Privacy as a Planned Behavior: Effects of Situational Factors on Privacy Perceptions and Plans

A K M Nuhil Mehdy
Computer Science Department, Boise State University
Boise, ID, USA
akmnuhilmehdy@u.boisestate.edu

Michael D. Ekstrand
People & Info. Research Team, Boise State University
Boise, ID, USA
michaelekstrand@boisestate.edu

Bart P. Knijnenburg
School of Computing, Clemson University
Clemson, SC, USA
bartk@clemson.edu

Hoda Mehrpouyan
Computer Science Department, Boise State University
Boise, ID, USA
hodamehrpouyan@boisestate.edu

ABSTRACT

To account for privacy perceptions and preferences in user models and develop personalized privacy systems, we need to understand how users make privacy decisions in various contexts. Existing studies of privacy perceptions and behavior focus on overall tendencies toward privacy, but few have examined the context-specific factors in privacy decision making. We conducted a survey on Mechanical Turk (N=401) based on the theory of planned behavior (TPB) to measure the way users' perceptions of privacy factors and intent to disclose information are affected by three situational factors embodied hypothetical scenarios: information type, recipients' role, and trust source. Results showed a positive relationship between subjective norms and perceived behavioral control, and between each of these and situational privacy attitude; all three constructs are significantly positively associated with intent to disclose. These findings also suggest that, situational factors predict participants' privacy decisions through their influence on the TPB constructs.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**.

KEYWORDS

privacy, decision making, behavior modeling, situational factors

ACM Reference Format:
A K M Nuhil Mehdy, Michael D. Ekstrand, Bart P. Knijnenburg, and Hoda Mehrpouyan. 2021. Privacy as a Planned Behavior: Effects of Situational Factors on Privacy Perceptions and Plans. In *Proceedings of the 29th ACM Conference on User Modeling, Adaptation and Personalization (UMAP '21), June 21–25, 2021, Utrecht, Netherlands.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3450613.3456829

UMAP '21, June 21–25, 2021, Utrecht, Netherlands

ACM ISBN 978-1-4503-8366-0/21/06…$15.00
https://doi.org/10.1145/3450613.3456829

1 INTRODUCTION

Users' decision to share their personal information, and the perceptions of risk that inform this decision, vary from situation to situation. Situations consist of various factors such as the information type, recipient of the information, and the trust source behind the motivation for sharing. Past research has not paid much attention to how these factors can be used to model and predict users' contextual privacy concerns and decisions. This is an important shortcoming, as decision research suggests that users' privacy preferences are malleable rather than stable and that privacy behavior may vary based on situational and contextual factors [18, 20, 39]. Moreover, individual's privacy expectations depend on the contexts in which the user is sharing information [19, 29, 30, 35].

In order to understand, model, and possibly predict human privacy behavior in various situated environments, there have been several factors and parameters documented to influence users in their privacy decisions. The theory of planned behavior (TPB) [3], an extension of the theory of reasoned action [41], is a behavioral theory that helps modeling users' perceptions and plans. However, most privacy research based on this theory have either studied single situations, or have considered a very limited set of situational factors [16, 37]. As a result, understanding the characteristics and impact of various situational factors on users' privacy decision is still an active area of research.

In this work, we study users' situational privacy decisions, through a scenario-based survey with 401 participants, each responding to several of 48 different scenarios. Each data point consists of responses to a set of questionnaires that measure participants' attitudinal evaluations of each scenario as well as their perceptions and intention to disclose private information under the specified situation. Alongside the scenario-specific questions, participants responded to a set of general attitude questions to elicit their general attitude towards information disclosure. We perform a path analysis to model participants' privacy perceptions and plans, taking into consideration their attitudinal evaluations on *subjective norm*, *perceived behavioral control*, and *attitude* by manipulating three situational factors: information type, recipient role, and trust source. The results from the analysis reveals how users make privacy decisions in various situations, and how the situational factors have significant effects on users' perceptions of privacy factors and intention to disclose potentially private information. This paper

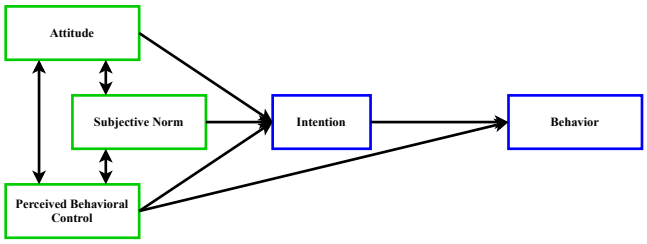

Figure 1: Theory of planned behavior and its core components[3].

is the first to our knowledge to combine the Theory of Planned Behavior with a contextual approach to privacy modeling. This study also contributes several insights to the area of user-tailored privacy modeling and personalized privacy systems[20], through the following research questions:

(1) How do users' subjective perceptions of TBP constructs differ in different informational situations?
(2) How do situational perceptions affect users' intent to disclose information?
(3) How do users' situational perceptions and intents relate to their general privacy attitudes?

2 BACKGROUND AND RELATED WORK

Since our path model is based on the theory of planned behavior, we first briefly introduce this behavioral theory in this section. In the following subsections, we review the related research that uses this theory to model users' privacy decision-making process. We also briefly review research that models users' contextual privacy decisions.

2.1 Theory of Planned Behavior (TPB)

According to the TPB, people's behavior is directly determined by their behavioral *intentions*, which are in turn influenced by their *attitude*, perception of the *subjective norms*, and *perceived behavioral control*. Also, the *perceived behavioural control* can, together with *intention*, be used to explain the actual *behavior*. In the literature [7, 16] these constructs are defined as follows:

- Attitude (A) is defined by the positive or negative evaluation of the decision (e.g., how well the participant understands the value of an action).
- Subjective norm (SN) is defined as a culturally appropriate and desired behavior that is generally expected of a person with in his/her social group (e.g., how a participant's closest relatives act on similar situation).
- Perceived behavioral control (PBC) is defined by the perceived ease or difficulty that the individual addresses to perform the behavior.

The theory states that these constructs or components together shape an individual's behavioral intentions. Thus, it provides a model to capture humans' behavioral intention (Figure 1). Theory of planned behavior is used in many research areas and has demonstrated its effectiveness in predicting human behavior in various fields such as privacy[16, 42], use of the internet [44], health [12], environmental psychology [28], etc.

2.2 Modeling Users' Privacy Decisions Using TPB

In spite of the dynamic nature of privacy behavior [18, 39] and the fact that privacy paradox shows that users' intentions and attitudes may not always result in privacy-protective behaviors [2], studies have used the TPB to investigate and model the most important factors that influence users' privacy decision-making process [3]. Heirman et. al. [16] analyzed the impact of the TPB factors (i.e., attitude, subjective norm, perceived behavioral control) on the disclosure of private information through a structured survey. A similar TPB-based approach was utilized by Saeri et. al. to investigate Facebook users' privacy protection tendency based on descriptive norms, risk, and trust [37]. Yao et. al. extended the TPB to model users' intention to adopt an online privacy protection strategy [44]. Their analysis showed that "the intention to adopt online privacy self-protection is a function of one's attitude towards protective strategies, the subjective norm of adoption, and the perception of behavioral control". Lwin et. al. combined Laufer and Wolfe's multidimensional approach to privacy [25], and an extended version of Ajzen's theory of planned behavior [3] to study the privacy behavior of online users Lwin and Williams [27]. They partially used a TPB inspired conceptual framework to investigate the reasons behind users' intention to disguise their identities (i.e., private information). While TPB is normally used for grounding designs and analyses related to any type of human behavior towards an action [42], researchers have successfully used TPB for in-depth analysis of privacy attitudes and privacy behavior [8, 11, 17] with ample justifications [13].

All of the above-mentioned works have one common limitation: they assumed the users' privacy perceptions (TPB construct measures) to be stable and did not take into account the potential impact of contextual factors. The way contextual dimensions influence TPB remains underexplored.

2.3 Modeling Users' Contextual Privacy Decisions

Many researchers have studied modeling users' decision-making process in the context of various types and recipients of the information. Knijnenburg and Kobsa [21], while exploring the design parameters of social network site's privacy-settings UI (user interfaces), discovered about how the type of information and their specific recipients have significant effect on user's sharing tendency. In their study participants were asked to set their privacy settings on a custom made privacy settings UI of an imagined Facebook-like social network site by indicating which of their profile information they would share with whom. At the end of the study, they measured the users' interpersonal privacy concerns using a post-experimental questionnaire. In another user study, Knijnenburg et al. [22] validated the primitive idea of users' privacy calculus (i.e., costs vs benefits which measures the benefits of privacy allowances and the resulting costs [14]) and how it led them to disclose different types of information to different types of websites in a purpose-specific manner. They found that the perceived risk and perceived

relevance of the disclosure depends on the interaction between the type of the information and the type of the website/recipient, and that this perceived risk and relevance decreases and increases disclosure, respectively. While both studies show how the perceived relevance and risk of the information—as well as the disclosure activity or intention—depend on the type and recipient of the information, neither of these studies takes into consideration the impact of ephemeral situations (i.e., scenarios or contexts) on the participants' behavior.

In a contextual setup, Lederer et al. [26] investigated the relative effects of information recipient and the situation towards information disclosure. They conducted a study with 130 participants by providing them with two hypothetical situations (working lunch, social evening) and four inquirers/recipients (spouse, employer, stranger, merchant). They asked each participants to imagine using a mobile phone which is capable of collecting and sharing profile and location information to the requesting parties. Through a web based questionnaire they analyzed the user's preferences and found that "identity of the information inquirer is a stronger determinant of privacy preferences than is the situation in which the information is collected". However, they found that the situation is also an important determinant but only when the information inquirer is an employer. Even though they incorporated scenarios and recipients' role in the study, the characteristics of the scenarios were unchanged and represents only two static situations. In this regard, their contextual behavior analysis is limited to these two situations only. Nevertheless, the above-mentioned work and other similar works have demonstrated the influence of various contextual factors on users' privacy behavior [33, 34].

2.4 Representing Contexts with Scenarios

One way of contextualizing a survey is to introduce various scenarios to the participants and ask them to respond to questionnaires linked to each of those scenarios [26]. However, one challenge in this regard is to create proper scenarios with an appropriate level of detail. Researchers from the area of scenario-based survey have introduced many different approaches to create hypothetical scenarios using text, graphics, games, app interfaces, etc. [15, 24, 43, 45]. Among all of these, text-based scenarios are preferred in case of surveying the participants. A set of methods have been well-established for the development of such scenarios, especially in the privacy survey domain, such as the factorial method, storytelling method, and claim analysis. The factorial method involves creating scenarios "based on a set of predefined factors that describe all or a subset of possible combinations seen in a situation or decision problem" [9]. These factors could be socioeconomic, behavioural, or clinical issues, defined as categorical variables with two or more levels. However, the number of factors and their levels are subject to be decided carefully. Otherwise, the number of combinations of factor categories increases very rapidly, which in turn increases the total number of unique scenarios. On the other hand, the storytelling method suggests creating a few illustrative scenarios, usually based on the experience of the members of the research team. In our work, we adopt the former method to create the scenarios while keeping the number of factors and their categories low.

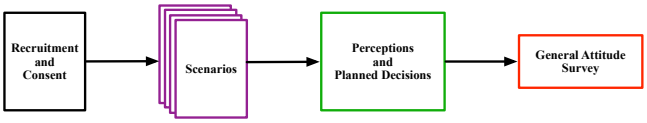

Figure 2: Overview of the experimental flow.

3 SURVEY METHODOLOGY

The overall flow of our experiment can be divided into three main steps: i) recruitment and consent ii) capturing scenario-specific perceptions and planned decisions iii) general attitude survey (Figure 2). After consenting to the study, a participant is assigned a set of 8 random hypothetical scenarios and asked to respond to those scenarios one after another. Each scenario gives the participant a situation in which he/she must decide whether or not to share a piece of information. This incorporates the situational factors on which participants might have a degree of reliance for their perception and decision towards disclosure intention (see Section 3.1). A participant has to read a given scenario and respond to all of the corresponding questions before proceeding to the next assigned scenario.

In the next step, the participant takes a short survey to capture their general privacy attitudes independent of any particular scenario. This step is designed to capture such perceptions that are assumed to be stable over time and do not usually change based on any situation. There is another final step for collecting the demographic information of the participants, in which participants are asked to optionally input their gender, age group, country of residence, and the duration of residence in that country. It is worth mentioning that the presented scenarios are hypothetical; none of the participants' personally identifiable information is collected in any step of the survey, explicitly or implicitly.

3.1 Factor Manipulation

We manipulate 3 situational factors in order to measure their effect on participant response:

Information Type (IT) The general category information that may be disclosed. Each scenario is about one of three categories: health, finance, or relationship.

Recipient's Role (RR) The kind of recipient the information may be disclosed to, with their relationship to the participant. We use four roles: family, friend, colleague, and online (e.g. discussion forum).

Trust Source (TS) Where the idea of disclosing this information to this recipient came from. We test four trust sources: family, friend, expert (e.g. physician or financial adviser), and online (e.g. searching the web).

This choice of factors is partly inspired from the theory of contextual integrity (CI) [6, 32]. The CI theory provides the ground of informational norm where, norm is formulated as a tuple of access permission (ρ, τ), environmental conditions (ψ), and transmission principle (η). Hence, a norm, n is represented as: $n = ((\rho, \tau), \psi, \eta)$ where, n = Informational norm, ρ = Recipient's Role, τ = Information type, η = Transmission principle. These factors yield a total of 48 (3*4*4) unique situations. Every situation and the associated

questionnaire is intended to measure the situational privacy perceptions of the participant through 3 constructs: i) attitude ii) subjective norm iii) perceived behavioral control

3.2 Scenario Generation

For each combination of situational factors, we wrote a scenario in which a trust source encourages the participant to share information with a recipient. To minimize extraneous variability, we made each scenario as similar as possible while presenting the combination of factors in a natural and coherent manner. As an example, the scenario for *health* as information type, *friend* as trust source, and *family member* as recipient's role is:

> Your doctor called and told you that your lab results came back positive for a disease. One of your friends suggested discussing the situation with a family member and asking their support, saying it could be helpful.

Changing the trust source from friend to family and recipient's role from family to online yields another scenario:

> Your doctor called and told you that your lab results came back positive for a disease. A family member suggested asking other patients and doctors on an online discussion forum, saying they have found it helpful for dealing with their similar condition.

In this study, the domains of the scenarios are health, finance, and relationship. This means, we have generated 3 sets of scenarios for these three types of information. Each of these sets contains 16 different scenarios (i.e., 4 RR x 4 TS values) resulting in a total of 48 scenarios. For each scenario, the participants answered a set of questions to measure their perception of TPB constructs in that scenario and indicated whether or not they would share the information.

3.3 Scenario Randomization

As discussed earlier, every participant is assigned a set of 8 random scenarios with associated questionnaires. To ensure a minimum level of variability within each user's situations (and therefore responses), we used rejection sampling to require that each user's 8 scenarios covered all 11 distinct factor levels at least once. Redrawing a fresh, independent set of 8 scenarios if a user's initial assignment excludes a level ensures maximal statistical independence subject to our inclusion requirement. We further randomly order scenarios for each participant to avoid order effects. Also, we implicitly account for the variability of judgements of the questions and scales across the participants by setting random per-user intercepts while doing the analysis.

3.4 Testing the Experiment

We piloted the experiment and surveys with 6 colleagues from our research lab. Their feedback helped fix issues in the survey application, user-experience/user-interface, and clarity of the scenarios and questions. We then soft-launched the survey on Amazon Mechanical Turk with an initial round of 10 participants to collect information on the average time needed to complete the survey and estimate total survey cost.

3.5 Participants

We recruited the participants for the final survey via Amazon Mechanical Turk, an online crowd-sourcing marketplace. We filtered for Workers from the USA with a good reputation (i.e., at least 95% HIT approval rate and 50 hits approved) who are at least 18 years old. We paid $2.00 per survey based on pilot trials indicating Turkers could complete it in about 15 minutes.

3.6 Data Collection and Cleaning

We employed a number of filters to ensure the quality of the data. First of all, we capture the time a participant spent on each scenario step and removed the data points (i.e., responses associated with a specific scenario) from our analysis if the spent time was too low (less than 15 seconds per scenario) to be realistic. Secondly, we embedded attention check questions randomly in between survey questions on two surveys per participant, and removed 9 data points for failing the attention check. Since participation is anonymous and therefore a participant could potentially submit several responses, we restricted this incident by setting a browser cookie for 3 days after a successful submission.

We converted the 5-point scale responses to TPB questions (ranging from *Strongly Disagree* to *Strongly Agree*) into a numeric format (1 to 5). We represent the *Share* and *Not Share* options for the final decision question in logical numeric form, 1 and 0. We dummy-coded categorical variables for the situational factors. We then computed a standardized scale-score for each TPB construct by taking the mean of the responses on its questions (see Section 4.2), after inverting negative questions, so that 5 represents the opinion most in favor of sharing for each question.

4 TPB-BASED QUESTIONNAIRE AND PATH MODEL

As previewed in Section 2.1, we designed our survey to measure participants' behavioral intention and their situational perception of three constructs from TBP: attitude (A), subjective norm (SN), and perceived behavioral control (PBC). We followed the scenario-specific questionnaires with a short survey to assess participants' general attitude towards privacy. We integrated the TPB constructs, manipulated factors, and general privacy attitude into an initial path model shown in Figure 3. The colors on the figure follow the convention of Knijnenburg et al.'s evaluation framework [23], where purple = manipulations, green = subjective evaluations, red = personal characteristics, and blue = behavior. We evaluate this path model through a causal modeling technique called *path analysis* to determine if our causal model fits the survey data well. Note that path analysis is "not intended to discover causes but to shed light on the tenability of the causal models that a researcher formulates" [36]. We apply this technique to examine the relationships between the observed variables in terms of the strength and direction of the path beta coefficients.

4.1 Model Specification

The dummy variables representing the three scenario parameters—information type, recipient's role, and trust source—comprised the *exogenous* variables(variables that have arrows outbound from them

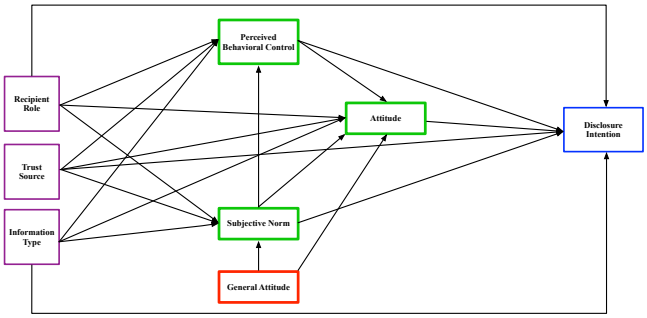

Figure 3: The initial path model.

and not caused by any other variables of the model [40]) in the preliminary path model, together with general attitude. Trust source was eliminated from the final model because of its non-significant association with the TPB constructs. In our initial model the exogenous variables were causally related to attitude, perceived behavioral control, and subjective norm, although some of these relations (e.g. from information type to perceived behavioral control) were removed due to a lack of significance. Relationships among attitude, perceived behavioral control, and subjective norm were also modeled. Finally, all variables were causally related to disclosure intention, although only attitude, perceived behavioral control, and subjective norm were found to be significant. The final model has a total of 27 free parameters, and 28 fixed parameters whose values are estimated from the data.

We fit the model with Mplus, a statistical analysis tool for conducting the analysis as well as constructing the diagram of our path model [31].

4.2 Questionnaire

The survey contains two sets of questions - *i) scenario specific questions (12 in total) ii) general attitude questions (4 in total).* The first set of 12 questions are repeated for each of the 8 assigned scenarios to each participant. The second set of questions are presented at the last step of the survey. The scenario-specific questionnaire is inspired by Heirman et al. [16], which operationalized the constructs in the theory of planned behavior [3]. The second set of questions is inspired by prominent privacy research [1, 10].

The following questions were asked once per scenario:

(1) *Attitude (Cronbach's alpha: 0.68)*
   (a) I would benefit from sharing this situation. (Scale: Completely disagree (1) to Completely agree (5))
   (b) I am concerned about where this information would be stored or recorded if I shared it with *$recipient.* (1-5, reversed)
   (c) I do not expect any significant risks if I share this situation. (1-5)
   (d) I have concerns about who will learn about this situation. (1-5, reversed)

(2) *Subjective Norm (Cronbach's alpha: 0.79)*
   (a) I think my friends or family would share in this situation. (1-5)
   (b) A friend or family member would likely suggest that I disclose this situation. (1-5)
   (c) My friends would approve of me disclosing this situation. (1-5)
   (d) Some people in my life would disapprove if they knew I shared this situation. (1-5, removed from the scale)

(3) *Perceived Behavioral Control (Cronbach's alpha: 0.66)*
   (a) I have control over how my information will be used after I share it in this situation. (1-5)
   (b) I trust the recipient of my information to honor my wishes if I ask them to keep my situation a secret. (1-5, removed)
   (c) Sharing this situation would put me at risk. (1-5)

(4) *Disclosure Intention*
   (a) What would you do in this scenario? (Scale: Not share (0) or Share (1))

The following questions were asked once per participant:

(1) *General Attitude (Cronbach's alpha: 0.68)*
   (a) In general, I am concerned about threats to my personal privacy. (1-5, reversed)
   (b) I am generally concerned about my privacy while using the internet. (1-5, reversed)
   (c) I believe other people are too concerned about online privacy issues. (1-5, removed)
   (d) I think I am more sensitive than others about the way my contacts handle information I consider private. (1-5, reversed)

We performed Cronbach's alpha test to measure the items' scale reliability. Thus, item (d) was removed from the subjective norm scale because of its negative effect on the alpha score. We removed item (c) from perceived behavioral control, and item (c) from general attitude because of the same reason. Items (b) and (d) in the attitude scale were reversed while calculating their score because of their negative phrasing. All items in the general attitude scale were reversed to align this factor with the context-specific attitude.

5 RESULTS

This section describes the path analysis results in detail. First we talk about the descriptive analysis and the quality of the model fit. Then we describe the direct and indirect effects of the factors and constructs in subsequent sections. Figure 4 depicts our final path model.

5.1 Descriptive Statistics

Table 1 reports the demographic information of the participants. We share this information not because these are relevant factors in this context but for those who may attempt to reproduce this results with a similar setup. Figure 5 reports the differences in attitude, subjective norm, perceived behavioral control, and disclosure intention between the different value of the scenario parameters "information type" and "recipient role", including standard error bars. For example, we can see how the participants perceive a higher level of behavioral control when the recipient is family member or friend than that of colleague or online platforms.

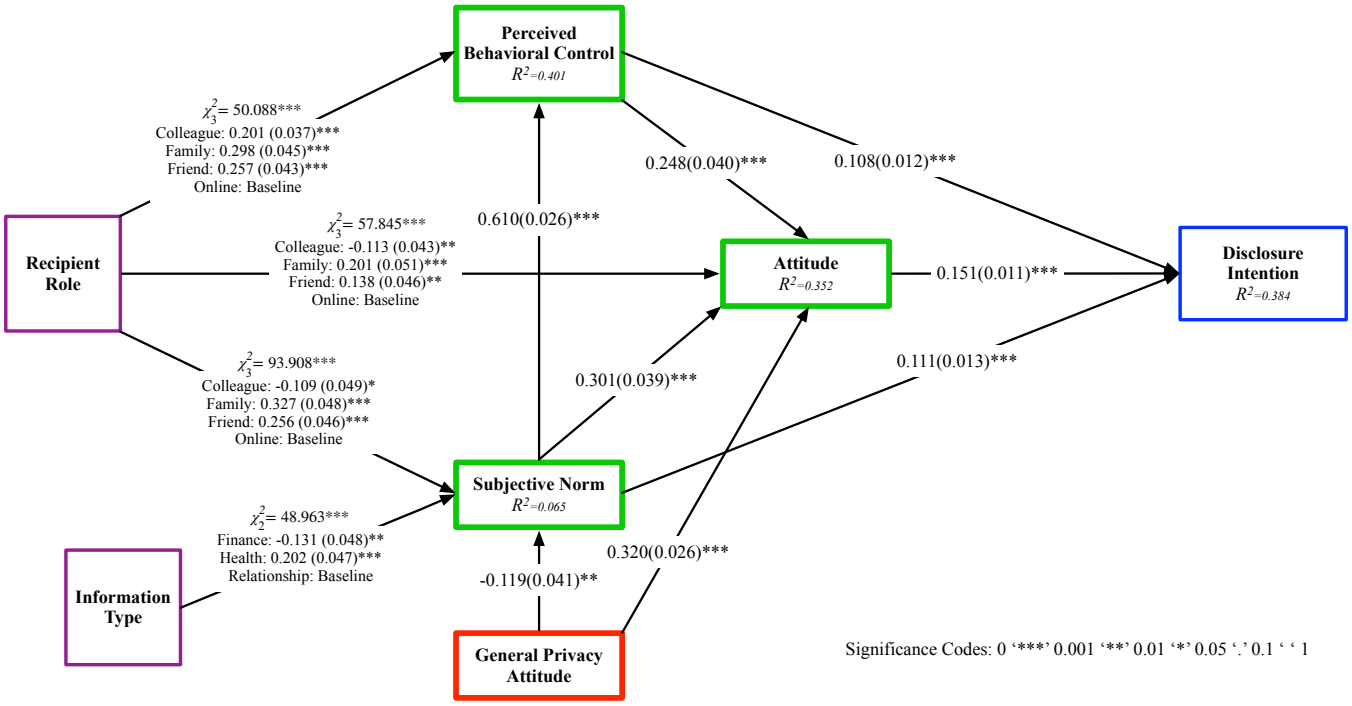

Figure 4: Path model results. Paths that are non-significant ($p > .05$) are removed from the model.

Table 1: Demographic information of the participants.

Constructs	Distribution
Gender	Man: 252
	Woman: 144
	Not Answered: 3
	Non Binary: 1
	Woman,Man: 1
Age	18-30: 108
	31-40: 148
	41-50: 75
	51-60: 49
	60+: 19
	Not Answered: 2

5.2 Model Fit

Figure 4 depicts the final results of the path model analysis in detail. The model fits the data very well with $\chi^2_{11} = 12.017$, $p = 0.3623$, $CFI = 1.0$, $TLI = 0.99$, $SRMR = 0.008$, $RMSEA = 0.005$, 90% $CI = 0.000$ to 0.020. A non-significant χ^2 value ($p > .05$) is indicative of a path model that fits the data well [38]. Also, the comparative fit index (CFI) and Tucker-Lewis index (TLI) values which ranges from 0 to 1 show near-perfect scores. Moreover, the relationships in the model explain 38.4% ($R^2 = 0.384$) of the variance in disclosure intention, 35.2% of the variance in attitude, 6.5% of the variance in subjective norm, and 40.1% of the variance in perceived behavioral control.

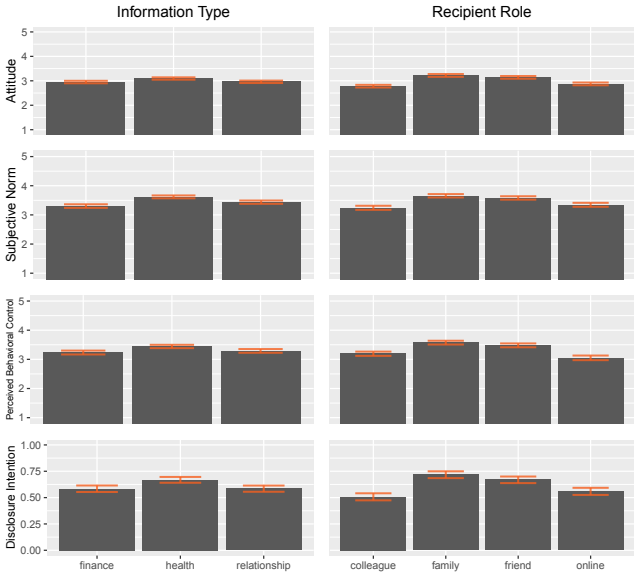

Figure 5: Constructs vs Mean Scale-score based on Information Type and Recipient's Role.

5.3 Effect of the Scenario Parameters on TPB Constructs

This section describes the significant effects of the scenario parameters (recipient role and information type) on the TPB constructs (the privacy perceptions of the user). These effects are measured by

the paths from the purple (square) boxes to the green (rectangular) ones in Figure 4.

(1) The recipient's role in the scenario has a significant influence on perception of behavioral control. Compared to "people online", participants are estimated to perceive significantly more control when the recipient is a colleague (0.201 SD higher), a family member (0.298 SD higher) or a friend (0.257 SD higher).
(2) Likewise, the recipient's role in the scenario has a significant influence on attitude. Compared to "people online", people are estimated to have significantly more positive attitude toward disclosure when the recipient is a family member (0.201 SD higher) or a friend (0.138 SD higher), but more negative attitude when the recipient is a colleague (0.113 SD lower).
(3) The recipient's role in the scenario has a significant influence on subjective norm. Compared to "people online", participants are estimated to believe that individuals close to them would be more likely to agree with the scenario when the recipient is a family member (0.327 SD higher) or a friend (0.256 SD higher), but less when the recipient is a colleague (0.109 SD lower).
(4) The information type in the scenario has a significant influence on subjective norm. Compared to "relationship information", participants are estimated to believe that individuals close to them would be more likely to agree with the scenario when the information type is health (0.202 SD higher) but less reliance when the information type is finance (0.131 SD lower).

5.4 Effects between General Attitude and Situational Perceptions

We now turn to the relationships between constructs, both situational TPB constructs and the influence of general attitude on these constructs. The following effects refer to the paths among the green (rectangular) boxes and between the red (rectangular) box and the green ones in Figure 4.

(1) The participants' perceived subjective norm regarding the scenario is positively associated with their perception of behavioral control. A 1 SD difference in subjective norm results in an estimated 0.610 SD difference in perceived behavioral control.
(2) Participants' subjective norm is also positively associated with their attitude towards disclosure. A 1 SD difference in subjective norm results in an estimated 0.301 SD difference in attitude.
(3) The perception of behavioral control of the participants regarding the scenario is positively associated with their attitude towards disclosure. A 1 SD difference in perceived behavioral control results in an estimated 0.248 SD difference in attitude.
(4) The participants' general attitude is positively associated with their situational attitude towards disclosure. A 1 SD difference in general attitude results in an estimated 0.320 SD difference in attitude.
(5) General attitude is also negatively associated with perceived situational subjective norm. A 1 SD difference in general attitude results in an estimated -0.119 SD difference in perceived subjective norm.

5.5 Effects of Situational Perceptions on Disclosure Intention

This section briefly describes about the significant effects between the situational TPB constructs (the privacy perceptions of the user) and users' disclosure intention. The following effects refer to the paths between the green (rectangular) boxes and the blue (rectangular) one in Figure 4.

(1) Participants who perceived a higher level of behavioral control were more likely to engage in the disclosure described in the scenario. Particularly, the odds of disclosure of participants who have a 1 SD higher level of perceived behavioral control are estimated to be 11.4% higher.
(2) Participants who have a higher level of perceived subjective norm were more likely to engage in the disclosure described in the scenario. Particularly, the odds of disclosure of participants who have a 1 SD higher level of perceived subjective norm are estimated to be 11.7% higher.
(3) Participants who have a more positive attitude were more likely to engage in the disclosure described in the scenario. Particularly, the odds of disclosure of participants who have a 1 SD higher level of attitude are estimated to be 16.2% higher.

Although not directly comparable, it's worth mentioning a comparison with the results from [16] in this section while showing the relationships between the TPB constructs and disclosure intention. According to their analyses which take into account only the stable factors, an individual's intent to disclose is influenced primarily by a subjective norm and subsequently by attitude, not significantly by perceived behavior control. In contrast, our study shows the order of significant influence of the TPB constructs to disclosure intention as, attitude > subjective norm > perceived behavioral control. It should be noted that in our study, the TPB constructs are already affected by the situational factors.

5.6 Total Effects of the Scenario Parameter on Disclosure Intention

All effects of scenario parameters on disclosure intention were fully mediated by perception of TPB constructs—that is, after controlling for scenario effects through TPB constructs, there were no statistically significant residual effects of scenario parameters on disclosure intention. This section describes the total significant (indirect) effects of the scenario parameters on the users' disclosure intention. The following effects do not refer to any direct paths between the purple (square) boxes and the blue (rectangular) one in Figure 4. Rather, they refer to the paths from the leftmost boxes to the rightmost box via the mediator rectangular boxes in between. These total effects describe *how* users' intention changes from one scenario to another; the mediating TBP factors provide an explanation for *why*. The latter may help with future generalizability.

(1) With regard to the recipient's role in the scenario, compared to the recipient "people online", the odds of disclosure were estimated to be 16.6% higher when the recipient was a family member and 12.9% higher when the recipient was a friend. Both of these differences were significant ($p = 0.000$ and $p = 0.000$, respectively). There was no significant difference between the recipient "people online" and a colleague.
(2) With regard to the type of information, compared to relationship information, the odds of disclosure were estimated to be 3.1% lower when the scenario involved financial information and recipient was a family member and 5.1% higher when the scenario involved health information. Both of these differences were significant ($p = 0.007$ and $p = 0.000$, respectively).

6 DISCUSSION

The results from our path analysis show how users make privacy decisions in various situations: the situational factors have significant effects on users' perceptions of privacy factors, which in turn have an effect on their intention to disclose their private information. Unlike most existing studies of privacy perceptions and behavior modeling, we developed a set of unique scenarios by manipulating parameters to imitate various situations and used a TPB-based model to introduce mediating factors that explain the effects of these situational factors on participants' disclosure intentions. This situation-specific extension of the TPB fulfils our initial goal of understanding users' contextual privacy decision-making process.

This study reveals that the recipient's role in the scenario has a significant influence on peoples' perception of behavioral control, their attitude, and subjective norm (RQ1). People are estimated to perceive a higher level of behavioral control when the recipient is a family member, a friend, or a colleague than when the recipient is people online (e.g., social media, forum etc.). Likewise, people are estimated to have a more positive attitude toward disclosure when the recipient is a family member or a friend than people online, but a less positive attitude when the recipient is a colleague. Users' subjective norm also shows similar order of perceptions. As a result of these effects, people are more likely to disclose their information to friends and family than to colleagues or people online.

The information type in the scenario also has significant influence on participants' subjective norm. The model shows that people believe that individuals close to them would be most likely to agree with the scenario when it involves health information, followed by relationship information, and finally financial information. These differences propagate to small differences in disclosure intentions as well.

The results from the analysis also show that participants' perceived subjective norm regarding the scenario is positively associated with their perception of behavioral control and attitude towards intention to disclose (RQ2). In other words, one can make a hypotheses that when users perceive an expectation to share, they also expect that sharing to be respected? Likewise, their perception of behavioral control is a good predictor of their attitude. Moreover, from the results, we can see the positive effects of these three constructs on users' disclosure intention. Users' attitude has the strongest effects on their disclosure intention relative to the other two constructs. Participants with a higher level of positive attitude were more likely to engage in the disclosure described in the scenario. Section 5.5 contains specific detail of these effects. Additionally, our results reveal the significant influence of general attitude on some TPB constructs (RQ3). Participants' general attitude is positively associated with their situational attitude towards disclosure. In contrast, general attitude is negatively associated with perceived situational subjective norm.

Most importantly, our study demonstrates that the effects of the contextual parameters (the recipient's role and information type) on the users' disclosure intention was fully mediated by participants' attitude, subjective norm, and perceived behavioral control. As such, these TPB constructs serve as significant and sufficient mediators explaining why users disclose more information in some scenarios than in others. These findings contribute important insights to the area of user-tailored privacy modeling and personalized privacy systems by providing a quantitative analysis of the privacy decision making factors.

6.1 Limitations

Even though path analysis is often referred to as a causal inference technique[5], readers should be advised that this model reveals the predictive properties between the factors and constructs. These properties are measured in terms of path coefficients. Therefore, our path analysis shows how the hypothesized model fits the survey data which in turns aims to explain users' privacy decision making process. We also acknowledge that we are only manipulating a few levels per factor in our study, and there could be much more granularity in the information type, recipient's role, and trust source factor; future work should explore this. Additionally, since the results reveal significant relationships between situational factors and disclosure intention, we feel the necessity to integrate additional factors in future studies.

We also note that our scenarios had a hypothetical nature, and hence did not measure actual disclosure but rather users' *intention* to disclose their private information. This is a limitation that our work shares with many other privacy studies [44], especially in light of the "privacy paradox" which shows a discrepancy between disclosure intentions and behaviors, as behaviors tend to be influenced by extraneous factors like default settings and choice framing [4]. Arguably, though, the absence of such extraneous influences makes users' disclosure intentions a more honest representation of their privacy preferences.

7 CONCLUSION

In this paper we have presented the results of a scenario-based survey to understand users' *situational* privacy perceptions and disclosure intentions. These results constitute a contextualized understanding of users' privacy behaviors, connected to the Theory of Planned Behavior, and provide new insights that can help build future user-tailored privacy models. The impact of various situational factors on users' privacy decision is still an active area of research; one particular need is more study of the gap between users' intention versus reported and actual behavior. In future work, we plan to bridge the gap between intention and behavior by incorporating reported or actual behavior in the model. We also plan to evaluate

the predictive power of the current path analysis by surveying a new sample of users. Moreover, we plan to increase the sample size significantly and employ machine learning based algorithms along with the statistical approaches, as a means to compare various analysis methods for explaining contextual privacy behavior. For now, we can advise the user-modeling community to take the recipient and information type into account when modeling users' situation-specific privacy concerns, and to perhaps build these models not as a uni-dimensional construct, but to include aspects of behavioral control, social norms, and attitude, as suggested by the Theory of Planned Behavior.

ACKNOWLEDGMENTS

The authors would like to thank National Science Foundation for its support through the Computer and Information Science and Engineering (CISE) program and Research Initiation Initiative(CRII) grant number 1657774 of the Secure and Trustworthy Cyberspace (SaTC) program: A System for Privacy Management in Ubiquitous Environments.

REFERENCES

[1] Mark S Ackerman, Lorrie Faith Cranor, and Joseph Reagle. 1999. Privacy in e-commerce: examining user scenarios and privacy preferences. In *Proceedings of the 1st ACM conference on Electronic commerce*. 1–8.

[2] Idris Adjerid, Eyal Peer, and Alessandro Acquisti. 2016. Beyond the privacy paradox: Objective versus relative risk in privacy decision making. *Available at SSRN 2765097* (2016).

[3] Icek Ajzen et al. 1991. The theory of planned behavior. *Organizational behavior and human decision processes* 50, 2 (1991), 179–211.

[4] Reza Ghaiumy Anaraky, Bart P Knijnenburg, and Marten Risius. 2020. Exacerbating mindless compliance: The danger of justifications during privacy decision making in the context of Facebook applications. *AIS Transactions on Human-Computer Interaction* 12, 2 (2020), 70–95.

[5] Kheana Barbeau, Kayla Boileau, Fatima Sarr, and Kevin Smith. 2019. Path analysis in Mplus: A tutorial using a conceptual model of psychological and behavioral antecedents of bulimic symptoms in young adults. *The Quantitative Methods for Psychology* 15, 1 (2019), 38–53.

[6] Adam Barth, Anupam Datta, John C Mitchell, and Helen Nissenbaum. 2006. Privacy and contextual integrity: Framework and applications. In *2006 IEEE Symposium on Security and Privacy (S&P'06)*. IEEE, 15–pp.

[7] Lisa Beck and Icek Ajzen. 1991. Predicting dishonest actions using the theory of planned behavior. *Journal of research in personality* 25, 3 (1991), 285–301.

[8] Zakariya Belkhamza, Mohd Niasin, and Adzwin Faris. 2017. The Effect of Privacy Concerns on Smartphone App Purchase in Malaysia: Extending the Theory of Planned Behavior. *International Journal of Interactive Mobile Technologies* 11, 5 (2017).

[9] Paula M Brauer, Rhona M Hanning, Jose F Arocha, Dawna Royall, Richard Goy, Andrew Grant, Linda Dietrich, Roselle Martino, and Julie Horrocks. 2009. Creating case scenarios or vignettes using factorial study design methods. *Journal of advanced nursing* 65, 9 (2009), 1937–1945.

[10] Tom Buchanan, Carina Paine, Adam N Joinson, and Ulf-Dietrich Reips. 2007. Development of measures of online privacy concern and protection for use on the Internet. *Journal of the Association for Information Science and Technology* 58, 2 (2007), 157–165.

[11] Sarah Burns and Lynne Roberts. 2013. Applying the theory of planned behaviour to predicting online safety behaviour. *Crime Prevention and Community Safety* 15, 1 (2013), 48–64.

[12] Mark Conner, Sara FL Kirk, Janet E Cade, and Jennifer H Barrett. 2003. Environmental influences: factors influencing a woman's decision to use dietary supplements. *The Journal of nutrition* 133, 6 (2003), 1978S–1982S.

[13] Tobias Dienlin and Sabine Trepte. 2015. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European journal of social psychology* 45, 3 (2015), 285–297.

[14] Tamara Dinev and Paul Hart. 2006. An extended privacy calculus model for e-commerce transactions. *Information systems research* 17, 1 (2006), 61–80.

[15] Pardis Emami Naeini, Martin Degeling, Lujo Bauer, Richard Chow, Lorrie Faith Cranor, Mohammad Reza Haghighat, and Heather Patterson. 2018. The influence of friends and experts on privacy decision making in iot scenarios. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–26.

[16] Wannes Heirman, Michel Walrave, and Koen Ponnet. 2013. Predicting adolescents' disclosure of personal information in exchange for commercial incentives: An application of an extended theory of planned behavior. *Cyberpsychology, Behavior, and Social Networking* 16, 2 (2013), 81–87.

[17] Shirley S Ho, May O Lwin, Andrew ZH Yee, and Edmund WJ Lee. 2017. Understanding factors associated with Singaporean adolescents' intention to adopt privacy protection behavior using an extended theory of planned behavior. *Cyberpsychology, Behavior, and Social Networking* 20, 9 (2017), 572–579.

[18] Leslie K John, Alessandro Acquisti, and George Loewenstein. 2011. Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of consumer research* 37, 5 (2011), 858–873.

[19] Rezvan Joshaghani, Stacy Black, Elena Sherman, and Hoda Mehrpouyan. 2019. Formal specification and verification of user-centric privacy policies for ubiquitous systems. In *Proceedings of the 23rd International Database Applications & Engineering Symposium*. 1–10.

[20] Bart P Knijnenburg. 2017. Privacy? I Can't Even! making a case for user-tailored privacy. *IEEE Security & Privacy* 15, 4 (2017), 62–67.

[21] Bart Piet Knijnenburg and Alfred Kobsa. 2014. Increasing sharing tendency without reducing satisfaction: finding the best privacy-settings user interface for social networks. (2014).

[22] Bart Piet Knijnenburg, Alfred Kobsa, and Hongxia Jin. 2013. Counteracting the negative effect of form auto-completion on the privacy calculus. (2013).

[23] Bart P Knijnenburg, Martijn C Willemsen, Zeno Gantner, Hakan Soncu, and Chris Newell. 2012. Explaining the user experience of recommender systems. *User Modeling and User-Adapted Interaction* 22, 4 (2012), 441–504.

[24] Priya Kumar, Shalmali Milind Naik, Utkarsha Ramesh Devkar, Marshini Chetty, Tamara L Clegg, and Jessica Vitak. 2017. 'No Telling Passcodes Out Because They're Private' Understanding Children's Mental Models of Privacy and Security Online. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (2017), 1–21.

[25] Robert S Laufer and Maxine Wolfe. 1977. Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of social Issues* 33, 3 (1977), 22–42.

[26] Scott Lederer, Jennifer Mankoff, and Anind K Dey. 2003. Who wants to know what when? privacy preference determinants in ubiquitous computing. In *CHI'03 extended abstracts on Human factors in computing systems*. 724–725.

[27] May O Lwin and Jerome D Williams. 2003. A model integrating the multidimensional developmental theory of privacy and theory of planned behavior to examine fabrication of information online. *Marketing Letters* 14, 4 (2003), 257–272.

[28] Octav-Ionuț Macovei. 2015. Determinants of consumers' pro-environmental behavior–toward an integrated model. *Journal of Danubian Studies and Research* 5, 2 (2015).

[29] AKM Nuhil Mehdy and Hoda Mehrpouyan. 2020. A User-Centric and Sentiment Aware Privacy-Disclosure Detection Framework based on Multi-input Neural Network.. In *PrivateNLP@ WSDM*. 21–26.

[30] Hoda Mehrpouyan, Ion Madrazo Azpiazu, and Maria Soledad Pera. 2017. Measuring personality for automatic elicitation of privacy preferences. In *2017 IEEE Symposium on Privacy-Aware Computing (PAC)*. IEEE, 84–95.

[31] Linda K Muthén and Bengt O Muthén. 1998. Mplus user's guide (Version 7). *Los Angeles, CA: Author* (1998).

[32] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.

[33] Judith S Olson, Jonathan Grudin, and Eric Horvitz. 2005. A study of preferences for sharing and privacy. In *CHI'05 extended abstracts on Human factors in computing systems*. 1985–1988.

[34] Sameer Patil and Jennifer Lai. 2005. Who gets to know what when: configuring privacy permissions in an awareness application. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. 101–110.

[35] Theodore Patkos, Giorgos Flouris, Panagiotis Papadakos, Antonis Bikakis, Pompeu Casanovas, Jorge González-Conejero, Rebeca Varela Figueroa, Anthony Hunter, Guðjón Idir, George Ioannidis, et al. 2015. Privacy-by-norms privacy expectations in online interactions. In *2015 IEEE International Conference on Self-Adaptive and Self-Organizing Systems Workshops*. IEEE, 1–6.

[36] Elazar J Pedhazur. 1997. *Multiple regression in behavioral research: Explanation and prediction*. Wadsworth Publishing Company.

[37] Alexander K Saeri, Claudette Ogilvie, Stephen T La Macchia, Joanne R Smith, and Winnifred R Louis. 2014. Predicting Facebook users' online privacy protection: Risk, trust, norm focus theory, and the theory of planned behavior. *The Journal of social psychology* 154, 4 (2014), 352–369.

[38] Rinal B Shah. 2012. A multivariate analysis technique: Structural equation modeling. *Asian Journal of Multidimensional Research (AJMR)* 1, 4 (2012), 73–81.

[39] Itamar Simonson and Amos Tversky. 1992. Choice in context: Tradeoff contrast and extremeness aversion. *Journal of marketing research* 29, 3 (1992), 281–295.

[40] David L Streiner. 2005. Finding our way: an introduction to path analysis. *The Canadian Journal of Psychiatry* 50, 2 (2005), 115–122.

[41] Robert J Vallerand, Paul Deshaies, Jean-Pierre Cuerrier, Luc G Pelletier, and Claude Mongeau. 1992. Ajzen and Fishbein's theory of reasoned action as applied

to moral behavior: A confirmatory analysis. *Journal of personality and social psychology* 62, 1 (1992), 98.

[42] Paul Van Schaik. 1999. Involving users in the specification of functionality using scenarios and model-based evaluation. *Behaviour & Information Technology* 18, 6 (1999), 455–466.

[43] Primal Wijesekera, Joel Reardon, Irwin Reyes, Lynn Tsai, Jung-Wei Chen, Nathan Good, David Wagner, Konstantin Beznosov, and Serge Egelman. 2018. Contextualizing privacy decisions for better prediction (and protection). In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–13.

[44] Mike Z Yao and Daniel G Linz. 2008. Predicting self-protections of online privacy. *CyberPsychology & Behavior* 11, 5 (2008), 615–617.

[45] Jun Zhao, Ge Wang, Carys Dally, Petr Slovak, Julian Edbrooke-Childs, Max Van Kleek, and Nigel Shadbolt. 2019. I make up a silly name' Understanding Children's Perception of Privacy Risks Online. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–13.