Reciprocity Attacks

Feng Zhu[1] Sandra Carpenter[2] Ajinkya Kulkarni[1] Swapna Kolimi[1]

[1]Department of Computer Science
The University of Alabama in Huntsville
Huntsville, Alabama, USA
{fzhu, ask0004, spk0006@cs.uah.edu}

[2]Department of Psychology
The University of Alabama in Huntsville
Huntsville, Alabama, USA
carpens@uah.edu

ABSTRACT

In mobile and pervasive computing environments, users may easily exchange information via ubiquitously available computers ranging from sensors, embedded processors, wearable and handheld devices, to servers. The unprecedented level of interaction between users and intelligent environments poses unparalleled privacy challenges. We identify a new attack that can be used to acquire users' private information—using reciprocity norms. By mutually exchanging information with users, an attacker may use a psychological method, the norm of reciprocity, to acquire users' private information. We implemented software to provide a rich shopping experience in a mobile and pervasive computing environment and embedded the reciprocity attack. Our experiments showed that participants were more willing to provide some types of private information under reciprocity attacks. To the best of our knowledge, this is the first attempt to understand the impact of the norm of reciprocity as an attack in mobile and pervasive computing environments. These human factors should be taken into consideration when designing security measures to protect people's privacy.

Categories and Subject Descriptors

H.1.2 **[User/Machine Systems]**: Software psychology; D.4.6 **[Security and Protection]**: *Invasive software.*

General Terms

Experimentation, Security, Human Factors

Keywords

Reciprocity; psychology; identity management; security; privacy

1. INTRODUCTION

Information exchange between people and environments becomes unprecedentedly convenient in mobile and pervasive computing environments. Embedded processors, sensors, and servers that saturate intelligent environments provide rich context information and network services to users. Using their handheld and wearable computers, users are also ready to provide their digitized information to the intelligent environments. The increasing convenience in communication and information exchange poses serious privacy and security challenges. While users acquire more services from intelligent environments, they may also provide, knowingly or unknowingly, more private information about themselves. Our goal is to evaluate one of the human factors that impact this exposure of private information.

Identity is an important piece of private information. Theft of personal data and trading personal data without permission are among the top three privacy concerns [1]. According to Newman and McNally's report [2], it is estimated that 10 million people in the United States experience identity theft every year. Meanwhile, service providers frequently collect identity information. According to the Georgetown Study of commercial websites, the common practice is that almost all service providers (more than 90%) collected identity information [3]. Some service providers aggressively collect as many as 100 identity elements from a user [4]. As we are moving towards mobile and pervasive computing environments, identity information collection might reach an all-time high. In this paper, we focus on this important part of privacy—identity information.

Previous studies show that people are very concerned about their identity information, but they may not protect their personal information well and may unnecessarily expose the information [5-6]. A few recent studies [7], including our earlier work [8], suggest that people are less aware of the privacy issues raised by mobile and pervasive computing. While people cannot protect their privacy well under benign circumstances, conditions in which privacy is attacked may cause even more serious problems. Anderson indicated that real attacks exploit psychology at least as much as technology [9]. To the best of our knowledge, our experiment is the first study on psychological attacks in mobile and pervasive computing environments. Our long-term goal is to identify ways to protect users from psychological attacks on identity privacy. In this paper, our contribution to the literature is to show the effectiveness of the reciprocity attack, under varying conditions. These conditions can thereby provide a foundation for future work on how to mitigate the effectiveness of such attacks.

The following is an example of a private information exposure situation. Our experiment used a scenario designed along similar lines. We assume a user called Bob, who has a smartphone with embedded RFID technology to read RFID tags and who also has a Bluetooth headset. While browsing in a bookstore, Bob comes across a poster advertising the latest album released by one of his favorite music artists. Bob notices that the poster has a RFID tag, which can be read to access more information about the new album. Bob uses his smartphone's embedded RFID reader to read the RFID tag on the album poster. The RFID tag on the poster emits a URL, which redirects Bob's smartphone browser to show a map of that particular store. The map gives Bob directions to find the aisle in the store, where the album is physically located to be sold. Bob finds the album, which has its own RFID tag. Bob once again reads the RFID tag on the album, using his smartphone's RFID reader. The URL emitted by the RFID tag on the album, redirects Bob's smartphone browser to a web page which renders a recommendation agent, called Alice. Alice welcomes Bob and lets him know she has more information about the album. Now Bob communicates with Alice, using the microphone and the earphone in his Bluetooth headset. Alice

Symposium On Usable Privacy and Security (SOUPS) 2011, July 20-22, 2011, Pittsburgh, PA, USA.

provides Bob with the information about the album, such as the track list of the album, the album's release time, and editorial reviews from reliable sources. When Bob asks Alice about the album's popularity, Alice provides the information along with suggestions of sample music videos from the tracks of that album. After watching a few sample music videos, if Bob is still interested, he can ask for more information from Alice.

It is well known in psychology that when one person exposes information about himself or herself to another person, the second party is more likely and willing to return the favor and expose his or her information (i.e., reciprocate) [10-11]. As the interaction continues, more sensitive and private information may be exposed and exchanged. This type of "tit-for-tat" exchange is known as the norm of reciprocity. Although people may avoid exposing their private information in most situations, the norm of reciprocity makes it more likely that people will disclose. Further studies show that the norm of reciprocity is so strong that people reciprocate exposures in interactions with computers [12] and strangers [14]. Additional research shows that increasing reciprocity leads to increasing trust [13], and that increasing trust mitigates concerns about privacy [14] and increases vulnerability [13]. Reciprocity has also been intensively studied in economics. For example, an experimental study showed that employers refuse to reduce salaries when the unemployment rate is high and workers underbid for a lower salary [15]. Instead, they pay the normal salary and expect workers to devote proper efforts via reciprocity.

The reciprocity norm underlies most types of social exchange. "Things exchanged may be concretely different but should be equal in value, as defined by the actors in the situation.[16]" Sometimes, identical types of resources are exchanged [16], such as information for information when two people are getting acquainted. In our studies we investigated both of these types of reciprocal exchanges: exchanges for identical types of resources (information for information) and reciprocal exchanges of different types of resources (information for services/goods). Most social exchanges are considered to provide benefits (value) to the respective parties. Using the examples in the previous paragraph: in conversation, sharing information can help to develop a relationship; in business, a salary is expected to elicit appropriate work behaviors from employees. Social exchanges are preferred if they are perceived to be fair and balanced.

We identified that in mobile and pervasive computing environments the norm of reciprocity can be used as a new privacy attack. Attackers may intentionally gather people's private information by using the norm of reciprocity that underlies exchanges as a strategy to elicit identity and other private information, a process that users may not expect in this environment. Moreover, in pervasive computing environments, private information is digitized and may be permanently stored.

This paper demonstrates the effectiveness of the reciprocity attack to acquire one aspect of private information, identity information, which is believed to be essential for accountability, access control [17], and trust [18]. The malicious usage of reciprocity, however, might be used to obtain various types of very personal and sensitive information including emotions and feelings. Bruce Schneier warned us that only amateurs attack machines, whereas professionals target people [9]. It might be much easier for attackers to directly target people's private information in various ways via mobile and pervasive computing than in other environments.

We evaluated the impact of reciprocity attacks on private information disclosure. We developed software with an animated recommendation agent, Alice, and provided a rich CD shopping experience using PDAs. Across several pilot studies and experiments, 167 participants came to our lab to participate in the research. We selected identity elements with different levels of sensitivity, based on our previous study [8], to determine how reciprocity attacks impact the disclosure of various types of private information. Requests for the identity elements were embedded as different types of reciprocity attacks, suggesting exchange of personal information for information, products, or services. Our analysis shows that participants were susceptible to the attacks to different degrees, depending on the type of information requested and the type of reciprocal exchange offered. Over the 6 months of our study, we improved our methodology for conducting privacy studies, identifying problems, and differentiating trust and reciprocity effects.

The rest of the paper is structured as follows. We first discuss related work in the Section 2. We then describe our experimental design, method, software, and participants in Section 3. Next, we present our analysis *and* key findings with respect to the effectiveness of the reciprocity attacks in Section 4. After that, we discuss the lessons that we learned and other findings in Section 5 and limitations of our research are discussed in Section 6. Last, we outline our future work and conclude by discussing our contributions in Section 7.

2. RELATED WORK

Reciprocity can exist even between people and computers. Moon reported that research participants were more likely to disclose intimate details about themselves to computers when the rules of reciprocity were followed [12]. During the interaction, a computer displayed text information and a question. Then, a participant typed in an answer. When the norm of reciprocity was followed, participants answered questions about their feelings and emotions in more detail than in the non-reciprocity control condition. For example, the computer displayed a message showing that it felt "guilt" because all of its capabilities are infrequently used. Then, participants could reveal their guilt in their daily life or sexual fantasies. In addition, Reeves and Nass argued that people may interact with computers in the same way as real social relationships [19]. Fogg demonstrated that computers may use multiple technologies (e.g., audio, video, hyperlinked content, graphics) to match people's preferences and achieve persuasive impact [20]. This work highlights a reciprocal exchange of information for information.

The reciprocity effect has also been shown among strangers. In Berg, Dickhaut, and McCabe's experimental study of the norm of reciprocity [21], participants played an investment game. The game players did not know or see each other and their information was kept anonymous during and after the games. The experiment results showed that reciprocity was the reason that participants gave money to unfamiliar people. This research demonstrates reciprocity can provide a foundation for interactions between unfamiliar others.

People are concerned about privacy, but studies have shown that they unnecessarily provide too much information. In Ackerman, Cranor, and Regale's survey research, more than half of the participants provided information about their income, investments, and investment goals to a banking website [6]. An Internet shopping experiment demonstrated that self-reported privacy preferences do not necessarily match privacy disclosure behavior. For instance, about 40% of the participants provided their home address without any reason to do so [5].

There are studies about people's privacy concerns in mobile and pervasive computing environments. For example, Nguyen at el. investigated privacy issues with everyday sensing and tracking technologies (including RFID tags) [7] and wearable cameras (SenseCam) [22]. However, there are few experimental or empirical studies of privacy attacks. In this research, we study people's identity exposure behavior under various reciprocity attacks.

Privacy and identity exposure may have potential benefits, such as saving time, saving money, and customizing information [23]. Thus, some people value these personalized information and services. Nevertheless, they often underestimate the privacy impact and overvalue small immediate benefits [23]. Acquisti used a general game theoretic model to show that people are unlikely to make rational decisions because they do not have complete information, but rather have bounded rationality (i.e., one incapable of calculating various parameters for the payoff functions) [1]. He further pointed out that people may sacrifice long term privacy for immediate gratification. Our study suggests that the norm of reciprocity may be one of the reasons that people behave irrationally. People may provide their identity information and expect services to be provided via reciprocity.

Identity exposure is essential in daily tasks [18, 24-25]. Marx classified the broad range of identities into seven types [26]: a person's legal name, address, unique symbols (alphabetic or numerical), pseudonyms that cannot be linked back to a person, a person's distinctive appearance or behavior patterns, social categorization (such as gender, ethnicity, religion, etc.), and possession of knowledge (such as password and secret codes). Goldberg expressed the identities in four sensitivity levels: verinymity (e.g., social security number), persistent pseudonymity (e.g., pen name), linkable anonymity (e.g., prepaid phone card), and unlinkable anonymity (e.g., cash) [25]. Goldberg's privacy-preserving approach tried to use the least sensitive identity level and the anonymous servers in the infrastructure. Thus, unnecessary identity exposure was reduced. Since the original anonymity idea was proposed to achieve untraceable emails [27], many approaches have been designed to achieve anonymity by using anonymous servers including the solutions for mobile and pervasive computing environments such as Mix Zone [28] and k-anonymous location servers [29]. While anonymity is an effective privacy protection approach, it may not be available or applicable to various identity exposure situations in mobile and pervasive computing environments. Often, people need to make decisions on whether they should expose their identity information or how much detailed identity information they should provide.

Our earlier work focused on identity exposure in mobile and pervasive computing environments [8]. Specifically, we conducted an extensive survey and experiments on five aspects of identity exposure: (a) identity elements that people think are important to keep private (their attitudes); (b) their privacy concerns; (c) actions people claim to take to protect their identities and privacy; (d) people's identity exposure behavior in mobile and pervasive computing environments; and (e) whether rational suggestions can help people avoid unnecessary identity exposure by using our RationalExposure model [24]. We found that although their attitudes, concerns, and claimed actions seemed rational, their actual behavior did not always match their privacy preferences. Those study results serve as our baseline data for this new study and help us to understand identity exposure behavior under reciprocity attacks.

Research on animated interface agents inspired our work. Animated agents have been used for cognitive function support to improve understanding and learning [30]. Various agent forms, based on real video, cartoon-style drawings, 3D-models, and life-size models, have been developed in standalone and web-based applications. Although different empirical studies suggest different effects in terms of whether animated agents change users' behavior or whether they provide positive outcomes of human computer interactions, studies do show that usage of agents significantly increases users' concentration and interest [30]. Bickmore and Cassell applied a conversational strategy, small talk, and an animated agent to build trust with users [31]. Suzuki and Yamada used animated agents to apply overheard communication (one of the persuasion techniques) to change people's attitude and behavior [32]. We also implemented a cartoon-style recommendation agent with simple expressions and mouth movements in order to engage participants but not overly distract them from the basic tasks of the experiment.

3. EXPERIMENTAL DESIGN

We hypothesized that participants in the reciprocity attack condition would disclose more of their private information than those in the control condition.

We assume that attackers need to know only that the reciprocity norm is an effective strategy at eliciting personal identity information from people. The attack is not limited to pervasive computing environments, but can also be employed using other technologies such as websites. If our research shows that these attacks are effective, security countermeasures would need to be developed as mitigations.

We conducted experiments and surveys to achieve the following goals.

- Gain an understanding of participants' identity exposure behavior under reciprocity attacks. We wanted to document participants' exposure behavior for different identity elements. We predicted that more participants would disclose information in the reciprocity condition than in the control condition.
- Identify the relationships between people's attitudes towards protecting their identity elements and their exposure behavior under reciprocity attacks.

The participants were recruited from the students who were taking introductory psychology classes at The University of Alabama in Huntsville. Psychology can serve as a general education requirement for most undergraduates; the sample therefore consisted of students having majors in science, engineering, liberal arts, business, and nursing. We posted our experimental descriptions (without mention of privacy or security issues), and the students signed up to attend our study at times convenient for them. In return for participating, the students received "activity points" toward their course assignments; they were not compensated in any other way. It is the practice of psychology departments at research universities in the United States to expect students to have “hands-on” experiences with research.

We used a mixed-method design, an experiment and a follow-up questionnaire, to study participants’ identity exposure behavior and their privacy rationale. The participants were asked to come to our lab in the Computer Science department and were assigned to either the control (non-reciprocity) condition or the reciprocity attack condition. The research was presented as a third-party (Tune Nation) marketing survey, in order to alert the participants that their information would be shared with entities other than the experimenters.

We advertised and conducted the experiments as a future shopping experience with the focus on accessing rich product information via handheld devices. After participants evaluated their shopping experience in the questionnaires, we asked them to rate the importance of various identity elements, privacy concerns, and the frequency of privacy protection actions. This follow-up questionnaire allowed us to study participants’ behavior and attitudes without biasing them towards privacy and security during the simulated shopping experience. We also asked the participants not to reveal the information to the fellow students for the sake of the integrity of the experiment.

3.1 Procedure

Upon arrival, we provided every participant a PDA with earphones and a brief overview of the experiment (a future shopping experience). If a participant was not familiar with the controls, the touch screen, or the stylus, we provided them with a tutorial. Participants used the software (called InfoSource) to access eight CDs that were displayed on shelves. One to four participants could attend a session (most commonly, sessions had two participants), but they did not interact with each other. All participants in a session were, as a group, randomly assigned to the reciprocity or control condition (leading to unequal sample sizes). Once participants finished shopping, they were assigned a computer to complete the questionnaire. Participants usually spent 30 minutes to complete the entire process, but completed the study at their own pace.

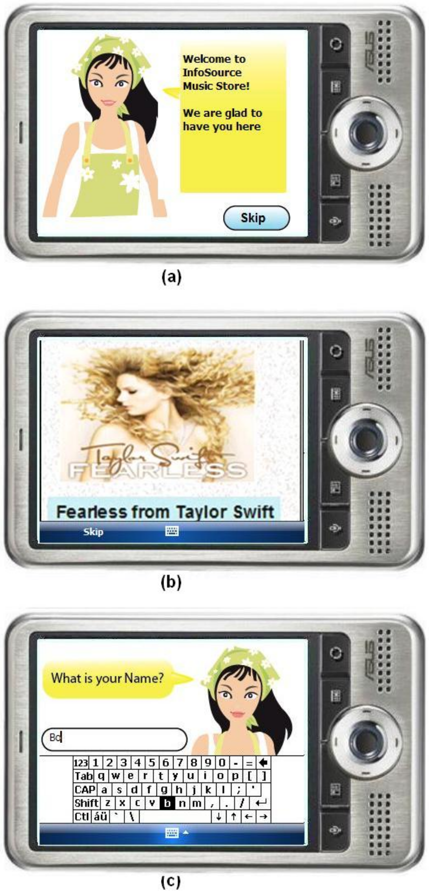
To protect participants’ privacy, we did not record any identity information. Instead, we recorded *whether* they provided a certain piece of information. Their actual identity information was deleted as they were inputting the information, but participants were not aware of this at the time. After they finished the experiments and questionnaires, however, we told them that none of their actual information had been recorded or sent to a server. In addition, the lab was arranged in a way that wireless communication was encrypted using AES and none of the PDAs or computers was connected to the Internet or any other computers that were not part of this study. The procedures of the experiment and the measures taken to protect participants’ privacy were approved by our university’s IRB.

3.2 The InfoSource Software

We used InfoSource V3.0 in the experiments, which provided more interactive and a smoother user experience than InfoSource V1.0 that we used in another study [8]. An animated recommendation agent, Alice, introduced herself and greeted the user as shown in Figure 1 (a). When she was talking, her mouth moved. (We recorded the voice of a real woman and played it back.) We attempted to achieve a reasonable amount of ecological validity by simulating an “app” that could actually be developed and appreciated by users.

Alice guided a user through the CD shopping experience. If a user was interested, Alice presented the CD’s background information, its popularity, sales information, and other information. When she presented the information, related photos were displayed in the slide show form with the key phrases shown on the screen (Figure 1 (b)). A user might click a skip button at anytime to skip the information and resume interactions with Alice. Alice also offered sample music videos of the songs in the CD. A user viewed it in the full screen mode. Similarly, a user might stop the video by tapping on the screen and return to the interaction with Alice. When Alice asked questions, participants used a stylus to input text as shown in Figure 1 (c).

We designed the software to include an animated agent to increase participants’ attention, interest, and trust. On the other hand, we did not want to introduce other factors that might affect participants’ identity exposure behavior. In the experiments, Alice therefore stated detailed information about the CDs in an objective way. When Alice interacted with participants, no strategy other than the reciprocity attack was used.


Welcome to InfoSource Music Store!

We are glad to have you here

Fearless from Taylor Swift

What is your Name?

Figure 1. The InfoSource software screenshots. (a) Alice introduces the music store and herself. (b) Information related to a CD is displayed in a slideshow form. (c) A screen for users to input data.

3.3 Participants

Sixty-nine participants attended our main experiment. (Ninety-eight participants attended our pilot studies, which will be discussed in Section 5). All of the 69 participants who were involved in the experiment were college students. Of the 69 participants in the experiment, about 68% were female students. Their ages ranged from 18 to 40, with an average of 22. All participants in a session used the same software.

3.4 Reciprocity Attacks

The reciprocity attacks were embedded in the experiments. The questions were designed such that the norm of reciprocity was used. That is, for each identity question, Alice provided information first. Then, she asked a participant to provide his or her information. Four different reciprocity approaches were used, as described below. Note that these interactions approximate the types of reciprocal exchanges that are typical between users and service providers. Twenty-three participants were in the reciprocity attack condition. The scripts for the reciprocity and control conditions are shown in Appendix A.

Reciprocity 1. Alice provided music-related information and asked for participants' date of birth. Alice discussed personality and the music preferences related to different zodiac signs. For example, after a participant watched a music video of Matt and Kim's Grand, Alice would say: "Indie rock and alternative rock music such as Matt and Kim's Grand is usually popular with people born under the zodiac sign of Aries, born in between March 21 and April 19, as they are known to be adventurous, active and outgoing." Then, she requested that the participant input his or her date of birth. In this case, information is being exchanged for information.

Reciprocity 2. Alice told participants that they would get additional services by providing their monthly income or monthly expenses. Alice told them: "At Tune Nation, we seek to provide great customer satisfaction by accurately recommending songs and music albums that our customers are going to love. We are building a world class music genre recommendation system to bring you great value and accuracy. More than 75% of the customers like the albums that we suggested. I would like to recommend you another album." Then, Alice asked participants to select a music genre and input their monthly income information. Service providers are already exploiting this type of reciprocity exchange when they ask for users' preferences (e.g., Netflix provides suggestions for movie selections based on the user's ratings of movies they have already watched). In this case, information is being exchanged for information (recommendations).

Reciprocity 3. Alice offered potential monetary benefit to participants in return for their identity information. Alice said: "Throughout the year, we mail coupons to our customers. You will save 20% - 30% on any regular or on sale music or video product purchased in store or online. On your birthday, you will receive an exclusive 40% off coupon." Then, she asked participants to give their home addresses. This type of reciprocity exchange already occurs when shoppers get a discount on food when they use a supermarket-specific identity card (containing a variety of identity information). Here, information is being exchanged for a product (or compensation).

Reciprocity 4. Alice offered a music download service and asked for participants' phone numbers, indicating that the phone number would be used as a form of identification; using that phone number the participant could download the purchased songs, music albums or movies from the store website directly to the participant's cell phone. Alice also told the participants that they could switch to another phone number at any time, in case they felt the need. Alice also assured the participant, "Tune-Nation does not make any sales calls to the phone number that you provide." In this case, information would be exchanged for a service.

Forty-six participants were in the control group. They used the software with all features except the reciprocity attacks. Alice asked for identity information when a certain feature, such as a sample music video, was viewed.

In our experiments, participants typed their responses using a stylus. The input could potentially be replaced with a wearable microphone and voice recognition technologies in alternative devices.

3.5 Questionnaire

The questionnaire that participants completed after the experimental portion of the study had three sections: the first section was for demographic data, the second section gathered users' feedback on our software, and the third section was dedicated to privacy-related questions. Prior to the third section of the questionnaire, participants were not aware that our research had any relation to privacy; thus, their previous disclosure behaviors would not have been influenced or contaminated by this knowledge.

In the section that contained participants' feedback on the software, we asked them questions including whether the recommendation agent (Alice) was helpful, which features they liked most and least, whether the shopping experience was realistic, and whether they would use the technology.

For the privacy part of the questionnaire, we asked participants whether they had provided accurate identity information. We had only recorded *whether* a participant had provided information and did not record the actual information. We asked participants to be honest with us at this point and to indicate, for each of the five identity items, why they provided correct identity information, why they did not provide identity information, or why they provided fake identity information. As these queries occurred immediately following the shopping experience, we expect that participants had good recall of how they responded.

Moreover, participants rated the importance of eleven identity elements, their concerns on six privacy related issues, and the frequency of privacy and security protection actions that they took. These questions were selected and based on our statistical analysis results in our previous study [8]. The questions enabled us to gauge a participant's privacy attitudes, concerns, and claimed private protection actions. After all participants had completed the study, we sent an email debriefing to all participants, indicating that our goal in this research project was to identify the types of private information they would provide to us in various contexts.

3.6 Selection of the Identity Elements for the Experiments

In one of our previous research projects [8], we asked 229 participants to rate how important it is to keep 26 identity elements private. Figure 2 shows participants' ratings on 9 identity elements that are representative.

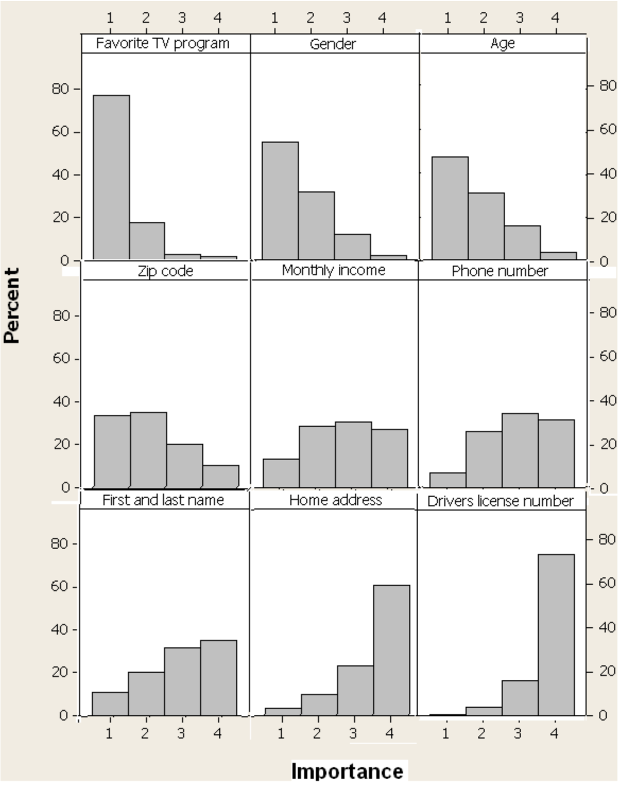


Figure 2. Importance ratings of the identity elements from our previous study in [8]. (1. Not at all important, 2. Somewhat important, 3. Substantially important, and 4. Extremely important.)

Based on participants' ratings, we could document their attitudes towards identity exposure. In general, their attitudes were quite different across these identity elements. For some identity elements, most participants had the same opinion. For example, they thought that driver's license numbers and information are extremely important to keep private and their favorite TV programs are not at all important. For other identity elements, such as zip codes or phone numbers, their opinions diverged widely.

For our experiments, we selected the identity elements from this original pool that are related to the CD shopping context and are sensitive (i.e., people want to keep them private). We asked for the following identity elements: home address, phone number, date of birth, and monthly income. Selection of the identity elements was a critical task in this study. We will discuss additional findings relevant to this selection and lessons that we learned in a later section of this paper.

4. EXPERIMENTAL RESULTS AND KEY FINDINGS

Most participants thought that Alice was helpful. When we asked them whether they liked the interaction with Alice, over 85% of the participants were positive. Participants' own words best expressed their experience.

"I really enjoyed the videos! It reminds me of the display used by [store name omitted by the authors] to sample CDs. I think the interaction with Alice also enhanced the experience. I also enjoyed the zodiac information it made me interested in what songs I would be interested in."

"I like the fact that the handheld device talks to you, it is nice how it interacts with people. I disliked how it asked a lot of questions because I just wanted to know about the product."

4.1 Identity Exposure Behavior

In the control condition, participants' overall identity exposure behavior matched the importance ratings of the identity elements in our survey data [8]. Among the identity elements that Alice requested (shown in Table 1) the percentage of participants who provided their income information was relatively low. Many participants wrote that they believed that their monthly income was not relevant to music shopping, so fewer participants were willing to provide their income information. The identity exposure behavior of the 23 participants in the experimental reciprocity attack condition, however, revealed this information at a much higher rate (also shown in Table 1).

Table 1. Number of participants who provided the identity elements in the control group and the reciprocity condition.

	Control		Reciprocity	
Income	12	26%	13	57%*
Date of Birth	31	67%	21	91%*
Phone	19	41%	7	30%
Address	18	39%	7	30%
No. of Participants	46		23	

* Asterisks indicate the percentage is significantly larger than the control group (p-value < 0.05).

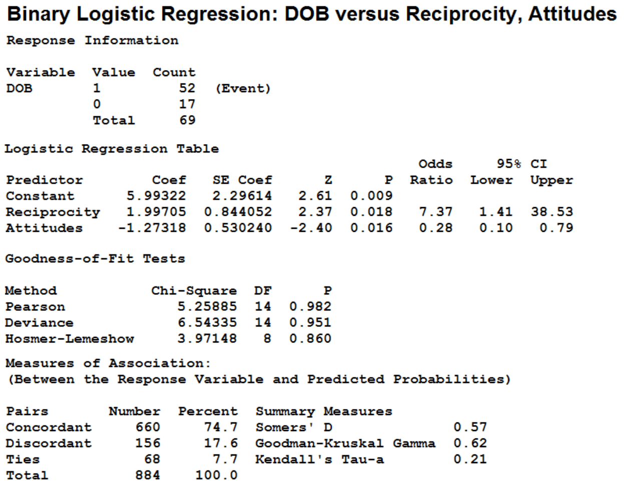
Alice successfully acquired about 57% of the participants' monthly income information in the reciprocity condition. In comparison, only 26% of the participants provided the monthly income information in the control group. Thus, the attack proved to be effective (Z = -2.50 and p-value = 0.006), as indicated by a Z-test comparing the proportions in the two conditions. The odds ratio that measures the influence of exposure on reciprocity attack equals 3.68. That is, the odds of exposing income information were about three to four times greater for participants who were under the reciprocity attack than those who were not. We do not believe that monthly income is related to music preferences, but participants seemed willing to see the relationship between the two. One participant thought that "it was necessary for the program to provide me with music feedback." Some participants were more cautious and did not provide their real income information. One wrote: "[I] want to try out the selection based on the input I give." Other participants believed that their income information was personal and they avoided inputting the information.

After Alice presented the zodiac sign related to the CD album, about 91% of the participants provided their date of birth information. Compared to the participants in the control group (67% provided the information), the reciprocity approach seems quite successful. We ran the two proportion test (left-tailed) to compare whether the reciprocity condition group was more likely to provide their information than the control group. With the Z = -2.64 and p-value = 0.004, it was statistically significant that participants in the reciprocity condition were more likely to provide their date of birth information than those in the control group. To evaluate the effect size of the reciprocity attack, we calculated the odds ratio (odds ratio = 5.08). We concluded that the odds of exposing date of birth information were five times greater for participants who were under the reciprocity attack than those who were not.

Participants' feedback provided additional insight about their exposure behavior. Some participants mentioned that information about the zodiac signs were one of their favorite features. Actually, information about the zodiac signs was the second most popular feature (the most popular one was the sample music video). One participant wrote "I liked the feature which lists compatible music for zodiac signs and other interesting information." A few participants did not like the zodiac sign information since they did not believe in it. One wrote: "The previews of music videos were very helpful, but I wasn't concerned with the zodiac information."

It seems that when people think that the reciprocal information or services provided are relevant, they are willing to provide their identity information. This behavior deviates, however, from their attitudes about providing identity information. For example, about 22% of the participants in the reciprocity condition believed that information about their date of birth was extremely important to keep private, but only 9% of the participants in this condition did not provide this information under the reciprocity attack. Compared to the control group, fewer participants in the reciprocity attack condition provided their phone numbers and home addresses. The percentages in the two conditions, however, are not statistically different than each other. Therefore, reciprocity attacks on these two elements were not successful. Future research should identify which identity elements can be elicited by using reciprocity attacks and which are more resistant to this psychological strategy.

Alice offered to mail coupons to participants' home addresses. All large majority of participants stated that they did not want junk mail. Participants clearly knew the consequences of providing their home address and chose to keep that information private.



```
Binary Logistic Regression: DOB versus Reciprocity, Attitudes
Response Information

Variable  Value  Count
DOB       1         52  (Event)
          0         17
          Total     69

Logistic Regression Table
                                                      Odds     95% CI
Predictor        Coef   SE Coef      Z      P  Ratio  Lower  Upper
Constant      5.99322   2.29614   2.61  0.009
Reciprocity   1.99705  0.844052   2.37  0.018   7.37   1.41  38.53
Attitudes    -1.27318  0.530240  -2.40  0.016   0.28   0.10   0.79

Goodness-of-Fit Tests

Method           Chi-Square  DF      P
Pearson             5.25885  14  0.982
Deviance            6.54335  14  0.951
Hosmer-Lemeshow     3.97148   8  0.860

Measures of Association:
(Between the Response Variable and Predicted Probabilities)

Pairs       Number  Percent  Summary Measures
Concordant     660     74.7  Somers' D              0.57
Discordant     156     17.6  Goodman-Kruskal Gamma  0.62
Ties            68      7.7  Kendall's Tau-a        0.21
Total          884    100.0
```

Figure 3. Logistic regression results showing the relationships among behavior, the reciprocity attack, and attitudes.

4.2 Relationships among Behavior, Attitudes, and Attacks

Experimental research on identity exposure behavior poses the challenge that participants' behavior may be affected by other currently unknown factors. Although people's privacy attitudes may be acquired via surveys [7-8], their behavior may not always match their attitudes [5-6]. With attitude data from the post-experimental questionnaire and behavioral data from the experiment, we conducted quantitative analysis of the relation between behavior, attitudes, and reciprocity attacks. In this subsection, we discuss our model of the relations.

We used logistic regression to test the relationships among behavior, the reciprocity attack, and attitudes. We used the following model to predict the exposure of date of birth.

$$\textit{Date of Birth exposure} = \beta_0 + \beta_1 x_1 + \beta_2 x_2$$

where x1="Reciprocity attack"

(dummy coded with no reciprocity attack = 0)

x2="Attitudes"

Our previous research [8] revealed that people's attitudes towards identity elements can be separated into three clusters. Within each cluster, they rated the identity elements as similarly important to keep private. We selected ratings of three representative identity elements in each cluster (zip code, home address, and credit card number) to calculate participants' attitudes. We used the average of the three ratings as indicative of participants' attitudes.

The logistic regression results are shown in Figure 3. The p-values for both factors (reciprocity attack and attitudes) are less than 0.05. Thus, there is sufficient evidence that both factors influence participants' behavior. The negative coefficient of the attitudes indicates that participants were less likely to expose their dates of birth if they rated the identity elements as more important to keep private. The Goodness-of-Fit tests (Pearson, Deviance, and Hosmer-Lemeshow) show that there is no evidence that our model does not fit the data adequately. In the measures of association section, the summary measures (Somer's D, Goodman-Kruskal Gamma, and Kendall's Tau-a) indicates that the model provides 21% to 62% of the predictive ability.

We did not find a model that significantly captured the relationships between the reciprocity attack, attitudes, and participants' exposure of their income information.

5. OTHER FINDINGS AND LESSONS LEARNED

We conducted several pilot studies that informed the design of our primary experiment. We believe that it might be worth sharing how our research program developed and the lessons we learned along the way.

5.1 Trust and Identity Exposure

In the first experiment on the reciprocity attack, we asked participants about five identity elements: name, gender, age, birthday, and zip code. Approximately half the participants were in the reciprocity (n = 24) and the other half in the control (n = 25) condition. Regardless of condition, almost all participants provided all of the identity information that we requested. Among the three participants who did not provide their names, at least two of them did not know how to use the stylus and approached one of our researchers during the experiment for assistance. Results of this experiment are shown in the first pair of data columns (labeled Reciprocity and Control) in Table 2.

When we evaluated the comments made by participants in the survey following the experiment, we found that many reported trusting us with their identity information. The experiments were conducted in our lab on campus and all participants were college students. They believed that the exposure of their identity information was safe with us. We therefore speculated that this trust might be the main factor that exposure rates in these preliminary experiments were high.

Table 2. Number of participants who provided the identity elements in the reciprocity condition, the control condition, and additional low trust control condition.

	Reciprocity		Control		Low Trust Control	
Name	21	88%	25	100%	28	97%
Gender	24	100%	24	96%	28	97%
Age	24	100%	25	100%	29	100%
Birthday	24	100%	24	96%	26	90%
Zip code	21	88%	23	92%	23	79%
# Participants	24		25		29	

Participants' perceptions of our trustworthiness challenged us to design a more ecologically valid setting – one in which participants should have some level of privacy concerns. One approach that we used to increase these concerns was to present some informational slides before conducting the experimental sessions. In the slides, we introduced a third-party, Tune Nation, which ostensibly created the software and collected the data. In addition, we provided a "disclaimer," stating that we merely conducted the experiments for Tune Nation and would share personal information with them. After a few iterations of modifying the slides to reduce trust levels, we were able to reduce trust to some extent, as indicated by comments in the follow-up survey such as "I think I pressed the skip button. I don't like to give out my number because I do not like strangers calling me."

We thereafter ran an additional control condition of the experiment in this low trust situation. The results are shown in the third pair of data columns (labeled Low Trust Control) in Table 2. Compared to participants in the high trust situations, the participants in this lower trust condition were less likely to expose their zip code and birthday information. Overall, however, 72% of the participants still exposed all of the requested information.

Other factors might also contribute to high trust. For instance, if participants carefully read our consent form, they knew that we promised no harm to them. Thus, a low trust condition may be difficult to avoid in a research setting on a college campus (or even in some retail situations).

5.2 Unawareness of the Sensitivity of Identity Elements

According to Sweeney's report [33], four pieces of the identity elements (gender, zip code, age, and birthday) may uniquely identify 87% of the individuals in the United States. Thus, by using a name and the other four identity elements, one may be uniquely identified in the United States.

It might be surprising that people can be uniquely identified by the combination of zip code, date of birth, and gender. The following calculation, however, shows that people may be uniquely identified. Divide 300 million people in the U.S. by 40,000 zip codes, 365 days a year, 2 gender types, and possibly 100 different ages; the result is about 0.1.

Since the combination of one's name, gender, age, birthday, and zip code may uniquely identify an individual, participants should be cautious in disclosing their information. The combination of the information is as sensitive as one's home address. Individuals' attitudes towards disclosing gender, age, zip code, and address are shown in Figure 2. Participants were more concerned about revealing their address than this combination, indicating a lack of awareness about the sensitivity of information when it is combined.

After identifying the potential importance of the trust factor and the participants' unawareness of the riskiness of exposing the five identity elements, we modified the design of our experiments to take these factors into account. We then used the identity elements that are representative and more sensitive in our later experiments, as we showed in Table 1.

5.3 Helping People Understand Technologies and Exposure Consequences

During the experiments containing low trust conditions, we found that some participants believed that their identity information was stored locally on the PDAs and that their information was safe. To address the issue, we added a slide to the introduction of the experiment that depicted information flow from the campus location to the hypothetical location of Tune Nation. It showed that participants' information would transmit to a server in the store, and then it would transmit to the Tune Nation's central server.

An encouraging finding in our experiments is that if one knows the consequence of an identity exposure, he or she may make a better identity exposure decision, one that better reflects his or her attitude. For example, in one of the reciprocity attacks, Alice told participants about the service that would be provided to them. And then, she added: "Remember Tune Nation does not make any sales calls to the phone number that you provide." One participant responded in the questionnaire as follows. "Even though the agent said that the customer care agents won't bug me, I usually don't give out my phone numbers to anyone."

5.4 Reciprocity Attacks by Exchanging Equivalent Information

We also wanted to study whether a reciprocity attack in which exchanging equivalent identity information was used would be successful. This reciprocity approach follows Moon's work, with disclosure of "equivalent" intimate details between people and computers [12].

We asked participants to provide four pieces of information: date of birth, income, phone number, and home address. The experimental setting and software were the same as we discussed in Section 3. Twenty participants attended this experiment.

For some identity elements, such as name, it would not seem unnatural for an exchange to occur between Alice and participants. Nevertheless, it would be strange if Alice provided her phone number and home address. It would become even more unrealistic if Alice talked about her date of birth or income. Therefore, Alice discussed a singer's date of birth and address, and Alice's own phone number and contribution to the store's income.

We did not obtain any additional disclosure effects due to reciprocity in these conditions. But it may be worth examining a case in detail. Before Alice asked participants' phone numbers, she said: "If you need more information about any music album, please feel free to call me. My personal phone number is 1-800-CALL-TUNES." Most participants responded in their questionnaires that they did not need to provide their phone numbers and they did not want to receive telemarketing calls. Thus, the specific framing of these reciprocity attacks may have been weak or unrealistic.

There are two aspects that vary between our experiment and Moon's study. First, our experiment was conducted in a low trust setting. That is, we warned participants that information that they provided would be disseminated beyond the experiment environment. Second, participants in Moon's study disclosed information about feelings and behaviors, rather than disclosing identity information that might be used in malicious ways.

5.5 Using the Follow-up Questionnaire to Understand Behavior

We faced several dilemmas in our research on privacy. We want to understand people's identity exposure behavior while, at the same time, protecting our participants' identity information by not collecting it.

Throughout these studies, the follow-up questionnaire became the major tool for understanding participants' behavior. We used it to ascertain why a participant would provide accurate information, fake information, or no information. In addition, we used the questionnaire to learn about participants' reactions to various software features, their attitudes, and their responses to high trust conditions.

6. LIMITATIONS OF OUR STUDY

Like any other experimental study, we have faced our own share of limitations while conducting our experiment. We discuss the limitations we consider most salient and important to share.

University Setting: During the initial runs of the experiment many students mentioned that they felt comfortable giving their private information to the experiment because it was conducted on campus. They trusted us enough to feel safe exposing their private information. In order to remove this "university factor" and to make the experiment more ecologically valid, we introduced a pretend third party store, Tune Nation. We informed participants, before they started the experiment, that the experiment was being conducted on behalf of this third party store and that the university was not responsible for any private information the participants chose to provide to this third party store. This change had the intended effect – participants were less likely to provide identity information.

Undergraduate participants: Most of the participants that were recruited were undergraduate students and most of them were between the ages of 18 and 22, which limits the generalizability of our results. Perhaps this generation, however, is most representative of users of modern computing devices for mobile and pervasive computing environments. Younger adults are likely more open to new technologies, such as shopping while interacting with a computer animated online recommendation agent. We also suspect that these are the ages when people first begin to start shopping online, such that college students were a good sample for the experiment. In our future work we plan to study the behavior and attitudes of participants from more diverse backgrounds and age groups.

When the participants were providing their private information during the experiment, we did not actually record the information but rather we just recorded whether they gave the information or not. And at the end of experiment we asked the participants, in a questionnaire, which private information they provided, faked or did not provide at all. So, these results in our study depend on whether the participants remember and accurately reveal which information they provided, faked, or did not provide at all. We chose to take this risk, rather than the potential risk of participants' true identity information possibly being compromised. We also expected that their recall of how they responded to the 5 identity requests would be accurate so soon after the shopping experience.

Another limitation of our study is that it is a very specific case demonstrating a reciprocity attack that consumers may face while shopping via technology. There is a broad spectrum of scenarios to which the reciprocity attack can be applied. Thus, it is important to continue to explore how our findings about the effectiveness of reciprocity attacks generalize to other settings and other identity elements.

We used a computer animated recommendation agent to "deliver" the reciprocity attacks. Alice provided some information or service related to the music album and/or store in general in return to the private information provided by the participants. This may indicate the power of the norm of reciprocity. Reciprocity attacks may be even more effective if a human agent is involved. Future research can address this possibility.

7. CONCLUSION AND FUTURE WORK

Our major goal and the contribution of this research were to verify that the norm of reciprocity can be used effectively as a psychological privacy attack. In mobile and pervasive computing environments, malicious attackers may utilize the attack and the convenience of the communication between people and intelligent environments to acquire various aspects of personal information. We conducted experiments to show that under reciprocity attacks participants may be more likely to provide some of their sensitive identity information that could be used to uniquely identify them. The exposure behavior deviated from participants' self-stated attitudes about identity information and their intention to keep the information private.

Our theoretical model for the research is based on the norm of reciprocity and how it provides a foundation for exchanges. We chose reciprocity as our construct for understanding information disclosure because it can encompass a variety of types of exchanges (e.g., for information, services, products). Thus, it can account for value propositions, in which disclosure occurs for a concrete benefit (money, service) in return, as well as interpersonal interactions (getting to know one another).

We learned about some limitations of these kinds of attacks. The specific attacks were effective in obtaining disclosure of income and date of birth, but not for phone number and home address. Possibly, more effective approaches for reciprocity attacks may be designed for phone number and home address that are more compelling than ours. Alternatively, some identity information may be more resistant to this type of strategy than others. Future research needs be conducted to determine which types of attacks are most effective in eliciting different types of identity information.

In our future work we will also be exploring the contexts in which people are more or less likely to disclose their private information. In the current research we investigated pervasive computing environments, but people may also disclose on the web, through social networks, or through other public computerized sources.

We are currently designing countermeasures for reciprocity attacks. Specifically, the design is based on our RationalExposure model. The RationalExposure model was the first application of game theoretic approaches to minimize identity exposure in mobile and pervasive computing environments. It models identity exposure between users and service providers as extensive games. To address the reciprocity attack, we need to extend and complement our game theoretic approaches discussed in [24]. In addition, we are also designing countermeasures based on psychological theories and methods related to effective persuasion strategies and their mitigations.

One of our ongoing research programs is to make rational privacy exposure suggestions to users. Our goal is to provide users with enough information to make exposure decisions and to avoid unnecessary exposure. The challenge is that users may be aware of the appropriate rational actions, but they may not adopt them. Another challenge is the interaction between users and our software via mobile devices. Potentially, more users will accept our rational suggestions when we provide detailed information and data. But we need to adapt the suggestions to the small screen size, and we want to maximize users' attention.

8. Acknowledgment

The authors are grateful to Dr. Sonia Chiasson and the anonymous reviewers for helping them to greatly improve this paper.

9. REFERENCES

[1] A. Acquisti, "Privacy in Electronic Commerce and the Economics of Immediate Gratification," in 5th ACM conference on Electronic Commerce, New York, NY, 2004.

[2] G. Newman and M. McNally, "Identity Theft Literature Review," U.S. Department of Justice2005.

[3] M. Culnan, "Protecting Privacy Online: Is Self-Regulation Working?," Journal of Public Policy & Marketing, vol. 19, pp. 20-26, 2000.

[4] L. Sweeney, "k-ANONYMITY: a Model for Protecting Privacy," International Journal on Uncertainty,Fuzziness and Knowledge-based Systems, vol. 10, pp. 557-570, 2002.

[5] S. Spiekermann, et al., "E-privacy in 2nd Generation E-Commerce: Privacy Preferences versus actual Behavior," in Proceedings of the 3rd ACM conference on Electronic Commerce, Tampa, Florida, 2001.

[6] M. S. Ackerman, et al., "Privacy in E-Commerce: Examining User Scenarios and Privacy Preference," in Proceedings of the 1st ACM conference on Electronic commerce, Denver, Colorado, 1999.

[7] D. H. Nguyen, et al., "An Empirical Investigation of Concerns of Everyday Tracking and Recording Technologies," in Proceedings of the 10th international conference on Ubiquitous computing, Seoul, Korea, 2008.

[8] F. Zhu, et al., "Understanding and Minimizing Identity Exposure in Ubiquitous Computing Environments," in Proceedings of the 2009 International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (Mobiquitous 2009), Toronto, CA, 2009.

[9] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Edition: Wiley, 2008.

[10] R. B. Cialdini, "The Science of Persuasion," Scientific American, vol. 284, pp. 76 - 81 2011.

[11] I. Altman and D. A. Taylor, Social penetration: The development of interpersonal relationships: Holt, Rinehart & Winston, 1973.

[12] Y. Moon, "Intimate exchanges: Using computers to elicit self-disclosure from consumers," Journal of Consumer Research, vol. 26, pp. 323 - 339, 2000.

[13] D. L. Ferrin, et al., "It takes two to tango: An interdependence analysis of the spiraling or perceived trustworthiness and cooperation in interpersonal and intergroup relationships," Organizational Behavior and Human Decision Processes, vol. 107, pp. 161 - 178, 2008.

[14] G. R. Milne and M.-E. Boza, "Trust and concern in consumers' perceptions of marketing information management practices," Journal of Interactive Marketing, vol. 13, pp. 5-24, 1999.

[15] E. Fehr and A. Falk, "Wage Rigidity in a Competitive Incomplete Contract Market," Journal of Political Economy, vol. 107, pp. 106-134, 1999.

[16] A. W. Gouldner, "Norm of Reciprocity : a Preliminary Statement " American Sociological Review, vol. 25, pp. 161-178, 1960.

[17] M. Bishop, Computer Security: Addison Wesley, 2003.

[18] J.-M. Seigneur and C. D. Jensen, "Trading Privacy for Trust," in Trust Managment. vol. 2995/2004, ed: Springer, 2004.

[19] B. Reeves and C. Nass, The Media Equation: How People Treat Computers, Television, and New Media Like Real People and Places,: CSLI Publications, 1998.

[20] B. Fogg, "Persuasive Technology: Using Computers to Change What We Think and Do," Ubiquity, vol. 2002, 2002.

[21] J. Berg, et al., "Trust, Reciprocity, and Social History," Games and Economic Behavior, vol. 10, pp. 122-142, 1995.

[22] D. H. Nguyen, et al., "Encountering SenseCam: Personal Recording Technologies in Everyday Life," in Proceedings of the 11th international conference on Ubiquitous computing, Orlando, Florida, 2009.

[23] A. Kobsa, "Privacy-Ehanced Personalization," Communications of the ACM, vol. 50, pp. 24-33, 2007.

[24] F. Zhu and W. Zhu, "RationalExposure: a Game Theoretic Approach to Optimize Identity Exposure in Pervasive Computing Environments," in IEEE Annual Conference on Pervasive Computing and Communications (Percom 2009), Galveston, TX, 2009.

[25] I. Goldberg, "A Pseudonymous Communications Infrastructure for the Internet," PhD thesis, Computer Science, University of California at Berkeley, 2000.

[26] G. Marx, "Identity and Anonymity: Some Conceptual Distinctions and Issues for Research," in Documenting Individual Identity: The Development of State Practices in the Modern World, J. Caplan and J. C. Torpey, Eds., ed, 2001.

[27] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Communications of the ACM, vol. 24, pp. 84-90, 1981.

[28] A. Beresford and F. Stajano, "Location Privacy in Pervasive Computing," IEEE Pervasive Computing, vol. January-March, pp. 47-55, 2003.

[29] M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking," in 1st international conference on Mobile systems, applications and services, New York, NY, 2003.

[30] D. M. Dehn, "The Impact of Animated Interface Agents: a Review of Empirical Research," Journal of Human-Computer Studies, vol. 52, pp. 1-22, 2000.

[31] T. Bickmore and J. Cassell, "Relational Agent: a Model and Implementation of Building User Trust," in SIGCHI conference on Human Factors in Computing Systems, Seattle, WA, 2001.

[32] S. V. Suzuki and S. Yamada, "Persuasion through Overheard Communication by Life-like Agents," in IEEE/WIC/ACM International Conference on Intelligent Agent Techonolgy, Beijing, China, 2004.

[33] L. Sweeney, "Uniqueness of Simple Demographics in the U.S. Population," Carnegie Mellon University, Laboratory for International Data Privacy, Pittsburgh2000.

APPENDIX A: THE SCRIPT USED IN THE EXPERIMENT

Welcome to InfoSource Music Store! We are glad to have you here InfoSource has been assisting customers for the past 6 months in making a better selection of music that suites your preference.

I am an Intelligent Shopping Assistant in the InfoSource music store. My name is Alice Smith.

Please have a look at the CDs on display and enter the CD number of your choice.

[Depending on the CD chosen, participants were presented:]
Fearless is the second studio album by American country pop artist Taylor Swift, released on November 11, 2008.
It debuted at number one in the United States. Fearless has already been deemed one of the fastest selling country albums of all time.

Grand is the second album release from Brooklyn-based band Matt and Kim, recorded entirely in the Vermont home where Matt grew up. It was released on January 20, 2009.
Matt and Kim is a punk/dance duo formed in 2004.

Only by the Night is the fourth studio album by American rock band Kings of Leon, released worldwide in September 2008.
Only by the Night experienced commendable international commercial success and was the number-one album of 2008.
The single "Sex on Fire" came in at number one in the UK, Australia, and on the United States' Hot Modern Rock Tracks, and at number two in New Zealand.

The Fray is the second full-length studio album from piano rock band The Fray. It was released on February 3, 2009 in the United States.
Reviews range between very positive and very negative. Many reviews echoed the sentiment that the album was "nothing new," as put forth by Rolling Stone magazine.
Despite such reviews, The Fray still managed to debut at number 1 on the U.S. Billboard 200, dropping to number 4 by the next week.

No Line on the Horizon is the twelfth studio album by Irish rock band U2, released on 27 February 2009.
The band consists of Bono (vocals and guitar), The Edge (guitar, keyboards, and vocals), Adam Clayton (bass guitar) and Larry Mullen, Jr. (drums and percussion).

"Poker Face" is an electropop song by American pop singer-songwriter Lady Gaga from her debut album, *The Fame*.
Lady Gaga was born in Yonkers, New York and grew up in Manhattan, where she attended New York University's Tisch School of the Arts. At age 20, she began working for Interscope Records as a songwriter, penning songs for pop acts such as the Pussycat Dolls.

It's Not Me, It's You is the second studio album by British alternative singer-songwriter Lily Allen. It was released in the United Kingdom on February 9, 2009, and on February 10 in North America.
Lily Allen is well known for her Mockney style.
Reviewing for The Observer, Garry Mulholland awarded the album five out of five, calling this a "wonderful record".

Get Guilty is A.C. Newman's second solo album, released on January 20, 2009. The first single from the album is "The Palace at 4 AM."
Allan Carl Newman (born April 14, 1968) is a Canadian musician and songwriter. As well as being known for his solo work, A.C. Newman has been a member of bands such as Superconductor and The New Pornographers.

Do you want to watch a sample video from this Album?

Do you want to add this album to your Shopping Cart?

This is your shopping cart. Please Click on Go Shopping button to shop for music CDs. If you do not want to look for more CDs, you can directly click on Checkout button.

Thank you visiting InfoSource Music Store!

A.1 Reciprocity Condition

1. Birthday and Zodiac Signs

[*Participants were presented one of the following pieces of information before their birthday information was requested. A participant might browse multiple CDs and thus multiple pieces of information were provided, but their birthday information was only requested the first time.*]

CD 1. Country pop music album *Fearless* has its roots in soft pop which is usually popular with people born under the zodiac sign of Aquarius (born in between Jan 21 and Feb 19) as they are known to be sensitive, gentle and patient.

CD 2. Indie rock and alternative rock music such as Matt and Kim's *Grand* is usually popular with people born under the zodiac sign of Aries (born in between March 21 and April 19) as they are known to be adventurous, active and outgoing.

CD 3. The music for the album by Kings of Leon is one of a kind. The people who are born under the zodiac sign of Sagittarius (born in between November 22 and December 21) prefer this type of music because they too are fierce and independent.

CD 4. The Fray's pop rock and alternative style of music is usually popular with people born under the zodiac sign of Leo (born in between July 23 and August 22) as they are known to be dynamic, enthusiastic and full of energy.

CD 5. Rock music like *No line on the Horizon* is usually popular with people born under the zodiac sign of Scorpio (born in between October 23 and November 21) as their personalities are characterized by passion, desire and power.

CD 6. The pop dance music of Lady Gaga is usually popular with people born under the zodiac sign of Pisces (born in between February 19 and March 20) as they are known to be always in a dream world fantasizing about their lives.

CD 7. Electropop music as found on *The Fear* is usually popular with people born under the zodiac sign of Gemini (born in between May 21 and June 20) who are young at heart and variety is their spice of life.

CD 8. The music for the album *Get Guilty* is very original. The songs seem to be an obvious choice for people who are usually born under the zodiac sign of Capricorn (born in between December 22 and January 20) who always appreciate talent and creativity.

Question: What is your date of birth?

2. Email

Tune-Nation maintains a fan club website. The current screen shows one of the web pages. It can be viewed via your computer, a smart phone such as iPhone, or a handheld device such as iPod Touch. Unlike other fan club sites, our website focuses on new releases, customer ratings, and their recommendations. We will use your email addresses as your identification, while you specify your own display name to be displayed on the website. We will not send you any email unless you explicitly request it.

Question: Type your email address and your display name.

3. Monthly Income

At Tune-Nation, we seek to provide great customer satisfaction by accurately recommending songs and music CD albums that our customers are going to love. We are building a world class music genre recommendation system to bring you great value and accuracy. More than 75% of the customers like the CD albums that we suggested.

I would like to recommend another CD album for you.

Question: Select one of your favorite genres and tell me your monthly income.

Genres of the 8 CDs

Monthly income ranges: $0-$1000, $1000-$2000, $2000-$3000, $3000 or more

4. Phone Number

You may choose to maintain your purchase records within Tune-Nation. Any songs, CD albums, and movies that you purchase at Tune-Nation stores may be downloaded from Tune-Nation website to your smart phone or cell phone. Your phone number is your identification. You may switch to another phone number later. Remember Tune-Nation does not make any sales calls to the phone number that you provide.

Question: Provide your phone number to maintain your purchase records with Tune-Nation.

5. Home Address

Throughout the year, we mail coupons to our customers. You will save 20% - 30% on any regular or “on sale” music and video products in store or online. On your birthday, you will receive an exclusive 40% off coupon.

Question: What is your home address?

[SHOW A 40% OFF BIRTHDAY COUPON.]

A.2 Control condition

[While other experiences and software were the same (e.g., view sample videos, access CD related information), participants were requested for their identity information directly:]

1. **Birthday and Zodiac Signs**

Question: What is your date of birth?

2. **Email**

Question: Type your email address and your display name.

3. **Monthly Expenses**

Question: Select one of your favorite genres and tell me either your monthly income or your monthly expenses.

Genres of the 8 CDs

Monthly income ranges: $0-$1000, $1000-$2000, $2000-$3000, $3000 or more

Monthly expense ranges: $0-$1000, $1000-$2000, $2000-$3000, $3000 or more

4. **Phone Number**

Question: Provide your phone number to maintain your purchase records with Tune-Nation.

5. **Home Address**

Question: What is your home address?

APPENDIX B: THE SURVEY FEEDBACK QUESTIONS

Please select/enter following Demographic Information

1. Gender : Male/Female
2. Age
3. Ethnicity : White (Not Hispanic)/North American Indian or Alaskan Native/Pacific Islander/Asian-American/Asian/Hispanic/Black (Not Hispanic)/Other
4. UAH Email Address

Feedback on the recommendation agent Alice

1. InfoSource recommendation agent (Alice) was helpful : Strongly disagree/Disagree/Neutral/Agree/Strongly agree
2. Alice provides detailed information about the CD, sample video, age-wise and gender-wise sales information, zodiac signs. Do you like the interaction with Alice using text, voice, and video?
   Strongly disagree/Disagree/Neutral/Agree/Strongly agree
3. Which features do you like most? And which features do you dislike most?
4. Have you ever used any software or websites that have animated life-like agents (such as Alice in our application)? If so, please compare Alice to the other once that you used.
5. Did you pay attention to Alice's face? Did you feel it to be more interesting or did you get distracted during your shopping?

Feedback on the InfoSource Music Store Application

[Now we'd like for you to tell us a little about your shopping experience. Please use the scale below to make your ratings.]

Strongly disagree/Disagree/Neutral/Agree/Strongly agree

1. I was satisfied with the product options
2. It was easy to use the InfoSource technology while shopping
3. The shopping experience was realistic in terms of the product display
4. The shopping experience was realistic in terms of the product information that was available
5. I will use a handheld device or my cell phone as a handheld shopping assistant for my future shopping
6. I will use InfoSource technology for shopping in the near future

1. The messages prompted by the Identity Protection Software are helpful
2. I will use the Identity Protection Software technology to protect my privacy in the near future
3. Which suggestions that the Identity Protection Software made do you like most? And which suggestions do you dislike most?
4. What other privacy protection features do you hope the Identity Protection Software to provide?

Data provided

During the experiment, Alice asked you the following information. Please indicate if any of the following information that you provided was FALSE. You will NOT lose any Activity Points if you did falsify any of the information. So, please be honest with us from this point.

Name : Yes, I falsified Name ; No, I gave the Correct Information
If you have provided falsified Name, please tell us the reason.

Age: I gave the Correct Information. /I falsified Age after I read the message prompted by the Identity Protection Software.

Importance of the identity elements description

The following questions ask you to identify the type of information that you think are important to keep private. In this context, 'privacy' refers to information about yourself that you think should not be accessed without your consent or control.
Please indicate how important it is to keep each of the types of information private.

SCALE: Not at all Important/Minimally Important/Somewhat Important/Considerably Important/Extremely important

1. Gender
2. Date of Birth (month, day and year)
3. Birthday(month and day)
4. Age
5. Zip code
6. Home Address
7. Credit card number
8. Phone number
9. First name
10. First and Last name (in combination)

About Identity Protection Software

Gender : Yes, I falsified Gender /No, I gave the Correct Information

If you have provided falsified Gender, please tell us the reason.

Birthday: I gave the Correct Information./I falsified Birthday after I read the message prompted by the Identity Protection Software. /I would falsify Birthday even the Identity Protection Software did not display the message.

If you have provided falsified Birthday, please consider providing us the reason.

Zip Code: I gave the Correct Information./ I falsified Zip Code after I read the message prompted by the Identity Protection Software. / I would falsify Zip Code even the Identity Protection Software did not display the message.

If have provided falsified Zip Code, please consider providing us the reason.

Privacy concerns description

Please indicate how concerned you are about each of the following possible threats to your security. In this context, 'security' refers to a concern about someone or a company being able to potentially harm you (financially, socially or legally).

SCALE: Not at all/A little/Sometimes/Very concerned/Extremely concerned

1. A store, a company, or a website collects your private information
2. Price discrimination (offer best prices to VIP members)
3. Transfer or sale of your identity or private information to other companies
4. Identity theft
5. Knowing your financial situation

Actions taken to protect privacy and security

The following questions ask about the steps that you may or may not take to maintain your security. How often do you engage in the following behaviors?

SCALE: Never/Almost never/Sometimes/Frequently/Very often

1. Carefully read privacy policies
2. Reveal personal information on the Internet or filling out paper forms
3. Falsifying (lying) information about yourself on a website or paper forms
4. Revealing personal information if it will allow the provider to give you better service or price
5. Find out how a company or organization plans to use your identities or private information
6. Have multiple email accounts to protect privacy
7. Download security patches for your personal computer
8. Check credit card billing statements
9. Pay not to list your name in phone directories