Sharing Policies in Multiuser Privacy Scenarios: Incorporating Context, Preferences, and Arguments in Decision Making

Ricard L. Fogues, Universitat Politècnica de València
Pradeep K. Murukannaiah, North Carolina State University
Jose M. Such, Lancaster University
Munindar P. Singh, North Carolina State University

Social network services enable users to conveniently share personal information. Often, the shared information concerns other people, especially other members of the social network service. In such situations, two or more people can have conflicting privacy preferences; thus, an appropriate sharing policy may not be evident. We identify such situations as multiuser scenarios. Current approaches propose finding a sharing policy through preference aggregation. However, studies suggest that users feel more confident in their decisions regarding sharing when they know the reasons behind each other’s preferences. The goals of this paper are (i) understanding how people decide the appropriate sharing policy in multiuser scenarios where arguments are employed and defining a model based on this understanding; and (ii) make that model computational as an inference model. We survey 988 Amazon MTurk users about a variety of multiuser scenarios and the optimal sharing policy for each scenario. We evaluate the answers given by the participants and find that contextual factors, user preferences, and arguments influence the optimal sharing policy in a multiuser scenario. Then, we present an inference model that predicts the optimal policy given the three types of features with up to 86% accuracy.

CCS Concepts: • Security and privacy → Social aspects of security and privacy;
  General Terms: Experimentation; Human Factors

Additional Key Words and Phrases: Privacy; social media; multiuser; argumentation; crowdsourcing

ACM Reference Format:
DOI: 0000001.0000001

1. INTRODUCTION

A social network service (SNS) enables users to maintain social relationships via online interactions. As users on an SNS interact, they share information with each other. Often, the information shared on an SNS involves several users (e.g., a photo showing a group of people). Many SNSs enable users to connect the information they upload to other users so that the connected users can be notified of the uploaded information. Since the information shared varies depending on the SNS, these connections can take different forms, e.g., tags on a photo uploaded to Instagram or mentions in a tweet. Suppose Alice uploads a photo from last weekend’s party where she and her friend Bob appear together, and tags Bob in the picture. When these connections are created, the other users are linked to the uploaded information. Usually, a connection implies that the profile of the user can be accessed from the information or some personal information is shown in conjunction with
the uploaded data. Although connections between information and users are widely employed by SNSs, they can pose a privacy threat. For example, Bob may find that the photo Alice uploaded is sensitive. However, since Bob has no control over uploading that photo, Alice’s action can threaten Bob’s privacy. We identify a situation such as this as a multiuser privacy scenario.

Currently, SNSs do not provide mechanisms to handle multiuser privacy scenarios [Fogués et al. 2015]. Thus, a user who did not upload a piece of information concerning him must deal with the privacy settings chosen by the uploader; at best, the user can remove the connection that links him to the shared information, but the information itself remains nevertheless. An ideal solution in a multiuser scenario respects each user’s privacy. However, often such a solution may not be viable since the preferences of the users involved may conflict. For example, suppose Alice would like to share a photo in which Bob and she appear with her friend Charlie. However, Bob would like to share it only with his common friends and he does not know Charlie. Here, no solution completely respects both Alice and Bob’s preferences.

Several researchers, e.g., [Besmer and Richter Lipford 2010; Lampinen et al. 2011; Such et al. 2014; Wisniewski et al. 2012], have identified decision-support systems that help users resolve multiuser privacy conflicts as one of the biggest gaps in privacy management in social media. The main challenge that decision-support systems address is proposing an optimal solution: a solution most likely to be accepted by all those involved in the multiuser scenario. Although an optimal solution may not exist for each multiuser scenario, identifying one, when it exists, can minimize the burden on the users to resolve the conflict manually.

Other researchers, e.g., [Carminati and Ferrari 2011; Hu et al. 2013; Squicciarini et al. 2009; Such and Criado 2015; Thomas et al. 2010], have proposed methods to automatically determine solutions to conflicts based on users’ privacy preferences. These methods suffer from two main limitations. One, they always aggregate preferences in the same way regardless of the context. Two, they do not consider the reasons behind users’ preferences. However, evidence based on self-reported data [Lampinen et al. 2011; Wisniewski et al. 2012] suggests that users do listen to the explanations of others and that the optimal solution may depend on the particular context and reasons behind users’ preferences. Following this idea, we empirically study three types of factors that potentially influence a privacy decision: the scenario’s context, users’ preferences, and their arguments about those preferences. An argument is a justification a user employs to convince the others involved that the user’s expectations are reasonable and should be taken into account for making a decision.

Our key objective in this paper is to build an argumentation-based model that accurately represents a multiuser scenario. To this end, we (1) identify important factors that potentially influence the inference; (2) evaluate the relative importance of these factors in inferring an optimal solution; and (3) finally, make this model computational as an inference model that predicts an optimal solution for a given multiuser scenario.

We design a study where human participants are asked to choose what they think is the most appropriate sharing policy in a multiuser scenario we specified. Combining different values of the three types of factors we identified (context, preferences, and arguments), we generate 2,160 scenarios. Considering the sheer number of participants required, we conducted our study on Amazon Mechanical Turk (MTurk), collecting responses from 988 unique MTurk participants.

Contributions
(1) A novel model for representing multiuser privacy scenarios, employing three types of features: contextual factors, user preferences, and user arguments.
(2) Via a series of regression models, we evaluate each feature’s influence on the optimal policy.
(3) We describe an inference model that predicts the optimal policy for a multiuser scenario with up to 86% accuracy.

Organization
Section 2 identifies factors potentially influencing a multiuser privacy decision. Sections 3 and 4 describe our hypotheses and the MTurk study we designed to validate those hypotheses, respectively.
Section 5 describes our inference model based on data and Section 6 presents our results. Sections 7 and 8 provide a discussion of our results, some directions for future research, comparisons with related works, and a conclusion.

2. FACTORS INFLUENCING A MULTIUSER SHARING DECISION

We identify three important classes of factors that potentially influence the privacy decision in a multiuser scenario: context, user preferences, and arguments by users.

2.1. Context

Following Dey et al. [2001], we define the context of a multiuser scenario as any information—the information being shared or the people involved—that can influence the sharing decision. We identify four elements of the context:

- **Relationships among the individuals.** The type of relationship is known to play a crucial role when making individual decisions about privacy in social media [Kairam et al. 2012; Marwick and Boyd 2011]. Specifically, people share information differently with friends, family, and colleagues. We hypothesize that the types of relationships influence how a person negotiates in a multiuser scenario, as attributes of a relationship such as intimacy may influence how much an opinion is taken into account. For example, following Wisniewski et al. [2012], we imagine that a user’s friend would respect the user’s preferences.

- **Sensitivity of the information.** The sensitivity of the information to be shared is known to make an important contribution when making individual sharing decisions in social media [Sleeper et al. 2013; Wang et al. 2011]. Besides, judgments of appropriateness of information to be shared on an SNS are subjective. For example, in some cultures, drinking alcohol is taboo. Thus, a photo showing a person drinking can be inappropriate in such a culture, whereas it can be normal in other cultures. Each individual involved in a scenario has a perception of the sensitivity of the information. This perception may affect how important that person thinks his view is on the appropriate sharing decision.

- **Sentiment of the information.** Personal information may evoke certain sentiments. For example, a photo from a birthday party where people are having fun evokes a positive feeling. Conversely, a photo from a funeral would typically evoke a negative feeling. As Kairam et al. [2012] describe, the most common motivation to share information on an SNS is self-presentation: users care about what image they project. Therefore, the sentiment conveyed by the information they share can be important when deciding what to share.

2.2. Preferences

The goal of each individual in a multiuser privacy scenario is to persuade the sharer to apply the individual’s preferred sharing policy to the information. The individuals’ (including sharer’s) preferences can be compatible or conflicting. For example, Bob’s preference: “I do not want my parents to see this photo” is compatible with Alice’s preference: “I want only my friends to see it,” as long as Bob’s parents are not Alice’s friends. Optimally, the final decision to resolve a conflict should respect the preferences of every individual involved to the best possible extent. If all preferences are compatible with each other, the solution is trivial. However, in case of conflict, an acceptable solution may not be evident.

A sharing policy can imply no sharing, sharing publicly, or anything in between. Further, depending on the number of contacts and their type, sharing policies change from one SNS user to another. Given the large space of possibilities, for the sake of simplicity, we consider the possible sharing policies to three levels of disclosure:

- **Share with all.** Anyone on the SNS can access the information.
- **Share with common friends.** Only common friends of the individuals involved in the scenario can access the information.
Share among themselves. Only the individuals directly connected with the information can access the information.

2.3. Arguments

An individual involved in a multiuser scenario may employ arguments to convince the others that his preferred sharing policy should be used, or at least considered for making the final decision. There are potentially many arguments one can employ to negotiate with or persuade another. Arguments can be thought of as instances of argumentation schemes [Walton et al. 2008], representing forms of inference from premises to a conclusion. Walton et al. show that arguments used in everyday conversation fall into a small number of schemes.

We identify four argument schemes that can be effective in deciding an optimal solution for a multiuser privacy scenario: argument from (i) good consequences, (ii) bad consequences, (iii) an exceptional case, and (iv) popular opinion. It is important to note that we neither claim these as the only possible schemes applicable in resolving a multiuser privacy conflict nor do we seek to evaluate if these are the best possible schemes. Our objective is to evaluate if arguments, as instances of schemes, help in deciding the final policy in multiuser scenarios. Our purpose of using argument schemes is to restrict the arguments to be of a few well-defined types, instead of choosing the arguments arbitrarily.

Argument from good or bad consequences. The general structure of an argument from this scheme is:

If A is brought about, then good (bad) consequences will occur. Therefore, A should (not) be brought about.

An example of an argument from good consequences is: We had a lot of fun during the party. Everybody’s talking about how funny you were and they want to see your photos. Let’s share it with everybody. An example of an argument from bad consequences is: It’s a funny photo, but embarrassing since I appear drunk. I don’t want strangers seeing it.

An SNS user, who shares something, expects to obtain some benefit, e.g., friendship, jobs, or other social opportunities [Ellison et al. 2007]. Thus, it is reasonable to argue that sharing certain information implies a good consequence. But, sharing inappropriate information can harm people’s feelings and cause social tension. Thus, negative consequences can be valid arguments for not sharing.

Argument from an exceptional case. If the case of x is an exception, then the established rule can be waived in case of x.

Example: C’mom! it was our graduation party! something that we do only once in our lifetimes. We should show it to the world.

Although prior experience can guide future decisions, handling exceptions requires a different approach. Instances of this scheme cover cases where an unusual privacy configuration is required: potentially, the opposite of the policy that might have been adopted if the arguments were not provided. Obviously, an individual must make a strong case to justify that the information is exceptional.

Argument from popular opinion. If a large majority in a particular group G accepts A as true (false), then there is a presumption in favor of (against) A.

Example: The majority of the people that appear in the photo think that it should be kept private. Therefore, we should not share it with anyone.

We consider that users never argue that the correct sharing policy is the one supported by the majority. For example, we do not consider arguments like “The majority of us wants to share this photo only with common friends, hence, we should share it only with common friends.” Therefore, this argument emerges when two or more users suggest the same sharing policy. Thus, although no individual explicitly employed an argument from popular opinion, it is implicitly considered for the final outcome.
3. HYPOTHESES

We seek to evaluate the following hypotheses:

**H1: Context.** Contextual factors, specifically, sensitivity and sentiment of the information shared, and the relationships among individuals involved influence the optimal sharing policy in a multiuser privacy scenario.

**H2: Preferences.** Preferences of users involved in a multiuser scenario influence the choice of optimal policy for the scenario.

**H3: Arguments.** Users’ arguments for their preferred sharing policies influence the choice of optimal policy in a multiuser privacy scenario.

**H4: Prediction is enhanced by preferences.** Adding preferences to the contextual factors enhances the accuracy of an inference model predicting the optimal policy for a given multiuser privacy scenario.

**H5: Prediction is enhanced by arguments.** Adding arguments to preferences and contextual factors enhances the accuracy of an inference model predicting the optimal policy for a given multiuser privacy scenario.

**H6: Confidence is enhanced by preferences.** Adding preferences to the contextual factors enhances a user’s confidence in choosing the optimal policy for a given multiuser privacy scenario.

**H7: Confidence is enhanced by arguments.** Adding arguments to preferences and contextual factors enhances a user’s confidence in choosing the optimal policy for a given multiuser privacy scenario.

4. DATA COLLECTION

To test our hypotheses, we seek to investigate situations with varying degrees of sensitivity (one of the contextual factors). Doing so is problematic [Wang et al. 2011] as participants are reluctant to share sensitive information, biasing the study toward nonsensitive issues. An alternative would be asking participants to self-report how they behave when they experience a multiuser privacy scenario, but the results may not match participants’ actual behavior because of the well-known dichotomy between users’ stated privacy attitudes and their actual behavior [Acquisti and Gross 2006]. Therefore, we chose to create situations in which participants are immersed [Mancini et al. 2010] to improve actual behavior elicitation while avoiding biasing the study to nonsensitive situations.

We present information about two or more individuals in a specific circumstance: a combination of context, preferences, and arguments. We ask the subject to choose an optimal sharing policy for that circumstance.

We recruited participants for our study from Amazon MTurk [Paolacci et al. 2010]. We directed each participant to an external website that asked the participant to complete seven survey instruments: a presurvey questionnaire about demographics, five picture surveys (each involving a privacy conflict scenario and three sets of questionnaires), and a post-survey questionnaire about the participant’s general opinions about resolving multiuser privacy conflicts. The study was approved by the IRB at North Carolina State University (details about participants and rewards in Section 4.4).

4.1. Presurvey Questionnaire

We asked participants to report their age, gender, level of education, how frequently they use social media, and how often they share (multiuser) pictures online. Since some of the situations we presented to the participants could be inappropriate for young readers, we required participants to be older than 18 years of age and showed a disclaimer at the beginning that the survey may be inappropriate for some users.

4.2. Picture Survey

The picture survey is the core of our study. We first show a picture and describe a hypothetical scenario in which the picture was taken and next ask a series of questions. Table 1 shows two
examples of picture survey. We generated these and several similar picture surveys by combining factors identified in Section 2 as described below.

<table>
<thead>
<tr>
<th>Picture</th>
<th>Description</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aiko (C) took the picture above with her colleagues Ichiro and Katsu and, a French volunteer at the tsunami relief center</td>
<td>Identify the relationship between Aiko, Ichiro, and Katsu and rate the sensitivity and sentiment of the picture</td>
<td>Consider that Aiko wants to upload this picture to his social media account. What sharing policy should she apply for the picture?</td>
</tr>
<tr>
<td>Three friends, Mark, Alex, and John, took the picture above during Mark’s bachelor party on a boat in Ibiza</td>
<td>Identify the relationship between Mark, Alex, and John and rate the sensitivity and sentiment of the picture</td>
<td>Consider that Alex wants to upload this picture to his social media account. What sharing policy should he apply for the picture?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Case 1: Context</th>
<th>Case 2: Context</th>
<th>Case 3: Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aiko wants to upload this picture to his social media account. What sharing policy should she apply for the picture?</td>
<td>Next, consider the users’ preferences as follows</td>
<td>Finally, consider the users’ preferences and arguments as follows</td>
</tr>
<tr>
<td>— Ichiro: Share among ourselves</td>
<td>— Aiko: Share among ourselves</td>
<td>— Aiko: This was one of the worst natural disasters ever happened. Share among ourselves</td>
</tr>
<tr>
<td>— Katsu: Share with all</td>
<td>— Ichiro: Share among ourselves</td>
<td>— Ichiro: Tsunami was a disaster and our gestures are not appropriate; people may get the wrong idea. Share among ourselves</td>
</tr>
<tr>
<td>Now, considering the context and users’ preferences, what sharing policy should Aiko apply for the picture?</td>
<td>Now, considering the context and users’ preferences, what sharing policy should Alex apply for the picture?</td>
<td>Now, considering the context, and users’ preferences and arguments, what sharing policy should Aiko apply for the picture?</td>
</tr>
<tr>
<td>— Mark: Share among ourselves</td>
<td>— Alex: Share with common friends</td>
<td>— Mark: Share among ourselves</td>
</tr>
<tr>
<td>— Alex: Share with common friends</td>
<td>— John: Share with all</td>
<td>— Alex: This was one of the best day of our lives. Share with common friends</td>
</tr>
<tr>
<td>— John: Share with all</td>
<td>Now, considering the context and users’ preferences, what sharing policy should Alex apply for the picture?</td>
<td>— John: This is not like any other picture; it was from Mark’s bachelor party! Share with all</td>
</tr>
<tr>
<td>Now, considering the context, and users’ preferences and arguments, what sharing policy should Alex apply for the picture?</td>
<td>Now, considering the context, and users’ preferences and arguments, what sharing policy should Alex apply for the picture?</td>
<td>Now, considering the context, and users’ preferences and arguments, what sharing policy should Alex apply for the picture?</td>
</tr>
</tbody>
</table>

(1) Regarding context variables, we consider a predefined set of relation types, namely, friends, family, and colleagues. Further, we assume that all individuals involved in a scenario have the same type of relationship with each other (i.e., all of them are either friends, family, or colleagues). Also, the photos shown in the situations could be sensitive or nonsensitive and convey either a positive or a negative sentiment. This leads to 12 possible contexts. We found a representative
picture for each of those combinations. For example, in Table I, for the picture on the left the relationship is colleagues, sensitivity is low, and sentiment is negative; in contrast, for the picture on the right the relationship is friends, sensitivity is high, and sentiment is positive.

(2) Some combinations of argument and privacy policy would not make sense in a real situation. Specifically, an argument from bad consequence does not often support a share with all policy. Similarly, an argument from good consequence does not often support a share among themselves policy. Further, we restrict ourselves to scenarios where arguments from exceptional case only support policies at either extreme: share with all or share among themselves. This yields six policy-argument combinations.

(3) We limit the number of individuals involved in each scenario to three. This way, the implicit argument from popular opinion could work (when applied) without ties. Although some scenarios we employed showed pictures with more than three individuals, our scenarios discussed the preferences and arguments of only three of the individuals among the people involved with the picture.

(4) We make sure that not all three individuals in a scenario use the same policy-argument combination. Our objective is to understand how a user decides a final policy given the scenario, and the preferences and arguments of others in the scenario. If all users thought the same way and wanted the same result, the solution would be trivial.

Putting the above together, we have: 12 pictures based on context, six policy-argument combinations each of first two individuals can employ, and five policy-argument combinations the last individual can employ (last restriction above). That is, we generated 2,160 scenarios. Each MTurk participant was shown five unique scenarios, making sure that no participant is shown the same picture twice. Further, we asked participants to immerse themselves in the particular scenario and ignore the resemblance or lack of resemblance of each scenario to other scenarios in which they might have seen this picture.

Following the picture and its description were four sets of questionnaires. We asked participants to answer these questionnaires sequentially and when answering a questionnaire, to consider information provided to them up to that point only.

The first questionnaire asks participants to assign values to three contextual variables: sensitivity (Likert scale 1 = not sensitive at all, 5 = very sensitive), sentiment (1 = extremely positive, 5 = extremely negative), and type of relationship among the people involved in the conflict (family, colleagues, or friends).

The next three questionnaires tell participants that one of the individuals in the scenario wants to upload the picture to a social media account. We ask participants what sharing policy should be applied. The participants choose one of the policies from share with all, share with common friends, and share among themselves. In the first case, participants know only the contextual attributes, but not the preferences or arguments of the individuals in the scenario. This case is similar to a real scenario where a user wants to upload and share information without asking others potentially concerned with the information. The second case introduces the preferences of all the users, but without their arguments supporting preferences. The third case employs all of the elements: the individuals in the scenario expose their preferences and support them with arguments. We keep the preferences fixed from the second case to the third, so we can observe the effect arguments have on the final decision.

4.3. Post-Survey Questionnaire

The post-survey questionnaire asks the following questions (omitting some for brevity).

(1) How important do you think the following factors are in choosing an appropriate policy when sharing information concerning multiple users on social media? (a) Relationship between stakeholders; (b) Sensitivity of the information shared; and (c) Sentiment of the information shared. The response to each factor was on a Likert scale (1 = not important at all, 5 = extremely important).
How confident will you be in choosing an appropriate policy for sharing information concerning multiple users on social media in the following cases? (a) You do not know stakeholders preferences or arguments; (b) You know users preferences, but not their arguments; and (c) You know users preferences and arguments. The response to each case was on a Likert scale (1 = not confident at all, 5 = extremely confident).

Responses to the above questions allow us to find correlations (or lack thereof) between participants’ self-reported behavior and what they actually answered during the study. Also, we use responses to the second question to evaluate hypotheses H6 and H8.

4.4. Participants and Quality Control

We needed 432 participants to receive one response per scenario (each participant responds to five of 2,160 scenarios). We intended to get two responses per scenario for completeness. However, we anticipated that some participants would begin a survey but not finish it, leaving gaps in the completed responses. To address this challenge, we launched the study on MTurk in multiple batches. For each batch, we checked if a particular survey needed additional responses and restricted the posted tasks accordingly. The final number of unique participants that completed the study was 988. At the end, each scenario had received at least two responses and some three responses. Compensation was provided for only those who completed all seven steps in the survey.

For quality control, we required participants to have completed at least 50 tasks on MTurk and to have had a success rate of at least 90% [Peer et al. 2014]. We also included an attention check question in the ratings section of each picture survey, asking how many people (faces) were present in the picture, answering which requires counting from the picture.

Table II. Demographics of MTurk participants of our study

<table>
<thead>
<tr>
<th>Gender</th>
<th>Male: 46.3%, Female: 53.4%, Other: 0.3%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age</td>
<td>18–20: 2%, 21–29: 36.6%, 30–39: 36%, 40–49: 13.7%, 50–59: 7.5%, 60 or more: 4.1%</td>
</tr>
<tr>
<td>Education</td>
<td>Graduate degree: 11.2%, Bachelor degree: 44.4%, College no degree: 30.9%, High school: 12.4%, Less than high school: 1%</td>
</tr>
<tr>
<td>Social media usage</td>
<td>Daily: 83.9%, Weekly: 12%, Monthly: 3.7%, Never: 0.4%</td>
</tr>
<tr>
<td>Pictures shared</td>
<td>Many (&gt;5): 35.1%, Few (1–5): 45%, None: 18.1%, Not sure: 1.7%</td>
</tr>
<tr>
<td>Conflicts experienced</td>
<td>Many (&gt;5): 2.8%, Few (1–5): 30.1%, None: 66%, Not sure: 1.1%</td>
</tr>
</tbody>
</table>

Table II summarizes our participants’ responses to the presurvey questionnaire. The question corresponding to the last row in the table was in the post-survey questionnaire, so that participants understand what multiuser conflicts look like before answering that question. As shown, the majority of our participants used social media on a daily basis. Over 80% of our participants had shared a picture showing multiple users and about one-third of them had experienced privacy conflicts.

5. INFERENCe MODELS

After collecting data from all participants, we build statistical models to evaluate our hypotheses. In our setting:

A data instance. corresponds to a participant’s response to a picture survey.
The response (class) variable. is the final policy chosen by the participant. For regression, we map share with all to 0, share with common friends to 0.5, and share among themselves to 1. That is, larger values correspond to more restrictive policies. For our classifiers, the final policy is discrete.
The predictors (features). are divided into three cases corresponding to the three cases in the picture survey. That is, Case 1 consists of contextual features, Case 2 consists of contextual and...
preference-based features, and Case 3 consists of contextual, preference-based, and argument-based features. For brevity, we refer to these cases as Context, Preferences, and Arguments, respectively.

5.1. Features

5.1.1. Contextual Features. We compute the contextual features based on participants’ responses in the ratings section of the picture survey.

Sensitivity and sentiment. Ratings normalized to [0, 1].

Relationship. Since relationships can have many dimensions [Hassebrauck and Fehr 2002], e.g., love, flexibility, and empathy, no specific order is obvious. We experiment with this order and choose the one that yields the best result for the models we build. This order is: friendship is 0, family is 0.5, and colleagues is 1.

5.1.2. Preference-Based Features. We compute the following features based on the preferences portrayed in the corresponding scenario (picture survey). For concreteness, we base our examples on Table I (left).

Preference counts. represents three features corresponding to the number of participants preferring each of the three policies. In Table I (left), the preference counts are: share with all is 1, share with common friends is 0, and share among themselves is 2.

Most and least restrictive policies. represent, among the preferred policies of the users in a scenario, the policy restricting the sharing of information most and least, respectively. In Table I (left), the most restrictive policy is share among themselves, and least restrictive policy is share with all.

Majority policy. represents the policy preferred by the majority of the users involved in the scenario. This feature can be null if there is no majority. The majority policy in our example is share among themselves.

5.1.3. Argument-Based Features. Unlike preference-based features, argument-based features incorporate preferences within an argument, each of which is an instance of one of the argument schemes we consider.

Argument counts. for Table I (left) are as follows. Each of these three arguments has a count of 1: Aiko’s argument from an exceptional case supporting share among themselves; Ichiro’s argument from negative consequence supporting share among themselves; and Katsu’s argument from positive consequence supporting share with all. Each of the remaining three arguments (recall that there are six argument-policy combinations) has a count of 0.

Argument supporting least restrictive policy. is argument from positive consequence supporting share with all.

Arguments supporting least restrictive policy. are argument from positive consequence and argument from an exceptional case both supporting share among themselves.

Arguments supporting majority policy. are argument from positive consequence and argument from an exceptional case both supporting share among themselves.

When arguments from distinct schemes support a policy, as in the arguments supporting least restrictive policy and majority policy cases above, we employ the combination of arguments as a distinct feature value. Also, if a majority policy does not exist, we set the corresponding argument-based feature to null.

5.2. Models and Measures

To evaluate hypotheses H1–H4, we build multiple linear regression models (multiple predictors and one response variable). We adopt the coefficient of determination as a measure of goodness of fit of
these models. This measure is defined via:

\[ R^2 = 1 - \frac{\text{SSE}}{\text{SST}}, \]

(1)

where SSE is the sum of square errors, and SST is the total sum of squares. Further, we focus on regression coefficients and their statistical significance. These coefficients help us understand each feature’s relative influence on the optimal policy. To compare coefficients on the same scale, we normalize all features to \([0, 1]\).

We create regression models that include all the features of a type (contextual factors, preferences, and arguments), when possible. However, some features of the same type can be highly correlated, causing multicollinearity [Gujarati and Porter 2009]. In that case, the coefficients may change erratically in response to small changes in the data. To counter this effect, we create independent models for highly correlated predictors. It is worth noting that this correction usually leads to higher coefficients.

To evaluate H5 and H7, we build classification models. We evaluate the prediction accuracy of these models via:

\[
\text{precision} = \frac{\text{TP}}{\text{TP} + \text{FP}},
\]

\[
\text{recall} = \frac{\text{TP}}{\text{TP} + \text{FN}},
\]

\[
F_1\text{-measure} = 2 \times \frac{\text{precision} \times \text{recall}}{\text{precision} + \text{recall}},
\]

(2)

where TP, TN, FP, and FN refer to true and false positives and negatives. We implemented these models using Weka [Hall et al. 2009]. We perform 10-fold cross-validation and cross-validated paired \(t\)-test [Dietterich 1998] to test significance in differences, when required.

To evaluate H6 and H8, we perform the Kruskal-Wallis test [Hollander and Wolfe 1999] on self-reported data from the post-survey questionnaire. The Kruskal-Wallis test is a nonparametric extension (thus, does not require the assumptions that populations have normal distributions) of one-way ANOVA. This test compares medians to determine if all ratings come from the same distribution. If Kruskal-Wallis test determines that all the ratings do not come from the same distribution, we perform the multiple comparison test in Matlab [Matlab] (with default settings) to determine which variables are significantly different.

6. RESULTS

In this section, we evaluate each of our hypotheses from Section 3.

6.1. H1: Context

Table III shows the coefficients of the linear regression model, employing contextual factors as predictors. We highlight statistically significant differences at significance levels (\(\alpha\)) of 5% and 1% with * and **, respectively.

In the models for all three cases, we find that sensitivity and relationship type are significantly influential factors, but sentiment is not. Also, sensitivity has the largest coefficient among the three factors, indicating that it is most influential contextual factor in deciding on the final sharing policy. Our intuition, based on these observations, is that a highly sensitive picture is usually shared only among the individuals involved or with common friends; also, pictures involving colleagues and family tend to be shared more cautiously than pictures with friends.

Further, we observe that as additional factors are considered, the coefficients of the contextual factors decrease. Also, \(R^2\) decreases drastically from Context to Preferences. This indicates that when preferences and arguments are taken into account by users, the contextual factors’ influence on the optimal sharing policy diminishes.
To further analyze the contextual factors, we compare these results with self-reported data collected in the post-survey questionnaire. In this way, we can observe if participants’ opinions are consistent with the decisions they made in the picture survey. Figure 1 shows the boxplots for participants’ importance ratings to each contextual factor. A diamond dot in the boxplot indicates the mean. Each dot outside a box indicates an outlier.

From Table III and Figure 1, we observe that the regression model and self-reported values follow a similar pattern: sensitivity is the most influential factor. However, an important distinction between the two is that although relationship and sentiment have similar ratings in the post-survey questionnaire, sentiment is not significantly influential in the regression model. Also, in the post-survey questionnaire relationship and sentiment have high (median of 4) importance ratings. However, their low regression coefficients suggest that participants did not consider them as important as they said in the post-survey questionnaire.

### 6.2. H2: Preferences

The regression models for contextual factors suggest that employing preferences can influence the final sharing decision. Table IV shows the regression coefficients for models employing preference-based features. Since Context does not employ preferences, only Preferences and Arguments are shown. We note that preference counts are highly correlated: when one count increases, the other two (naturally) decrease, causing multicollinearity. To counter this effect, we create independent models for highly correlated predictors. Therefore, the coefficient values for the preference counts features are obtained from different regression models: each of these models only employs one preference count as predictor.

First, we observe that preference counts have a direct influence on the final sharing policy. The sign (positive or negative) of a coefficient indicates the directionality of the influence (recall that we treat all as 0, common as 0.5, and self as 1). Second, from the coefficients, we observe that the most restrictive policy has the most influence on the final policy, more so than even the majority policy. Finally, the coefficients of the preference-based features do not change much from Preferences to Arguments. This indicates that preferences remain important even when both preferences and arguments are considered.

---

Table IV. Regression coefficients for preference features

<table>
<thead>
<tr>
<th>Variable</th>
<th>Coefficients</th>
<th>Preferences</th>
<th>Arguments</th>
</tr>
</thead>
<tbody>
<tr>
<td># Share with all</td>
<td>−0.137**</td>
<td>–0.147**</td>
<td></td>
</tr>
<tr>
<td># Share with common friends</td>
<td>−0.065**</td>
<td>−0.059**</td>
<td></td>
</tr>
<tr>
<td># Share among themselves</td>
<td>0.15**</td>
<td>0.153**</td>
<td></td>
</tr>
<tr>
<td>Least restrictive policy</td>
<td>0.107**</td>
<td>0.15**</td>
<td></td>
</tr>
<tr>
<td>Most restrictive policy</td>
<td>0.448**</td>
<td>0.425**</td>
<td></td>
</tr>
<tr>
<td>Majority policy</td>
<td>0.113**</td>
<td>0.112**</td>
<td></td>
</tr>
<tr>
<td>( R^2 )</td>
<td>0.118**</td>
<td>0.119**</td>
<td></td>
</tr>
</tbody>
</table>

6.3. H3: Arguments

Table V shows the regression coefficients for the argument-based features. As for the policy counts, the argument counts are also highly correlated. Thus, we use different models for those features.

Considering the mean values of the coefficients (ignoring the sign), preferences supported by positive arguments have the highest coefficients (mean 0.1741), followed closely by those supported by exceptional case arguments (mean 0.1704); the arguments for negative consequences yield the lowest coefficients (mean 0.1329). This suggests that users tend to value the benefits more than the risks of sharing a picture. However, it is worth noting that argument from bad consequences supporting self (share among themselves) has the highest coefficient of all argument counts. This indicates that when a user makes a strong case for not sharing a picture, the other users respect that preference. This finding is consistent with those of Besmer and Richter Lipford [2010] and Wisniewski et al. [2012].

Table V. Regression coefficients for argument features

<table>
<thead>
<tr>
<th>Variable</th>
<th>Coefficients</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td># Positive supporting all</td>
<td>−0.208**</td>
<td></td>
</tr>
<tr>
<td># Positive supporting common</td>
<td>−0.12**</td>
<td></td>
</tr>
<tr>
<td># Negative supporting common</td>
<td>−0.045**</td>
<td></td>
</tr>
<tr>
<td># Negative supporting self</td>
<td>0.344**</td>
<td></td>
</tr>
<tr>
<td># Exceptional supporting all</td>
<td>−0.145**</td>
<td></td>
</tr>
<tr>
<td># Exceptional supporting self</td>
<td>0.153**</td>
<td></td>
</tr>
<tr>
<td>Positive supporting least restrictive policy</td>
<td>0.106**</td>
<td></td>
</tr>
<tr>
<td>Negative supporting least restrictive policy</td>
<td>0.152**</td>
<td></td>
</tr>
<tr>
<td>Exceptional supporting least restrictive policy</td>
<td>0.12**</td>
<td></td>
</tr>
<tr>
<td>Positive supporting most restrictive policy</td>
<td>−0.171**</td>
<td></td>
</tr>
<tr>
<td>Negative supporting most restrictive policy</td>
<td>−0.11**</td>
<td></td>
</tr>
<tr>
<td>Exceptional supporting most restrictive policy</td>
<td>−0.156**</td>
<td></td>
</tr>
<tr>
<td>Positive supporting majority policy</td>
<td>−0.266**</td>
<td></td>
</tr>
<tr>
<td>Negative supporting majority policy</td>
<td>−0.014</td>
<td></td>
</tr>
<tr>
<td>Exceptional supporting majority policy</td>
<td>0.277**</td>
<td></td>
</tr>
<tr>
<td>( R^2 )</td>
<td>0.117</td>
<td></td>
</tr>
</tbody>
</table>

6.4. H4 and H5: Prediction

The foregoing hypotheses concerned how various features influence a sharing policy. Now, we evaluate a predictive model that puts these features to use. Since our objective is to predict the actual policy (all, common, or self), we build three-class classifiers, which make discrete predictions (in contrast to regression models, which make continuous predictions).

To start with, we build decision tree classifiers, using the J48 implementation in Weka [Hall et al. 2009], for different feature sets. Table VI compares the prediction accuracies of decision trees for
Table VI. Accuracies of decision tree classifiers for the three cases, considering all data instances

<table>
<thead>
<tr>
<th>Class</th>
<th>Precision</th>
<th>Recall</th>
<th>$F_1$</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context</td>
<td>0.521</td>
<td>0.463</td>
<td>0.490</td>
<td>1032</td>
</tr>
<tr>
<td></td>
<td>0.493</td>
<td>0.420</td>
<td>0.454</td>
<td>1405</td>
</tr>
<tr>
<td></td>
<td>0.590</td>
<td>0.720</td>
<td>0.649</td>
<td>1463</td>
</tr>
<tr>
<td></td>
<td>0.537</td>
<td>0.544</td>
<td>0.537</td>
<td>weighted mean</td>
</tr>
<tr>
<td>Preferences</td>
<td>0.318</td>
<td>0.047</td>
<td>0.081</td>
<td>601</td>
</tr>
<tr>
<td></td>
<td>0.591</td>
<td>0.609</td>
<td>0.600</td>
<td>1590</td>
</tr>
<tr>
<td></td>
<td>0.606</td>
<td>0.772</td>
<td>0.679</td>
<td>1709</td>
</tr>
<tr>
<td></td>
<td>0.556</td>
<td>0.594</td>
<td>0.555</td>
<td>weighted mean</td>
</tr>
<tr>
<td>Arguments</td>
<td>0.326</td>
<td>0.100</td>
<td>0.153</td>
<td>628</td>
</tr>
<tr>
<td></td>
<td>0.614</td>
<td>0.641</td>
<td>0.627</td>
<td>1528</td>
</tr>
<tr>
<td></td>
<td>0.645</td>
<td>0.780</td>
<td>0.706</td>
<td>1744</td>
</tr>
<tr>
<td></td>
<td>0.581</td>
<td>0.616</td>
<td>0.586</td>
<td>weighted mean</td>
</tr>
</tbody>
</table>

Table VII compares the prediction accuracies for the three cases, considering only the consistent responses. Now, we observe that not only do the accuracies increase for each case, the differences in the accuracies of the cases increase as well.

Next, we make two interesting observations from counts in Tables VI and VII. First, we observe that the count for all class reduces drastically from Context to Preferences or Arguments. Thus,

\[ p < 0.01 \]
given preferences or arguments, users tend to choose more restrictive policies. Second, the count for common class reduces from Preferences to Arguments. This suggests that given only preferences, users tend to choose a safe option (common). However, supporting preferences by arguments can encourage users to choose extreme options in some scenarios (notice the increase in self and all classes for Arguments).

Table VIII. Accuracies of three classifiers for Arguments, considering consistent data instances only

<table>
<thead>
<tr>
<th>Classifier</th>
<th>Precision</th>
<th>Recall</th>
<th>F1</th>
<th>Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Naive Bayes</td>
<td>0.313</td>
<td>0.500</td>
<td>0.385</td>
<td>all</td>
</tr>
<tr>
<td></td>
<td>0.838</td>
<td>0.666</td>
<td>0.742</td>
<td>common</td>
</tr>
<tr>
<td>Logistic Regression</td>
<td>0.818</td>
<td>0.876</td>
<td>0.846</td>
<td>self</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.787</td>
<td>weighted mean</td>
</tr>
<tr>
<td></td>
<td>0.456</td>
<td>0.351</td>
<td>0.397</td>
<td>all</td>
</tr>
<tr>
<td></td>
<td>0.803</td>
<td>0.789</td>
<td>0.796</td>
<td>common</td>
</tr>
<tr>
<td></td>
<td>0.836</td>
<td>0.876</td>
<td>0.855</td>
<td>self</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.794</td>
<td>weighted mean</td>
</tr>
<tr>
<td>Random Forests</td>
<td>0.653</td>
<td>0.463</td>
<td>0.541</td>
<td>all</td>
</tr>
<tr>
<td></td>
<td>0.875</td>
<td>0.849</td>
<td>0.861</td>
<td>common</td>
</tr>
<tr>
<td></td>
<td>0.882</td>
<td>0.940</td>
<td>0.910</td>
<td>self</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.862</td>
<td>weighted mean</td>
</tr>
</tbody>
</table>

Finally, to make sure that our conclusion are not specific to decision trees, we experiment with three more classifiers: Naive Bayes, Logistic Regression, and Random Forests. Table VIII compares the accuracies of these models for Arguments. We observe that Random Forests, an ensemble learning approach, yields the best accuracies among all the four classifiers (including decision trees).

6.5. H6 and H7: Confidence

We compare a user’s confidence in choosing an optimal sharing policy given information corresponding to the three cases. Figure 2 shows the boxplots of the participants’ confidence ratings collected from the post-survey questionnaire. Further, from Kruskal-Wallis and multiple comparison tests, we find that the median ($\tilde{x}$) confidence rating for Preferences compared to Context, and Arguments compared to Preferences is significantly ($p < 0.01$) larger. This suggests that adding preferences and arguments to the contextual factors increases a user’s confidence in choosing an optimal sharing policy for a scenario.

$\tilde{x}(\text{Arguments}) \succ \tilde{x}(\text{Preferences}) \succ \tilde{x}(\text{Context})$ **

Fig. 2. Users’ confidence (from the post-survey questionnaire) in choosing the optimal policy for different cases
7. DISCUSSION

Our results show that contextual factors, preferences, and arguments influence the optimal sharing policy. However, we find a disconnection between the importance rating assigned by participants to contextual factors and how these factors actually influence the optimal policy. Participants considered that the sentiment a picture conveys is an important element (rating 4 out of 5). However, according to our regression model, the influence of sentiment over the optimal policy is not statistically significant.

The inference models show that arguments help in predicting the optimal policy. Moreover, the majority of participants reported that they feel much more confident about what policy to apply to a shared item if they know others’ arguments and preferences. These results indicate that approaches based only on aggregating user preferences, e.g., [Carminati and Ferrari 2011; Hu et al. 2011; Thomas et al. 2010] (as discussed below), may not be effective. Our results show that users are willing to accommodate others’ preferences if they know their reasons. Therefore, knowing only the preferences is not enough to set a policy that is satisfactory for the majority of the users involved.

7.1. Threats to Validity

We identify two threats to validity of our findings. First, any study based on surveys is susceptible to participant confusion. We mitigated this threat via quality control measures (Section 4.4). Second, to avoid both the unreliability of self-reported attitudes and the logistical challenges of finding participants in sets of three friends, we employ scenarios in which users immerse themselves and provide their assessment of the policies, preferences, and arguments under consideration. However, a user’s decision making as a third party (even if immersed) and as a person involved in a real scenario may be different.

7.2. Limitations and Directions

We identify three directions for future work. First, for logistical reasons, we employ predefined types of arguments, policies, and contexts. Thus, our findings are specific to these values. Nonetheless, other schemes can fit in a multiuser scenario. A future study could attempt to understand what arguments users would employ to support their preferences during a multiuser scenario—benefit being to discover new argumentation schemes. Automated techniques for identifying arguments [Lippi and Torroni 2015] can be valuable in this regard.

Second, privacy management on SNS is tedious [Fang and LeFevre 2010]; dealing with multiuser privacy conflicts only increase this burden. To lighten this task, users can take advantage of recommender tools to help them decide the optimal policy. As future work, we plan on building such recommender tool and test it with real users, so we can collect information about its accuracy and usability.

Third, our study is cross-sectional (one time) and in the scenarios of the study, decisions are to be made in one round. Thus, our study does not provide data to understand how users deal with situations where their arguments are countered by others’ arguments. A future study could require participants to engage in negotiation and persuasion to decide an optimal sharing policy for a scenario. Such a study requires coordinating multiple participants; thus, conducting such a study on MTurk is nontrivial. Employing automated agents (built based on the data we collected in our study) against one or a few real participants is a viable and interesting direction.

7.3. Related Work

Thomas et al. [2010] propose veto voting as a direct approach to manage multiuser sharing policies. That is, denying access takes precedence over granting access. Thus, if an individual wants to share the information with a given user, but another individual does not, the information is not shared. Whereas this approach does not allow privacy breaches, it may lead to utility loss. For example, suppose Alice and Bob appear together in a picture. Bob initially opposes sharing the picture with
Charlie as he does not know him. However, if Alice tells him that Charlie is her friend and that everything is OK, then Bob may accept sharing with Charlie. Had veto voting been applied, the picture would have not been shared with Charlie, thereby missing an opportunity to share the picture.

Other approaches too tackle multiuser privacy conflicts [Carminati and Ferrari 2011; Hu et al. 2013; Hu et al. 2011; Squicciarini et al. 2009; Wishart et al. 2010]. However, some of these approaches require too much human intervention during conflict resolution: [Wishart et al. 2010] require users to solve the conflicts manually and [Squicciarini et al. 2009] do so nearly manually, e.g., by participating in difficult-to-comprehend auctions with fake money for every possible conflict. Approaches that provide automation [Carminati and Ferrari 2011; Hu et al. 2011; Thomas et al. 2010] help resolve multiuser conflicts, but they consider only one fixed way of aggregating user preferences, without considering how users would compromise and the concessions they might be willing to make in a specific situation. [Hu et al. 2013] consider more than one way of aggregating user preferences, but the user that uploads the item chooses the aggregation method to be applied, which becomes a unilateral decision without considering any input from others. Clearly, solutions that do not consider input from all users involved may lead to solutions that are far from what some users would be willing to accept. In essence, current automated mechanisms do not readily adapt to different situations that may motivate users’ concessions, which has the potential to cause these mechanisms to suggest solutions that may not be acceptable to all concerned. This leads users to manually resolve conflicts most of the times. [Such and Criado 2014; Such and Criado 2015] provide an improvement over the fixed ways of aggregating user preferences by suggesting three, but only three, methods to be selected depending on the situation.

Some recent works, e.g., [Hu et al. 2014; Such and Rovatsos 2015], propose game-theoretic mechanisms to tackle multiuser privacy conflicts. These proposals provide formal frameworks based on established concepts such as Nash equilibrium. However, [Hu et al. 2014] show, such proposals may not work well in practice since they may not capture the social idiosyncrasies that users consider in real life [Lampinen et al. 2011; Wisniewski et al. 2012].

[Ilia et al. 2015] present a mechanism to enforce fine-grained access control in photos by blurring the faces of the users depicted in the photo based on each users’ access control list. This approach can limit the utility of sharing information. However, used in conjunction with a decision-support mechanism based our findings, Ilia et al.’s approach could enforce access control differently for different users in case they cannot agree on a sharing policy.

Arguments are used to resolve conflicts in other domains. [Murukannaiah et al. 2015] employ arguments to resolve conflicts in stakeholders’ goals during requirements elicitation. Their findings that arguments lead to consistent responses aligns with our observation. [Williams and Williamson 2006] incorporate arguments and Bayesian networks for breast cancer prognosis, where they exploit arguments to develop an explanation for the prognosis. A similar application in the privacy domain can be to explain to a user, via arguments, the consequences of a particular sharing decision.

8. CONCLUSIONS
Sharing all kinds of information on SNSs is routine for many people. Examples of such information are a photo from the Christmas party and a tweet about your imminent trip with friends. The shared information often involves multiple users. Tagging people is valuable except when it poses a threat to their privacy.

When the privacy preferences of two or more users do not align, they can negotiate to balance privacy and utility for each user. Related literature proposes methods based on aggregating privacy preferences. However, aggregation does not capture how people align with others’ preferences. In contrast, we propose employing arguments to support preferences. We present a model for multiuser privacy scenarios that employs three types of features: contextual, preferences, and arguments. Via a series of multiple linear regression models, we show that all three feature types influence the optimal sharing policy. Moreover, we present an inference model that, given a multiuser privacy scenario defined by its features, predicts the optimal sharing policy with up to 86% accuracy.
REFERENCES


Hongxin Hu, Gail-Joon Ahn, and Jan Jorgensen. 2013. Multiparty Access Control for Online Social Networks: Model and Mechanisms. IEEE Transactions on Knowledge and Data Engineering 25, 7 (July 2013), 1614–1627. DOI: http://dx.doi.org/10.1109/TKDE.2012.97


