not weight the chosen preference any higher than "Would Not Care" characterizations in calculating the optimal policy or determining fit. The chosen preference could be given more

weight, which would also result in lower fit scores and less-restrictive policies. Also, our calculations did not account for the cost or effort associated with the user having to adjust settings to the more desired audience—which should also be taken into account if similar methods were used to create defaults.

The segmentation of participants did not result in any improvements in our study. However, adjusting the calculations to address the aforementioned limitations may result in more room for improvement over the optimal policy. In addition, the segmented samples were rather small, and a larger sample may improve these results.

8. DISCUSSION

Our survey indicates that users do have differing privacy preferences, particularly for personal information considered less sensitive. Facebook's current default policy is permissive and does not match closely with users' reported privacy attitudes. Despite these differences, our policy comparison indicates that we can calculate defaults to better match reported user preferences. We explored not only using the stated preference but also the attitude toward alternative settings to calculate a policy that generates the highest satisfaction across users. This choice has several interesting implications.

Our optimal policy was based upon the same assumption as our fit evaluation—both were calculated from the "utility" score from participants. Thus, this policy resulting in the best fit over the test set of participants was not surprising. However, examining the differences and similarities across the policies reveals insights into various methods. While the mode choice better matched the stated preference for more users, over multiple iterations the fit scores showed inconsistency and would cause more users to be unhappy with that default setting. Interestingly, the Optimal policy was almost entirely a "friends-only" policy. For a time, Facebook had a "friends-only" global setting, which was a common and simple option users chose [Stutzman and Kramer-Duffield 2010]. Our results for the Optimal policy imply that was a reasonable option for many users, and it may be useful to resurrect a global "friends-only" privacy setting.

Interestingly, the fit score of the Restricted policy was also quite high. This demonstrated a limitation in how our participants characterized alternative audience choices. People reported being very tolerant to unmatched policy decisions if the decision change was to a more restrictive audience. Thus, default policies formed from reported privacy preferences may naturally err with more restrictive audience choices. Not every profile item was characterized the same; some had high disclosure rates, whereas other items were reportedly disclosed by only a few people. By gathering information that characterizes the sensitivity of profile items, default policies can use this to select more-restrictive audiences for those users that decide to disclose. This has the benefit of defaults providing additional privacy protections, but there is little social utility for posting personal information that is never shared. Thus, while an "Only Me" default may not concern most users, it may not be useful for social interaction. Similarly, if a default setting is more restrictive than the user preference, but the user does not mind the restrictive setting, they are less likely to change it. Often, users modify settings after a privacy intrusion; more-restrictive defaults may reduce unintended disclosure because users will only modify settings when information is truly needed by additional people. While this may better follow the principle of least privilege and result in fewer privacy intrusions, it will also result in information being shared less widely than users are comfortable with and possibly reduce the value of the site.

The low fit scores for the Facebook default policy highlighted the privacy paradox with reported privacy preferences. People socialize and share information with online social communities but report cautious sharing behavior. Thus, if people want to actually engage in more sharing, a more-restrictive policy may increase effort. However, all of

the data collected in this study was based on reported privacy preferences and the fit scores were generated from the same data. If training data were based on privacy behaviors or better captured sharing desires, the optimal policies might be less private and more closely resemble the Facebook default policy. The results here showed the Optimal policy calculated from training data with profile item characterizations for different audiences provided better fit scores over Mode and Restrictive policy fits. Even if the underlying data were to change and the fit scores appear different, the observation of more consistent average fit scores should improve the fit for the default policy.

The study presented in this article addresses managing privacy as controlling discretionary access to data items from a set group. While this addresses the larger research problem by starting with better default privacy settings, we are aware that managing privacy is more complex than this method. For example, the "Friends" group used in this study can be very large and include a variety of types of acquaintances. Configuring access for "friends" may not be an ideal level of granularity. Profile items in our study are also limited in complexity. "Birthday," "Gender," and "Religion" are somewhat atomic data items with a specific sensitivity. However, "Photos" can contain widely varying levels of sensitivity, and it is difficult to configure optimal privacy preferences for this type of data without regards to the content of individual photos. Our research is intended to help this problem by offering a better starting point for privacy management and to inspire additional research into further easing the burden for more complex configuration.

A notable design implication from our results is that most policy configuration mechanisms lack capabilities to gather additional reaction information to better characterize profile items as we did in the survey. Additional information for every profile item increases profile complexity and adds configuration burden. It remains unclear if the cost of gathering the additional information to generate better default policies would be greater than the reduction of burden achieved by those policies. However, the results here showed an improvement with a small community size—possibly as few as 40 people might be enough to improve default settings for even larger populations. Designs intended to improve complex policies would be more effective if they limited the number of people used for training data to better characterize profile items.

The results of the segmentation model reflected the known difficulties of privacy attitudes and segmentation. Privacy attitudes are complex and difficult to understand, and privacy behaviors are contextual. Segmentation models like Westin/Harris lack structure to account for differing contextual privacy attitudes that often exist within online social networks. The FBI scale [Ellison et al. 2007] measures Facebook usage and connectedness to the Facebook community, but people who are very active in online social networks may also have very different privacy attitudes. The Buchanan index includes questions about more modern technologies, but Buchanan et al. [2007] admittedly failed to capture different dimensions of privacy attitudes on Facebook. While the segmentation models we tested did not improve fit scores, segmentation based on attitudes that are more relevant to social media, or on actual history of behavior, may still be worth exploring.

The segmentation techniques used for the index scores were simple deviations from the mean score. More sophisticated supervised machine learning techniques may improve segmentation, especially over time, but the training sets would need to be larger. The differences with segmentation models in this set were very small and may be improved with larger community sizes and/or better segmentation techniques. It is also possible that the privacy attitude measurement techniques are not adequate enough for any segmentation function to match user privacy preferences. Future research is necessary to explore how these might be used to improve optimal privacy policy fit. If

successful, the burden of answering segmentation questions still needs to be less than the burden of customizing the settings for segmentation to be useful.

9. CONCLUSION

In this article, we explored using audience characterizations for SNS profile items to create a better default privacy policy. Audience characterization utility values were used to train an optimal policy from a training set and then determine how well different policies fit for a group of test participants. While gathering additional information from users required additional burden, we showed that an improvement in default settings can occur with as few as 40 people. While the algorithm may be improved upon, we believe this demonstrates that sites could better take into account user preferences without large amounts of user effort and community data. We further explored using privacy attitude segmentation to evaluate if privacy policies by attitude may improve fits, although these results were not beneficial.

Participants responded to the potential exposure of profile items to alternate audiences from the preferred disclosure audience. Our results indicated that user reactions were neutral for audiences that were more restrictive, but negative for those more permissive than the preferred setting. All policy fit scores accounted for this and the Restrictive policy seemed to benefit from this neutral reaction while the Facebook permissive policy reflected this with lower fit scores. Thus, the fit score itself may not portray a completely accurate representation of how a policy matched actual user needs, but we believe is an improvement over simply measuring accuracy against just the single preferred setting. We believe these results suggest methods for improving a default policy that reduces overall effort for configuring complex privacy settings. The user privacy attitudes for profile sharing in this article seemed to reflect that more-restrictive settings may represent an adequate starting place for users to later configure to actual preference, which at the same time is more privacy preserving than current policies often are. The results also suggest that utilizing user reaction to different audience choices may be useful in determining such default policies, especially if the limitations we discuss are addressed. While this work demonstrates how additional audience characterizations can be used for common social network audiences, we believe the concept can be extended to more granular audiences such as friend lists or circles, as well as additional types of settings beyond the ones we surveyed.

Future work can improve our findings by exploring the burden associated with gathering user reaction to alternate audiences. Additional analysis could be done with this or similar datasets to see if there are other factors that determine the impact or different weights of the audience characterizations. In particular, data from user-reported preferences can be combined with actual social activity to possibly balance the privacy paradox problem. Online social network interaction is dynamic and default settings are applicable to each new social interaction. Thus, more work is needed to examine how users would actually respond to such defaults and how much effort it would take to reconfigure settings for poorly predicted default settings. Complex privacy settings continue to require excessive configuration burden and future research should explore novel methods for minimizing effort needed to manage online privacy.

REFERENCES

Alessandro Acquisti and Ralph Gross. 2006. Imagined communities awareness, information sharing, and privacy on the Facebook. In *Privacy Enhancing Technology*. Springer Berlin Heidelberg, Cambridge, UK, 36–58.

Frank B. Baker and Seock-Ho Kim. 2004. *Item Response Theory: Parameter Estimation Techniques*, (2nd. ed.). CRC Press, Boca Raton, FL.

Andrew Besmer and Heather Lipford. 2009. Tagged photos: Concerns, perceptions, and protections. In *Proceedings of the 27th International Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA'09)*. ACM, New York, NY, 4585–4590. DOI: http://dx.doi.org/10.1145/1520340.1520704

d Boyd and N. B. Ellison. 2007. Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication* 13, 1 (October 2007), 210–230

Alex Braunstein, Laura Granka, and Jessica Staddon. 2011. Indirect content privacy surveys: Measuring privacy without asking about it. In *Proceedings of the 7th Symposium on Usable Privacy and Security (SOUPS'11)*. ACM, Pittsburgh, PA, USA, 1. DOI: http://dx.doi.org/10.1145/2078827.2078847

Tom Buchanan, Carina Paine, Adam N. Joinson, and Ulf-Dietrich Reips. 2007. Development of measures of online privacy concern and protection for use on the internet. *Journal of the American Society for Information Science and Technology* 58, 2 (January 2007), 157–165. DOI: http://dx.doi.org/10.1002/asi.20459

J. Cohen. 1960. A coefficient of agreement for nominal scales. *Educational and Psychological Measurement* 20, 1 (April 1960), 37–46. DOI: http://dx.doi.org/10.1177/001316446002000104

Jacob Cohen. 1988. *Statistical Power Analysis for the Behavioral Sciences*. Psychology Press, Sage, New York, NY, USA.

Tamara Dinev and Paul Hart. 2004. Internet privacy concerns and their antecedents—measurement validity and a regression model. *Behaviour & Information Technology* 23, 6 (November 2004), 413–422. DOI: http://dx.doi.org/10.1080/01449290410001715723

Serge Egelman, Andrew Oates, and Shriram Krishnamurthi. 2011. Oops, I did it again: Mitigating repeated access control errors on Facebook. In *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems (CHI'11)*. ACM, New York, NY, 2295–2304. DOI: http://dx.doi.org/10.1145/1978942.1979280

Nicole B. Ellison, Charles Steinfield, and Cliff Lampe. 2007. The benefits of Facebook "friends:" Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication* 12, 4 (August 2007), 1143–1168. DOI: http://dx.doi.org/10.1111/j.1083-6101.2007.00367.x

Lujun Fang and Kristen LeFevre. 2010. Privacy wizards for social networking sites. In *Proceedings of the 19th International Conference on World Wide Web (WWW'10)*. ACM, New York, NY, 351–360. DOI: http://dx.doi.org/10.1145/1772690.1772727

T. Govani and H. Pashley. 2005. Student awareness of the privacy implications when using Facebook. *Privacy Poster Fair at Carnegie Mellon University School of Library and Information Science.*

Ralph Gross, Alessandro Acquisti, and H. John Heinz, III. 2005. Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (WPES'05)*. ACM, 71–80. DOI: http://dx.doi.org/10.1145/1102199.1102214

Maritza Johnson, Serge Egelman, and Steven M. Bellovin. 2012. Facebook and privacy: It's complicated. In *Proceedings of the 8th Symposium on Usable Privacy and Security (SOUPS'12)*. ACM, 1. DOI: http://dx.doi.org/10.1145/2335356.2335369

P. Kumaraguru and L. F. Cranor. 2005. Privacy indexes: A survey of Westin's studies. Retrieved February 3, 2014, from Research Showcase @ CMU, Carnegie Mellon University. http://repository.cmu.edu/cgi/viewcontent.cgi?article=1857&context=isr.

Kun Liu and Evimaria Terzi. 2010. A framework for computing the privacy scores of users in online social networks. *ACM Transactions on Knowledge Discovery from Data* 5, 1 (Dec. 2010), 1–30. DOI: http://dx.doi.org/10.1145/1870096.1870102

M. Madejski, M. Johnson, and S. M. Bellovin. 2012. A study of privacy settings errors in an online social network. In *Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM'12)*. IEEE Lugano, Switzerland, 340–345. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6197450.

E. Michael Maximilien, Tyrone Grandison, Tony Sun, Dwayne Richardson, Sherry Guo, and Kun Liu. 2009. Privacy-as-a-service: Models, algorithms, and results on the Facebook platform. In *Proceedings of Web 2.0 Security and Privacy (W2SP)*, Vol. 2. IEEE, Oakland, CA, USA. http://alme1.almaden.ibm.com/cs/projects/iis/hdb/Publications/papers/privw2sp.pdf.

Tehila Minkus and Nasir Memon. 2014. On a scale from 1 to 10, how private are you? Scoring Facebook privacy settings. In *Proceeding of the Workshop on Usable Security*. Internet Society, San Diego, CA, USA.

Mingzhen Mo, Dingyan Wang, Baichuan Li, Dan Hong, and I. King. 2010. Exploit of online social networks with Semi-Supervised Learning. In *Proceedings of the International Joint Conference on Neural Networks (IJCNN'10)*. Barcelona, Spain, NJ, USA, 1–8. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5596850.

Mainack Mondal, Yabing Liu, Bimal Viswanath, Krishna P. Gummadi, and Alan Mislove. 2014. Understanding and specifying social access control lists. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, Menlo Park, CA, USA, 271–283.

Jonathan Mugan, T Sharma, and Norman Sadeh. 2011. *Understandable Learning of Privacy Preferences through Default Personas and Suggestions*. Technical Report. Carnegie Mellon University.

Daniel M. Oppenheimer, Tom Meyvis, and Nicolas Davidenko. 2009. Instructional manipulation checks: Detecting satisficing to increase statistical power. *Journal of Experimental Social Psychology* 45, 4 (July 2009), 867–872. DOI: http://dx.doi.org/10.1016/j.jesp.2009.03.009

R. Ravichandran, M. Benisch, P. Kelley, and N. Sadeh. 2009. Capturing social networking privacy preferences. In *Proceedings of Privacy Enhancing Technologies (PET'09)*. Springer Berlin Heidelberg, Seattle, WA, USA, 1–18. http://link.springer.com/chapter/10.1007/978-3-642-03168-7_1.

Robert W. Reeder, Clare-Marie Karat, John Karat, and Carolyn Brodie. 2007. Usability challenges in security and privacy policy-authoring interfaces. In *Proceedings of the 11th IFIP TC 13 International Conference on Human-Computer Interaction - Volume Part II (INTERACT'07)*. Springer-Verlag, Berlin, 141–155.

N. Sadeh, J. Hong, L. Cranor, I. Fette, P. Kelley, M. Prabaker, and J. Rao. 2009. Understanding and capturing people's privacy policies in a mobile social networking application. *Personal and Ubiquitous Computing* 13, 6 (August 2009), 401–412.

M. Shehab, G. Cheek, H. Touati, A. C. Squicciarini, and Pau-Chen Cheng. 2010. User centric policy management in online social networks. In *Proceedings of the IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY'10)*. IEEE, Chapel Hill, NC, USA, 9–13. DOI: http://dx.doi.org/10.1109/POLICY.2010.10

M. Shehab and H. Touati. 2012. Semi-supervised policy recommendation for online social networks. In *Proceedings of the 2012 International Conference on Advances in Social Networks Analysis and Mining (ASONAM'12)*. IEEE, Istanbul, Turkey.

Arunesh Sinha, Yan Li, and Lujo Bauer. 2013. What you want is not what you get: Predicting sharing policies for text-based content on Facebook. In *Proceedings of the 2013 ACM Workshop on Artificial Intelligence and Security (AISec'13)*. ACM, New York, NY, 13–24. DOI: http://dx.doi.org/10.1145/2517312.2517317

K. Strater and H. R. Lipford. 2008. Strategies and struggles with privacy in an online social networking community. In *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction-Volume 1 (BCS-HCI'08)*. British Computer Society, Swinton, UK, 111–119.

Frederic Stutzman. 2006. An evaluation of identity-sharing behavior in social network communities. *Journal of the International Digital Media and Arts Association* 3, 1 (May 2006), 10–18.

Fred Stutzman and Jacob Kramer-Duffield. 2010. Friends only: Examining a privacy-enhancing behavior in Facebook. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'10)*. ACM, New York, NY, 1553–1562. DOI: http://dx.doi.org/10.1145/1753326.1753559

Hisashi Tanizaki. 1997. Power comparison of non-parametric tests: Small-sample properties from Monte Carlo experiments. *Journal of Applied Statistics* 24, 5 (1997), 603–632. DOI: http://dx.doi.org/10.1080/02664769723576

Eran Toch, Norman M. Sadeh, and Jason Hong. 2010. Generating default privacy policies for online social networks. In *Proceedings of the 28th of the International Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA'10)*. ACM, New York, NY, 4243–4248. DOI: http://dx.doi.org/10.1145/1753846.1754133

Yang Wang, Gregory Norcie, Saranga Komanduri, Alessandro Acquisti, Pedro Giovanni Leon, and Lorrie Faith Cranor. 2011. "I regretted the minute I pressed share": A qualitative study of regrets on Facebook. In *Proceedings of the 7th Symposium on Usable Privacy and Security (SOUPS'11)*. ACM, New York, NY, 10:1–10:16. DOI: http://dx.doi.org/10.1145/2078827.2078841

Jason Watson, Andrew Besmer, and Heather Richter Lipford. 2012. +Your circles: Sharing behavior on Google+. In *Proceedings of the 8th Symposium on Usable Privacy and Security (SOUPS'12)*. ACM, New York, NY, 12:1–12:9. DOI: http://dx.doi.org/10.1145/2335356.2335373

Pamela Wisniewski, Heather Lipford, and David Wilson. 2012. Fighting for my space: Coping mechanisms for SNS boundary regulation. In *Proceedings of the 2012 ACM Annual Conference on Human Factors in Computing Systems (CHI'12)*. ACM, New York, NY, 609–618. DOI: http://dx.doi.org/10.1145/2207676.2207761

Pamela J. Wisniewski. 2012. *Understanding and Designing for Interactional Privacy Needs Within Social Networking Sites*. Ph.D dissertation. Charlotte, NC, USA.

Received May 2015; accepted August 2015