Proceedings of the Ninth International AAAI Conference on Web and Social Media

Predicting Privacy Behavior on Online Social Networks

Cailing Dong
Department of Information Systems
University of Maryland, Baltimore County
Baltimore, MD 21250 USA
cailing.dong@umbc.edu

Hongxia Jin
Samsung Research America
75 W Plumeria Dr
San Jose, CA 95134 USA
hongxia.jin@samsung.com

Bart P. Knijnenburg
Department of Informatics
University of California, Irvine
Irvine, CA 92697 USA
bart.k@uci.edu

Abstract

Online Social Networks (OSNs) have come to play an increasingly important role in our social lives, and their inherent privacy problems have become a major concern for users. Can we assist consumers in their privacy decision-making practices, for example by predicting their preferences and giving them personalized advice? In order to accomplish this, we would need to study the factors that affect users' privacy decision-making practices. In this paper, we intend to comprehensively investigate these factors in light of two common OSN scenarios: the case where other users *request* access to the user's information, and the case where the user *shares* this information voluntarily. Using a real-life dataset from Google+ and three location-sharing datasets, we identify behavioral analogs to psychological variables that are known to affect users' disclosure behavior: the *trustworthiness* of the requester/information audience, the *sharing tendency* of the receiver/information holder, the *sensitivity* of the requested/shared information, the *appropriateness* of the request/sharing activity, as well as some *contextual information*. We also explore how these factors work to affect the privacy decision making. Based on these factors we build a privacy decision-making prediction model that can be used to give users personalized advice regarding their privacy decision-making practices.

Introduction

The rising popularity of Online Social Networks (OSNs) has ushered in a new era of social interaction that increasingly takes place online. Pew Research reports that 72% of online American adults maintain a social network profile (Brenner and Smith 2013), which provides them with a convenient way to communicate online with family, friends, and even total strangers. To facilitate this process, people often share personal details about themselves (e.g. likes, friendships, education etc.). Many users even share their current activity and/or real-time location. However, all this public sharing of personal and sometimes private information may increase security risks (e.g., phishing, stalking), or lead to threats to one's personal reputation. It is therefore no surprise that privacy aspects of OSN use has raised considerable attention from researchers, OSN managers, as well as users themselves.

The privacy dilemma OSN users face is the choice between sharing their information (which may result in social benefits) and keeping it private or restricted to certain users only (thereby protecting their privacy). To help users with this decision, experts recommend giving users comprehensive *control* over what data they wish to share, and providing them with more *transparency* regarding the implications of their decisions (Toch et al. 2010). Advocates of transparency and control argue that it empowers users to regulate their privacy at the desired level: without some minimum level of transparency and control, users cannot influence on the risk/benefit tradeoff. Moreover, people can only make an informed tradeoff between benefits and risks if they are given adequate information (Sadeh et al. 2009). But the privacy decisions on ONSs are so numerous and complex, that users often fail to manage their privacy effectively. Many users avoid the hassle of using the "labyrinthian" privacy controls (Compañó and Lusoli 2010), and those who make the effort to change their settings do not even seem to grasp the implications of their own privacy settings (Liu et al. 2011). There is strong evidence that transparency and control do not work well in practice, and several prominent privacy scholars have denounced their effectiveness in helping users to make better privacy decisions (Nissenbaum 2009).

Are there more effective ways to assist consumers in their privacy decision-making practices? A solution that has recently been proposed is to learn users' privacy preferences and then give them *user-tailored decision support* (Knijnenburg and Kobsa 2013). Specifically, privacy recommendations and/or "adaptive defaults" would help to limit the number and complexity of privacy decisions that OSN users have to make. In order to accomplish this, though, we first need to study the factors that affect users' privacy decision-making practices. In this paper, we investigate these factors in light of two common OSN scenarios:

- **Information Requests:** When another OSN user asks for permission to get access to the user's personal information, the user needs to decide whether or not to accept this request. This scenario has an *extrinsic* motivation.
- **Information Sharing:** In this scenario the user has decided to share something on the OSN, such as status or her current location, and she has to decide whether to share

this information to all her contacts or just a part of her contact list. This scenario has an *intrinsic* motivation.

Although the motivation of the request in the two scenarios is different, the decision for the user (and, arguably, which factors determine the decision) remain the same: both of the scenarios result in a *trade-off* between the benefits of social interaction, and potential privacy risks.

Existing work has found several psychological factors that influence OSN users' privacy decision making. The users' *sharing tendency* obviously makes a big difference (Taylor 2003; Consolvo et al. 2005), but *trustworthiness* of the recipient is also highlighted as an important factor in many of these studies (Toch et al. 2010), as is the *sensitivity* of the requested information (Consolvo et al. 2005; Knijnenburg and Kobsa 2013), and the *appropriateness* of the request (Nissenbaum 2009).

Several researchers have attempted to *predict* OSN users' sharing decisions based on contextual factors (Ravichandran et al. 2009; Sadeh et al. 2009; Fang and LeFevre 2010), but have usually not considered the psychological factors described above. Moreover, while this existing work has made some strides in determining the factors that influence OSN users' privacy decisions, and even in predicting those decisions based on context, each work only considers a small subset of (one or two) contextual or psychological factors, in the context of a single OSN.

In this paper, we intend to more comprehensively study the important psychological and contextual factors that affect privacy decision making on OSN, and build a cohesive *privacy decision-making prediction model* that can be used to assist user to make appropriate privacy decisions. Specifically, we make the following contributions:

- We study the factors that affect privacy decision making in *multiple scenarios*. Information requests are studied by looking at "friend request" activity collected on Google+, while information sharing is studied by looking at location sharing data collected in a location sharing preference survey. We compare these scenarios to determine the robustness of different factors.
- We study a comprehensive set of psychological and contextual factors that we predict influence privacy decision making: the *trustworthiness* of the requester/audience, the *sharing tendency* of the user, the *sensitivity* of the information, the *appropriateness* of the request/disclosure, as well as several traditional *contextual factors* derived from the situation in which the sharing takes place. We provide a comparative evaluation of the importance of each factor in determining users' privacy decisions.
- We develop a privacy decision-making prediction model based on these factors to predict users' sharing behavior. We demonstrate that the predictions of this model can recommend appropriate privacy decision making for OSN users. We also show how much each of the determining factors contributes to the predication model.
- In effect, we create a generally applicable privacy decision-making prediction model that can be applied in a multitude of scenarios. Our results thus apply to a broad scale of OSNs, and arguably even other privacy-sensitive systems such as e-commerce systems.

Related Work

Privacy Decision Making

A majority of OSN users takes a pragmatic stance on information disclosure (Taylor 2003; Consolvo et al. 2005). These "pragmatists" (Westin 1998) have balanced privacy attitudes: they ask what benefits they get, and balance these benefits against risks to their privacy interests. This decision process of trading off the anticipated benefits with the risks of disclosure has been dubbed *privacy calculus* (Culnan 1993). In making this tradeoff, these users typically decide to share a subset of their personal information with a subset of their contacts (Consolvo et al. 2005; Lewis, Kaufman, and Christakis 2008).

The term *privacy calculus* makes it sound like users make "calculated" decisions to share or withhold their personal information. In reality though, these decisions are numerous and complex, and often involve uncertain or unknown outcomes (Knijnenburg and Kobsa 2013). Acquisti and Grossklags (2005) identified *incomplete information*, *bounded rationality*, and *systematic psychological deviations from rationality* as three main challenges in privacy decision making. Consequently, people's privacy behavior is far from calculated or rational. Most OSN users share much more freely than expected based on their attitudes (a disparity that has been labeled the "privacy paradox" (Norberg, Horne, and Horne. 2007)). Liu et al. (2011) quantified this disparity between the desired and actual privacy settings, and found that users' privacy settings match users' expectations only 37% of the time and oftentimes people shared more than they expected.

Predicting Privacy Decisions

When left to their own devices, users thus seem particularly inept at making even the simplest privacy decisions in a rational manner (Knijnenburg and Kobsa 2013), and many users actively try to avoid the hassle of making such decisions (Compañó and Lusoli 2010). Interestingly, though, scientists have had modest success *predicting* users' privacy decisions using machine learning practices.

For example, Ravichandran et al. (2009) found that a small number of default policies learned from users' context location sharing decisions could accurately capture a large part of their location sharing decisions. Similarly, Sadeh et al. (2009) demonstrated that they could accurately predict users' privacy preferences in a location-sharing system based on the type of recipient and the time and location of the request. Finally, in a social network context, Fang and LeFevre (2010) developed a privacy wizard that is able to configure users' privacy settings automatically and accurately with a machine learning model that they developed.

Psychological Antecedents of Privacy Decisions

Aside from these machine learning efforts, several works have identified *psychological* antecedents of OSN users' privacy decisions. For example, the user's *sharing tendency*

makes a big difference. Westin (1998) developed a privacy segmentation model that is most widely accepted in the privacy literature, which classifies people into three categories: *privacy fundamentalists*, *pragmatists*, and *unconcerned*. More generally speaking, users differ in their level of disclosure tendency, which influences their actual disclosure behavior (Taylor 2003). Quercia et al. (2012) studied the coronation between information disclosure and personality traits with gender effects. Beyond users' inherent sharing tendency, Adams (2000) identified three major factors that are key to users' privacy perceptions in multimedia environments: *information sensitivity*, *recipient* and *usage*.

Several studies have found that different types of information have different levels of *sensitivity*, and that users are less likely to disclose more sensitive information. For instance, Consolvo et al. (2005) and Lederer, Mankoff, and Dey (2003) both found that users are more willing to share vague information about themselves than specific information. Knijnenburg, Kobsa, and Jin (2013) demonstrated that people's disclosure behavior is in fact multi-dimensional, that is, different people have different tendencies to disclose different types of information. Generally speaking, though, more and less sensitive information can be discerned, users are typically less willing to share the more sensitive information.

The *trustworthiness* of the recipient of the information is also highlighted as an important factor in many studies (Toch et al. 2010). Lederer, Mankoff, and Dey (2003) even found that this factor overshadows more traditional contextual factors in terms of determining sharing tendency. OSNs have started to accommodate this factor by categorizing recipients into "groups" or "circles". Research shows that users make extensive use of this facility, albeit often ineffectively (Knijnenburg and Kobsa 2014).

Finally, several scholars argue that the *appropriateness* of the request plays an important role in determining users' sharing decisions (Nissenbaum 2009; Borcea-Pfitzmann, Pfitzmann, and Berg 2011). The appropriateness of an information request/disclosure depends on whether there is a straightforward reason why this recipient should have access to this piece of information. This reason is often related to a stated or imagined usage scenario.

Large-scale Psychology-based Prediction Using Behavioral Analogs

While machine learning studies have had modest success predicting users' privacy decisions, they have largely ignored *psychological* antecedents of privacy decisions. Similarly, although some researchers have uncovered relationships between disclosure and its psychological antecedents, machine learning models have not been built to exploit these relationships. The reason for this is simple: psychological antecedents are hard to quantify, especially on the large scale needed for successful machine learning. One contribution of this paper is to quantify such psychological antecedents by replacing them with *behavioral analogs*. Moreover, the factors (both psychological and contextual) identified by earlier works were analyzed one-by-one, on various different OSNs. Another contribution of this paper is to integrate these factors, and to test them across a multitude of OSNs.

In effect, we present a unified framework to analyze and utilize the psychological and contextual antecedents of users' sharing decisions systematically and interactively. To do this, we provide behavioral analogs of the *sharing tendency* of the user, the *trustworthiness* of the requester/audience, the *sensitivity* of the information, the *appropriateness* of the request/disclosure, as well as several traditional *contextual factors* that are important antecedents of users' privacy decision making. In the following sections, we quantify and analyze the influence of each factor on OSN users' privacy decision making. Then we integrate all factors into a privacy decision-making prediction model that can help OSN users to make better privacy decisions.

Data Collection

We investigate the main psychological and contextual factors affecting OSN users' privacy decision making in the two common scenarios, "information requests" and "information sharing", by finding behavioral analogs that are easier to observe and quantify. Below we describe these behavioral analogs for data collected on Google+ and a location sharing preference study.

"Friend requests" are the most common and direct way to get access to a user's information in many OSNs, and they serve as our "information request" scenario. Accepting a friend request discloses at least a part of one's profile and online activities to the requester, so the acceptance or rejection of a friend request is the focal privacy decision in this scenario. Two general friendship mechanisms exist on social networks: in *bilateral friendship requests* (e.g. Facebook) friendships are reflexive, and a friendship is only established after the user accepts the request. While this is the "cleanest" version of our scenario, the requests themselves are not accessible through the Facebook API, effectively making it impossible to observe rejected requests. In *unilateral friendship requests* (e.g. Twitter, Google+) users do not need permission to "follow" or "add to circle" other users, making one-sided "friendships" possible. Users who are followed/added to a circle may respond in one of three ways: (1) they may reciprocate the request by following/adding the requester back; (2) they may delete or block the requester; (3) or they may do nothing and simply leave the friendship one-sided. Behavior 1 is observable as a separate friendship request, but unfortunately behavior 2 is not accessible through the Twitter and Google+ APIs, making behaviors 2 and 3 indistinguishable. However, since users are notified of being followed, we argue that users will most commonly follow/add the requester back if they accept the request, and otherwise simply delete or ignore the requester. Our work is based on the assumption that when a user add the requester back to her friend circle, the request is accepted, otherwise it is rejected. We study this behavior in a Google+ dataset.

Then, we study the "information sharing" scenario in a location sharing setting. Location-sharing has gained popularity both in stand-alone apps (e.g. Foursquare, Glympse) and as a feature of existing OSNs (e.g. location-tagging on Facebook and Twitter). Location-sharing is an activity that is

particularly strongly influenced by privacy concerns (Zickuhr 2012). Unfortunately, existing location-sharing datasets often do not extend beyond check-in behaviors. In this paper we use a manually-collected rich dataset of location sharing preferences that includes twenty location semantics, three groups of audiences and several contextual factors.

In the following two subsections, we describe how the two datasets were collected, and provide key statistics describing the main characteristics of the datasets.

Google+ Dataset

Gong et al. (2011) crawled the whole evolution process of Google+, from its initial launch to public release. The dataset consists of 79 network snapshots, these stages can be used to uncover a rough chronological account of friendship creation (i.e. users adding each other to their circles). We focus on the first two stages to build our dataset, where "who sends the friend request to whom first" can be identified by the stage ids. In total, the dataset contains 3,481,544 active users[1] in stage 0 and 14,289,211 in stage 1.

The Google+ dataset consists of a set of tuples $\langle f(u), f(v),\ f(u,v), l\rangle$, where u is the requester, v is the receiver and l is the decision label indicating if v accepts (1) or rejects (0) u's request. $f(u)$ and $f(v)$ are collections of features associated with u and v respectively, and $f(u,v)$ represents the relationship between u and v. For a given user u, we call all the other users who add u to their friends circles as u's *followers*, and the users being added to u' friends circle are called u's *followings*. In Table 1, we list the whole set of features in our Google+ dataset. It includes features describing the requester and the receiver (USER FEATURES) and their relationship (RELATIONSHIP FEATURES). USER FEATURES are further classified into two groups: PROFILE FEATURES and ACTIVITY FEATURES.

PROFILE FEATURES focus on user's profile settings on Google+. The profile settings can be used to quantify *sensitivity* of the requested information. We argue that sensitivity $S(I)$ of a user u's profile item I depends on how common the user's setting/value of I is in the population: the more common of the value, the less sensitive of the information. Formally speaking:

Definition 1 (Sensitivity) *Suppose a profile item I has m possible settings $\{I_1, I_2, \ldots, I_m\}$ ($m \geq 1$). The distribution of different settings over the whole population is $P^I = \{p_{I_1}, p_{I_2}, \ldots, p_{I_m}\}$, where $0 \leq p_{I_i} \leq 1$ and $\sum_{i=1}^{m} p_{I_i} = 1$. If user u set her profile item I as I_k ($1 \leq k \leq m$), the sensitivity value of $S(I) = \frac{1}{p_{I_k}}$.*

On Google+, users have the option to fill out the profile items *Employer*, *Major*, *School* and *Places*. We calculate the sensitivity scores for these items and use them as our behavioral antecedents of *information sensitivity*.

We further defined the following ACTIVITY FEATURES: *followTendency* is a behavioral analog of users' *sharing tendency*, defined as the relative number of people they follow. Similarly, our behavioral analog of the requester's *trustworthiness* is based on the intuition that a user with relatively many followers is likely to have a higher reputation, and thus more trustworthy. The concept of *conservative* is another behavioral analog of *sharing tendency*, based on the idea that users with a lower sharing tendency follow other people in a more "conservative" fashion, i.e. they only follow people within their own "friends circle". Finally, the RELATIONSHIP FEATURES target on the ratio of common followers and common followings. We argue that these features are behavioral analogs for the *appropriateness* of the request: friendship requests are more appropriate if there is a lot of existing overlap between the two users' networks.

Location Sharing Preference Survey

To study the "information sharing" scenario, we used a study on users' location sharing preferences. We conducted this study by recruiting 1,088 participants using Amazon Mechanical Turk[2]. We restricted participation to US Turk workers with a high worker reputation who had previously used a form of location sharing services. The basic demographic distributions are: (a) age: 18 to 24 (21.43%), 25 to 34 (45.23%), 35 to 44 (20.24%), 45 to 54 (5.95%), 55 to 64 (7.15%); (b) gender: male (57.15%), female (42.85%); (c) marriage: married (40.47%), not married (59.53%).

We conducted the study by requesting users' feedback to systematically manipulated location sharing scenarios. Specifically, we considered twenty location semantics supported by Google Places[3]: *Airport, Art Gallery, Bank, Bar, Bus Station, Casino, Cemetery, Church, Company Building, Convention Center, Hospital, Hotel, Law Firm, Library, Movie Theater, Police Station, Restaurant, Shopping Mall, Spa* and *Workplace*. We asked users to imagine being at such a location, alone or with a *companion*, feeling a certain *emotion* (these contextual variables match features available on location sharing services, such as "who are you with", and emotion icons on Facebook). Participants were randomly assigned ten scenarios (different combinations of location and contextual information), and asked to choose whether they would share their location with three different groups of audiences: *Family*, *Friend* and *Colleague*.

For each targeted group of audience V, we collect a set of sharing records and represent each as a tuple $\langle f(u), f(u,V,loc), f(loc), l(V)\rangle$. $f(u)$ represents the user's features. $f(u,V,loc)$ describes the relationship between the three parties, i.e., *user u*, *audience V* and *location loc*. As the sharing information is the given location loc, we specifically include its feature $f(loc)$ into each tuple. The decision label $l(V)$ indicates if u shares her location with audience V (1) or not (0).

In the location sharing preference study, each user u only has one sharing option to each group of audiences under a specific scenario. That is, we do not have the "historical" sharing records of u under the same scenario. Thus, we use other users' sharing behavior to estimate individual u's sharing tendency. The final feature set is listed in Table 2, where $f(u)$ consists of a set of features with format $p^u(Q)$, which represents the sharing tendency of u based on feature Q.

[1] We call a user with at least one following as an "active user".

[2] https://www.mturk.com/mturk/

[3] https://developers.google.com/places/

User features $f(u)$, $f(v)$		Relationship features $f(u,v)$
Profile Features	Activity Features	
(1) $S(Employer)$	(5) $followTendency = \frac{\#followings}{\#followers+\#followings}$	(10) $JaccardFollowing_{(u,v)} = \frac{\lvert followings(u) \cap followings(v)\rvert}{\lvert followings(u) \cup followings(v)\rvert}$
(2) $S(Major)$	(6) $trustworthiness = \frac{\#followers}{\#followers+\#followings}$	(11) $JaccardFollower_{(u,v)} = \frac{\lvert followers(u) \cap followers(v)\rvert}{\lvert followers(u) \cup followers(v)\rvert}$
(3) $S(School)$	(7) $fIntersect = \lvert\{followings\} \cap \{followers\}\rvert$	(12) $comFollowing(u) = \frac{\#commonFollowing}{\#followings(u)}$
(4) $S(Places)$	(8) $fScale = \lvert\{followings\} \cup \{followers\}\rvert$	(13) $comFollower(u) = \frac{\#commonFollower}{\#followers(u)}$
	(9) $conservative = \frac{fIntersect}{fScale}$	(14) $comFollowing(v) = \frac{\#commonFollowing}{\#followings(v)}$
		(15) $comFollower(v) = \frac{\#commonFollower}{\#followers(v)}$

Table 1: Whole set of features in Google+ dataset.

	Features
$f(u)$	$p^u(age), p^u(gender), p^u(marriage)$ $p^u(privacyConcernLevel)$
$f(u,V,loc)$	$p^u_{loc}(companion), p^u_{loc}(emotion)$ $p^u_V(companion), p^u_V(emotion)$ $p^u_{loc}(V), p^u_V(loc)$
$f(loc)$	$S(loc) = \frac{1}{p^u_{loc}(\cdot)}$
$f(V)$	$trustworthiness(V) = p^u_V(\cdot)$

Table 2: Whole set of features in location dataset.

We estimate it by the sharing probability of the users in the given dataset R who have the same feature value of Q with u, regardless of different scenarios. We call such probability as *overall sharing probability*. In this study, we consider the *overall sharing probability* of u based on her demographic features and the claimed *privacyConcernLevel*. The set of features $f(u,V,loc)$ are described by probability $p^u_\alpha(Q)$, called *α-conditional sharing probability*, where α could be the current location loc or the audience V. We use the sharing probability of the users in R who have been under the scenario α and hold the same values of Q to estimate u's sharing probability. Formally speaking:

Definition 2 (Overall sharing probability) *Suppose a feature Q has m possible values $\{q_1, q_2, \ldots, q_m\}$ ($m \geq 1$). The sharing probability of the users with different feature values of Q over the whole records R is $P^u(Q) = \{p_{q_1}, p_{q_2}, \ldots, p_{q_m}\}$, where $0 \leq p_{q_i} \leq 1$ and $\sum_{i=1}^m p_{q_i} = 1$. That is, p_{q_i} represents the overall sharing probability of the users having q_i as the value of feature Q. If user u's feature value on Q is q_k ($1 \leq k \leq m$), the overall sharing probability of u based on feature Q is $p^u(Q) = p_{q_k}$.*

Definition 3 (α-conditional sharing probability) *Suppose an attribute Q has m possible values $\{q_1, q_2, \ldots, q_m\}$ ($m \geq 1$). The sharing probability of the users with different attribute values of Q over the whole set of sharing records R^α under scenario α is $P^u_\alpha(Q) = \{p^\alpha_{q_1}, p^\alpha_{q_2}, \ldots, p^\alpha_{q_m}\}$, where $0 \leq p^\alpha_{q_i} \leq 1$ and $\sum_{i=1}^m p^\alpha_{q_i} = 1$. If user u's feature value of Q on scenario α is q_k ($1 \leq k \leq m$), the α-conditional sharing probability of u based on Q under α is $p^u_\alpha(Q) = p^\alpha_{q_k}$.*

These features allow us to define behavioral analogs of *sensitivity* and *trustworthiness*. Specifically, the *location-conditional sharing probability* $p^u_{loc}(\cdot)$ denote the estimated sharing probability of u purely based on location *loc*: the higher its value, the less sensitive the location *loc*. Therefore, we use its reciprocal as a behavioral analog of the sensitivity of *loc*, $S(loc)$. Similarly, $p^u_V(\cdot)$ is the estimated sharing probability of u purely based on the audience type *V*: it represents the sharing tendency to a certain type of audience, thus serves as a behavioral analog of the *trustworthiness* of the audience V, denoted as $trustworthiness(V)$.

In total, we consider the five scenarios in our location preference study with different contextual information: (1) *location*; (2) *location + time*; (3) *location+ companion*; (4) *location + time + companion*; (5) *location + emotion*.

Factors Affecting Privacy Decision Making

In this section, we first investigate how the defined contextual and psychological aspects affect privacy decision makings in the two scenarios, and identify the most important aspects. In the next section we subsequently describe how we build the privacy decision-making prediction model based on the major aspects, and analyze the prediction performance of this model.

Scenario 1: information requests

Before combining the factors affecting privacy decision making into a general prediction model, we first investigate these features separately. In the Google+ dataset, we focus on requests from different users u sent to the same receiver v_{rec}. This allows us to factor out the receiver's features. We select the 20 users who have received the highest number of requests in the Google+ dataset, and denote the selected request sets as $GSet_{rec}$. Similarly, by building a dataset only containing the requests sent by the same requester u_{req}, we can analyze how different receiver v's features influence the final decisions, factoring out the requester's features. We select the 20 most prolific requesters in our Google+ dataset, and denote the selected request sets as $GSet_{req}$. The final Google+ dataset $D_{Google+}$ consists of all the tuples relevant to the 40 selected users, including 21,798 accepted requests and 114,400 rejected requests.

Feature ranking We first analyze which behavioral features (and therefore which analogous contextual and psychological factors) have the strongest impact on users' decision making process. Specifically, we rank the features based on their *chi-squared statistic* and *information gain* with respect to the decision outcomes using 10 cross-validation on Weka (Hall et al. 2009). Figure 1 shows the average *chi-squared statistic* (left y-axis, bars) and *information gain* (right y-axis, line) with regard to different features (x-axis, refer to the feature IDs in Table 1, over all the 20 receivers in $GSet_{rec}$ and 20 requesters in $GSet_{req}$, respectively. The

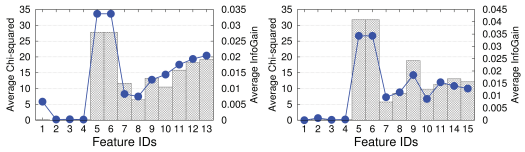

Figure 1: Average value of *chi-squared statistic* and *information gain* with regard to different features in $GSet_{rec}$ *(left)* and $GSet_{req}$ *(right)*

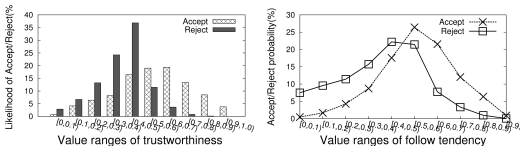

Figure 2: *trustworthiness* of a requester *(left)* and *follow tendency* of a receiver *(right)* on privacy decision making.

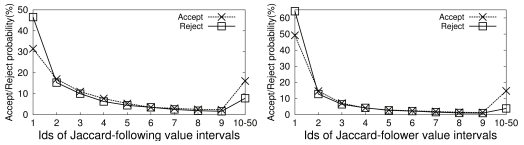

Figure 3: *Appropriateness* of requests in privacy decision making.

features analyzed in the two subsets show similar trends in terms of *chi-squared statistic* and *information gain*:

(I) *FollowTendency* (feature 5, a behavioral analog for *sharing tendency*) and *trustworthiness* (feature 6) are the two most important features. This is in line with our suggested psychological factors for *followTendency* on the receiver's end and for *sharing tendency* on the requester's end. The reason why both are important for both requesters and receivers, is because they are complementary by definition ($followTendency = 1 - trustworthiness$).

(II) In $GSet_{rec}$, receivers are also influenced by the RELATIONSHIP FEATURES (features 10-13) when they make privacy decisions. These features are behavioral analogs of the *appropriateness* of the request, such that requests from people with overlapping friend networks are more appropriate. Interestingly, the number of common followers has more influence on the decision than the number of common followings. Intuitively, this can be explained by the observation that followings are usually based on both friendship and interests, while followers are typically friends only. Two users who share many followings may have similar interests, but they may not know each other. While if two users share many followers, they probably know each other (at least through shared friendships).

(III) In $GSet_{req}$, whether the receiver is *conservative* (feature 9) is another important feature determining if they accept the requests or not. This feature is a behavioral analog of *sharing tendency*.

(IV) The *sensitivity* of profile items did not turn out to be an important feature in determining the final privacy decisions. Arguably, our sensitivity measures *S(Employer)*, *S(Major)*, *S(School)* and *S(Places)* on Google+ are based on a peripheral part of the user's profile that does not contribute much to the overall sensitivity of the shared information.

Analysis of important features We further investigate how these important features we identified affect privacy decision making. As mentioned before, *trustworthiness* and *followTendency* are complementary, therefore their influence on the decision making should be opposite. A requester's *trustworthiness* and a receiver's *followTendency* are behavioral analogs of psychological factors affecting privacy decision making, whereas a requester's *followTendency* and a receiver's *trustworthiness* are not. We thus analyze the former two features and discard the latter two.

a) *Trustworthiness* of the requester. To investigate how different the requesters' *trustworthiness* affects the receiver's privacy decision, we split the range of *trustworthiness* [0,1] into 10 equal intervals, and calculate the likelihood of accepting or rejecting requests within different intervals for the same receiver. The results with regard to a randomly selected receivers from $GSet_{rec}$ is shown on the left of Figure 2. As observed, the user is more likely to reject requests from requesters with lower levels of *trustworthiness*, and accept requests from requesters with higher levels of *trustworthiness*.

b) *FollowTendency* of the receiver. Intuitively, users who have followed or friended more people in the past are likely to have a higher overal *sharing tendency*, leading to a higher probability of accepting any future requests. To check this assumption, we split the range of *followTendency* [0,1] into 10 equal intervals, and calculate the likelihood of accepting or rejecting requests within different intervals. The results with regard to a randomly selected requesters from $GSet_{req}$ are shown on the right of Figure 2. This figure clearly shows that the higher the *followTendency*, the more likely receivers were to accept the requests.

c) *Appropriateness* of the request. Our psychological argument is that the more similar a pair of users (u, v) with respect to their networks of followings and followers, the more similar the two users are, and thus the *appropriate* the request is. We split the distance measures $JaccardFollowing_{(u,v)}$ and $JaccardFollower_{(u,v)}$ into 50 equal intervals, and plot the receiver's probability of accepting the request at each interval in Figure 3. This figure shows that more appropriate requests (i.e. requests where the receiver and the requester have more common followings and common followers) are more likely to be accepted.

Scenario 2: information sharing

To comprehensively study our information sharing scenario, we merge the information collected under different on/off settings of the manipulated scenario features regarding to different groups of audiences, which results in three location datasets: D_{Family} with 8,677 shared and 2,689 not shared tuples; D_{Friend} with 8,455 shared and 2,911 not shared tuples; $D_{Colleague}$ with 5,527 shared and 5,839 not shared tuples. In the following, we first rank the features by importance, then analyze the most important features individually.

Feature ranking To evaluate the importance of all the features in location sharing preference, we use the same rank-

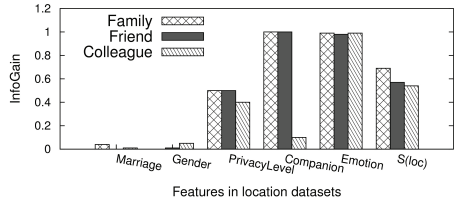

Figure 4: Average value of *information gain* with regard to different features in location datasets.

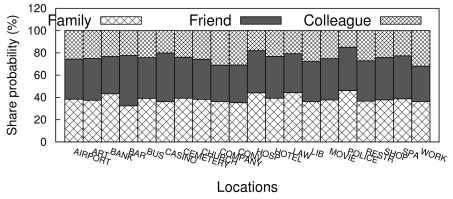

Figure 5: Sharing preferences with regard to the *trustworthiness* of audiences at different locations.

ing procedure as we used for "information requests". For the sake of clarity we treat disclosure to different audiences separately. Figure 4 shows the information gain with regard to different features. The features *marriage* and *gender* of the information holder have little predictive value, *companion*, *emotion* and location *sensitivity* do. Notably, there may exist differences in the effect of companion and sensitivity for different audiences, suggesting an *appropriateness*-effect.

Analysis of important features a) *Trustworthiness* of the audience. To investigate the *Trustworhiness* of different audiences we inspect the value of $p^u_{loc}(V)$, the probability of u sharing the current location with different V's, conditioned on different possible location types. The distribution is shown in Figure 5. We see that in most cases users are most likely to share their location with their family, and least likely to share their location with colleagues. Arguably, people trust their family more than their friends, and they trust their colleagues the least. In other words, the *trustworthiness* of information audience is an important factor in privacy decision making on location sharing.

b) *Sensitivity* of shared information. Figure 6 shows that users have different sharing tendencies for different location types. In general, participants are less likely to share their location at a *Bank*, *Bar*, *Bus Station*, *Casino*, *Police Station* and *Hotel*. Arguably, the probabilities of not sharing one's location represent the *sensitivity* of different location types.

c) *Appropriateness* of sharing. Figure 5 shows that the relative sharing probabilities to different audiences differ by location. Specifically, users share disproportionately more with their family when they are at a *Bank*, *Hospital*, *Law Firm* or *Police Station*; they share more with friends when they are at a *Bar* or *Casino*; and they share relatively more with colleagues at locations of type *Workplace* and *Company*. Arguably, this represents the *appropriateness* of the location sharing: it is appropriate for colleagues to know that the user is at a work-related place, it is appropriate for friends to know that the user is at a leisure-related place, and it is appropriate for family to know that the user is involved

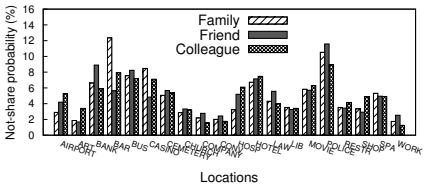

Figure 6: Distribution of "not share" among different locations.

Audience		Companion						
		(1)	(2)	(3)	(4)	(5)	(6)	(7)
Family	**N**	**0.069**	0.026	0.008	0.019	0.062	0.047	0.029
	S	0.154	0.068	**0.043**	**0.094**	**0.111**	0.167	0.104
Friend	**N**	**0.078**	0.029	0.014	0.028	0.051	0.040	0.033
	S	0.145	0.065	0.037	0.085	0.122	**0.174**	0.099
Colleague	**N**	**0.136**	0.059	0.029	0.059	0.107	0.109	0.036
	S	0.087	0.035	0.022	0.054	0.066	0.096	**0.105**

Table 3: Location sharing preferences with regard to *companion*.

in a financial, legal, or health-related activity.

d) *Contextual information*. While there are many contextual features that can be used in the prediction of location sharing activity (e.g. time, weather, companion, emotion), we here specifically consider the influence of receiver's *companion* and *emotion* on their location sharing preferences. The results of sharing tendency to different audiences when participants are with different companions are shown in Table 3. The companions include (1) *Alone*, or with different companions, i.e. (2) *Spouse*, (3) *Kids*, (4) *Family*, (5) *Girl/Boyfriend*, (6) *Friends*, or (7) *Colleagues*. "N" and "S" represent the probabilities of *not-share* and *share*, respectively. We can see that users are least likely to share when they are alone. Beyond that, they tend to share more with an audience that is similar to their companions. For instance, when with friends, users are more likely to share with friends; users are more likely to share with their family when they are with family (spouse, kids); and users are more likely to share with colleagues when they are with colleagues. These observations are consistent with the psychological factor *appropriateness*: it is more appropriate for an audience to know that the user is with a member of the same group, rather than someone from a different group.

We also found that participants are less likely to share their location when they have a negative emotion. Having a negative emotion may be perceived as a more *sensitive* situation than having a positive or neutral emotion. The effect is more pronounced for sharing with colleagues; arguably it is less *appropriate* to share negative emotions with one's colleagues than one's friends or family. We omit the statistics here due to space limitations.

Privacy Decision-making Prediction model

In our analysis above we have confirmed that the important features affecting privacy decision making relate to the following main psychological and contextual factors:

- *Trustworthiness* of the requester/information audience
- *Sharing tendency* of the receiver/ information holder

Dataset	#tuples	F1						AUC					
		All	removed features					**All**	removed features				
			(1)	(2)	(3)	(4)	(5)		(1)	(2)	(3)	(4)	(5)
$D_{Google+}$	43,596	**0.898**	0.889	**0.887**	0.898	0.889	-	**0.899**	0.892	**0.891**	0.898	**0.890**	-
D_{Family}	5,378	**0.845**	-	0.840	**0.833**	**0.833**		**0.879**	-	0.875	**0.867**	0.870	
D_{Friend}	5,822	**0.810**	-	**0.798**	0.802	0.800		**0.844**	-	0.840	0.839	**0.835**	
$D_{Colleague}$	11,054	**0.737**	-	0.730	**0.726**	0.727		**0.752**	-	0.748	**0.743**	0.745	

Table 4: Performance of using different feature sets in decision-making prediction model.

- *Sensitivity* of the requested/ shared information
- *Appropriateness* of the request
- *Contextual factors*

In this subsection we further verify their usefulness by combining them into a comprehensive privacy decision-making model. This model can be used to help OSN users to manage their privacy by predicting their sharing/disclosure behaviors and recommending corresponding privacy settings in line with this behavior. Specifically, based on the behavioral antecedents of the identified factors, we build a binary classification model that learns the influence of these factors on sharing/disclosure decisions (*accept* vs. *reject*, or *share* vs. *not share*).

We build a decision-making model for our Google+ dataset and the three location datasets separately. One problem with these datasets is they are imbalanced, that is, the number of accepts/shares is much larger or smaller than the number of rejects/not-shares. We employ the common machine learning practice to balance the sets by randomly removing items from the "large class" to match the size of the "small class". We use 10 fold cross validation to split the training and testing datasets, and average our classification results over the 10 test folds. We use several classification algorithms provided by Weka (Hall et al. 2009) to build our models, including *Naïve Bayes*, *J48*, *Random Tree*, etc. Among them, *J48* produced the best results, so we focus on this algorithm. We use the common *F1* and *AUC* as evaluation metrics. *F1* is the harmonic mean of precision and recall, and *AUC* is a statistic that captures the precision of the model in terms of the tradeoff between false positives and false negatives. The higher of these the values, the better of the performance. The results are shown in Table 4 under "All" feature sets, i.e., using all the identified factors as features. As we can see, our privacy decision-making prediction model has a good performance (cf. (Swets 1988)).

We further verify the effectiveness of each factor by testing the privacy decision-making model without the corresponding factor. Specifically, Table 4 compares the performance of the decision-making model with all features (*All*) against their performance after removing the features belonging to each of the factors: (1) *trustworthiness*; (2) *sharing tendency*; (3) *sensitivity*; (4) *appropriateness*; (5) *contextual factors*[4].

[4]As contextual factors are not studied in the *information requests* scenario, we have no results for removing such factors from $D_{Google+}$. Similarly, although *trustworthiness* of the audience is an important factor in the location sharing study, our privacy decision-making model is built for different groups of audiences separately (as these measures are repeated per scenario). Thus, *trustworthiness* is not a feature in D_{Family}, D_{Friend} and $D_{Colleague}$. Finally, the features belonging to *appropriateness* are difficult to split off from *contextual factors* in the location study, so those results are combined.

The results in Table 4 showed that removing some factors may reduce the prediction performance; in line with our feature ranking results, this is mainly true for the *trustworthiness* of requester and the *follow tendency* of the receiver as well as the *appropriateness* of the request in the *information requests* scenario. These factors are more important than the *senstivity* factors. In the *information sharing* scenario, the *sharing tendency* of the users, the *sensitivity* of the locations as well as the *contextual factors* are all important predictors that reduce the *F1* and *AUC* values when excluded.

Limitations

In our work, we identified behavioral antecedents of psychological factors that affect privacy decision making, and demonstrated their effect on disclosure/sharing behavior in our analyses. We also built a privacy decision-making model based on these factors that generated good prediction results, and demonstrated that these factors are in fact essential in *predicting* users' disclosure/sharing behavior. Still, there are some limitations with regard to our study that can be accounted for in future work.

The first limitation is our measurement of the psychological factors: on one hand, while users' real sharing behavior data (rather than questionnaire data) is more accurate in identifying the consequences of users' information sharing practices, the interpretation of this behavioral data as a proxy for psychological factors can at times be difficult. For example, we make use of a large dataset of Google+ users to analyze real user behavior, but this behavioral data is an imperfect proxy of the actual psychological factors influencing users' responses to "friend requests". On the other hand, questionnaire data is usually easier to interpret as psychological constructs, but it does not always provide a true reflection of the factors that affect users' actual decision making (cf. the "privacy paradox" (Norberg, Horne, and Horne. 2007)). In our case, the location sharing data is based on imagined scenarios rather than real sharing behavior. By including both types of datasets, this work takes a first step towards comprehensively and accurately studying the factors affecting users' privacy decision making; in the future we hope to provide further evidence for the robustness of our approach to using real behavioral data as proxies for psychological factors.

The second limitation involves the identified factors themselves. We analyzed the most important factors in privacy

decision making as identified by existing work; but the study of factors determining privacy decisions has been far from comprehensive in the past. To create a more generally applicable model, we also specifically selected factors that are applicable to a wide range of privacy decision-making scenarios in different social media, not restricted to online social networks. Consequently, we may miss system/domain-specific factors that could have a significant influence on privacy decision making. Finally, we tried to focus on very simple behavioral analogs in our study; more sophisticated analogs could likely be identified that further increase the prediction performance.

Our third limitation is that our privacy decision-making prediction model is built as a binary classifier. In practical applications of, say, a "privacy recommender", it is not always appropriate to make "hard" recommendations to users, e.g., to pervasively recommend either "accept" or "reject". Instead, it might be more applicable to calculate a "privacy risk" score based on the identified factors and let user make the final decision based on the score, or only intervene when the calculated risk passes a certain (user-defined) threshold.

Design Implications and Conclusion

In this paper, we investigated what the main psychological factors influence privacy decision making in online social networks. Focusing on two common scenarios, *information requests* and *information sharing*, we identified behavioral analogs of the psychological factors and analyzed how these factors influenced privacy decisions in several real-world and collected datasets. Our investigation specifically led to the following important observations that may affect future design of OSNs:

- Consistent with previous studies in *information sharing*, *who* is the information audience is an important factor deciding if the information will be shared. Similarly, in the scenario of *information requests*, *who* is the requester determines the *trust* from the receiver, therefore determines the final privacy decision-making outcome.
- As self-representation is one of the main purposes of OSNs, users' privacy decision making does not exclusively depend on their privacy concern, but more generally on the tradeoff between privacy and self-presentation. We captured this in the definition of *sharing tendency*.
- *Sensitivity* is not an objective concept; it varies with audience. For example, in our location sharing study, locations such as *Bar*, *Casino* are more sensitive if shared to *Colleague* or *Family* compared to *Friend*. This effect may be captured by the *appropriateness* of the request.
- Although the assumption of "rationality" in privacy decision making has been criticized by many studies, users do consider the *appropriateness* of the request/sharing activity. Consistent with our intuition and previous studies, users tend to share information with or accept requests when this is appropriate in the current context.
- *Contextual information* is an indispensable factor in privacy decision making, primarily due to its effect on *appropriateness*. However, the effect of different contextual factors varies.

While our work does not move beyond prediction, it proves the feasibility of an automated tool to predict users' disclosure/sharing behavior, and then helps users to attain a personally appropriate level of privacy. Such a "privacy adaptation procedure" could use the idea of *nudging* (cf. (Thaler and Sunstein 2008)) to give users a default setting or carefully selected piece of information that "nudges" them into the right direction. Nudges do not force any privacy decision upon the user, but they rather set up the decision environment in such a way that it becomes easiest to make the right decision. However, unlike traditional nudges, this privacy adaptation procedure does not determine what is the "right" decision based on some externally prescribed norm, but rather on (a prediction of) the users' *own* privacy preferences. In sum, the privacy adaptation procedure can help ease the burden on the user (who on most OSNs has to make an almost unreasonable number of privacy decisions) without reducing their autonomy to decide what level of privacy is best for them (cf. (Knijnenburg and Kobsa 2014; Smith, Goldstein, and Johnson 2013)).

Reflecting on our findings, we can make the following design suggestions for such a privacy adaptation procedure: the privacy adaptation procedure should make its prediction contingent on a combination of *who* the receiver (or audience) of the information is, and *what* is being shared. More specifically, our findings show that the procedure should be able to estimate the amount of *trust* we have in the recipient, the *sensitivity* of the information, and the *appropriateness* of sharing that specific information with that specific receiver. This prediction problem is in essence equivalent to the problem solved by a *context-aware recommender system* (cf. (Adomavicius and Tuzhilin 2011)). Whereas a typical recommender system estimates the values in a two-dimensional user-item matrix, a context-aware recommender system can incorporate additional contextual variables into the prediction model as additional dimensions. In this case, the recommender would predict the values in a three-dimensional user-item-recipient matrix (or even add additional dimensions for other factors such as companion or emotion). Given that we can distinguish different *types* of items and recipients that share similar levels of sensitivity, trust and appropriateness, such a context-aware recommender system is likely best implemented using variance reduction techniques such as Matrix Factorization (e.g. n-dimensional tensor factorization, (Karatzoglou et al. 2010)).

On a social network, the privacy adaptation procedure could assist users' selective sharing by predicting the audience with whom the user would be most likely to share the current post. The very same prediction model could also assist friend management by predicting which previous posts the user is most likely to share with a newly friended contact. This prediction could be used as the default setting for the post or the new friend, rather than the current default of "share everything with everyone" (cf. (Knijnenburg and Kobsa 2014; Smith, Goldstein, and Johnson 2013)).

Allowing some speculation, the same procedure could assist with users' privacy decisions regarding mobile apps; based on users' previous app installations, it could predict the optimal default privacy settings for a newly installed app

based on estimates of the sharing tendency of the user, the trustworthiness of the app, the sensitivity of the requested privacy setting, and the appropriateness of the setting, etc.

Concluding, the privacy adaptation procedure alleviates some of the burden of making a trade-off between the potential benefit and risk of information disclosure decisions; a tradeoff that is rather difficult for users to make. Our privacy decision-making prediction model combines several important psychological and contextual factors that influence this tradeoff, and learns their functionality by building a binary classifier. The proposed privacy decision-making prediction model produces good results based on the five identified factors, and can be used in a privacy adaptation procedure to assist users to protect their privacy in online social networks.

References

Acquisti, A., and Grossklags, J. 2005. Privacy and rationality in individual decision making. *IEEE Security & Privacy* 2:24–30.

Adams, A. 2000. Multimedia information changes the whole privacy ballgame. In *Proceedings of the Tenth Conference on Computers, Freedom and Privacy: Challenging the Assumptions*, CFP '00, 25–32. ACM.

Adomavicius, G., and Tuzhilin, A. 2011. Context-aware recommender systems. In *Recommender Systems Handbook*. Boston, MA: Springer US. 217–253.

Borcea-Pfitzmann, K.; Pfitzmann, A.; and Berg, M. 2011. Privacy 3.0 := data minimization + user control + contextual integrity. *Information Technology* 53(1):34–40.

Brenner, J., and Smith, A. 2013. 72% of online adults are social networking site users. *PewResearch Internet Project*.

Compañó, R., and Lusoli, W. 2010. The policy maker's anguish: Regulating personal data behavior between paradoxes and dilemmas. In *Economics of Information Security and Privacy*. Springer US. 169–185.

Consolvo, S.; Smith, I. E.; Matthews, T.; LaMarca, A.; Tabert, J.; and Powledge, P. 2005. Location disclosure to social relations: Why, when, & what people want to share. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '05, 81–90. ACM.

Culnan, M. J. 1993. "how did they get my name?": An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly* 17(3):341–363.

Fang, L., and LeFevre, K. 2010. Privacy wizards for social networking sites. In *Proceedings of the 19th International Conference on World Wide Web*, WWW '10, 351–360.

Gong, N. Z.; Xu, W.; Huang, L.; Mittal, P.; Stefanov, E.; Sekar, V.; and Song, D. 2011. Evolution of social-attribute networks: Measurements, modeling, and implications using google+. In *Proceedings of the 2012 ACM Conference on Internet Measurement Conference*, IMC'11, 131–144.

Hall, M.; Frank, E.; Holmes, G.; Pfahringer, B.; Reutemann, P.; and Witten, I. H. 2009. The weka data mining software: An update. *SIGKDD Explorations* 11(1).

Karatzoglou, A.; Amatriain, X.; Baltrunas, L.; and Oliver, N. 2010. Multiverse recommendation: N-dimensional tensor factorization for context-aware collaborative filtering. In *Proceedings of the Fourth ACM Conference on Recommender Systems*, 79–86.

Knijnenburg, B. P., and Kobsa, A. 2013. Making decisions about privacy: Information disclosure in context-aware recommender systems. *ACM Trans. Interact. Intell. Syst.* 3(3):20:1–20:23.

Knijnenburg, B. P., and Kobsa, A. 2014. Increasing sharing tendency without reducing satisfaction: Finding the best privacy-settings user interface for social networks. In *2014 International Conference on Information Systems (ICIS 2014)*.

Knijnenburg, B. P.; Kobsa, A.; and Jin, H. 2013. Dimensionality of information disclosure behavior. *International Journal of Human-Computer Studies* 71(12):1144–1162.

Lederer, S.; Mankoff, J.; and Dey, A. K. 2003. Who wants to know what when? privacy preference determinants in ubiquitous computing. In *CHI '03 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '03, 724–725.

Lewis, K.; Kaufman, J.; and Christakis, N. 2008. The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication* 14(1):79–100.

Liu, Y.; Gummadi, K. P.; Krishnamurthy, B.; and Mislove., A. 2011. Analyzing facebook privacy settings: user expectations vs. reality. In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, 61–70.

Nissenbaum, H. 2009. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Norberg, P. A.; Horne, D. R.; and Horne., D. A. 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs* 41(1):100–126.

Quercia, D.; Las Casas, D. B.; Pesce, J. P.; Stillwell, D.; Kosinski, M.; Almeida, V.; and Crowcroft, J. 2012. Facebook and privacy: The balancing act of personality, gender, and relationship currency. In *ICWSM'12*.

Ravichandran, R.; Benisch, M.; Kelley, P.; and Sadeh, N. 2009. Capturing social networking privacy preferences. In *Privacy Enhancing Technologies*, volume 5672 of *Lecture Notes in Computer Science*. Springer US. 1–18.

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

Smith, N. C.; Goldstein, D. G.; and Johnson, E. J. 2013. Choice without awareness: Ethical and policy implications of defaults. *Journal of Public Policy & Marketing* 32(2):159–172.

Swets, J. A. 1988. Measuring the accuracy of diagnostic systems. *Science (New York, N.Y.)* 240(4857):1285–1293.

Taylor, H. 2003. Most people are "privacy pragmatists" who, while concerned about privacy, will sometimes trade it off for other benefits. *The Harris Poll* 17(19).

Thaler, R. H., and Sunstein, C. 2008. *Nudge : improving decisions about health, wealth, and happiness*. New Haven, NJ & London, U.K.: Yale University Press.

Toch, E.; Cranshaw, J.; Drielsma, P. H.; Tsai, J. Y.; Kelley, P. G.; Springfield, J.; Cranor, L.; Hong, J.; and Sadeh, N. 2010. Empirical models of privacy in location sharing. In *Proc. of the 12th ACM intl. conference on Ubiquitous computing*, 129–138.

Westin, A. 1998. *E-commerce & Privacy: What Net Users Want*. Hackensack, NJ: Privacy & American Business.

Zickuhr, K. 2012. Three-quarters of smartphone owners use location-based services. Technical report, Pew Research.