ABSTRACT
As social media tends to get a more and more prominent place in our lives it is a growing source of potentially huge amount of money for entrepreneurs and investors. In order for entrepreneurs to make money they need to know how they can reach people’s information and turn it into money. This paper researches the potential of trading relevant information for the user in exchange for (some of) his privacy sensitive information. A web based game with Facebook integration was used to create an accessible way to measure the users willingness to give up privacy sensitive information. Under this assumption that users are willing to give up privacy sensitive information. Although few people played the game, a couple of interesting conclusions could be drawn. The main conclusion is once an application or service has the trust of a user he is willing to give somewhat all of his privacy sensitive information away. Based on the gathered knowledge on how users handle privacy sensitive information this paper proposes some new angles for research.

Keywords
Ubiquitous Computing, Privacy awareness, Rewarding, Facebook

1. INTRODUCTION
Recent studies have been conducted on the topic of privacy sensitive data that is generated by modern technology [2, 7, 11]. In these researches the main consideration is whether the tools businesses provide for preserving user privacy are sufficient. On the other hand there are studies which focus on the perspective of the user and research in what situations users are willing to give up privacy sensitive information [9, 11]. It is interesting to see that both types of research tend to be contradicting. First of all users take their privacy very seriously and they try to preserve it at all costs. On the other hand users are (un)willingly throwing major parts of their privacy out of the window just to get a little fun. This contradiction has been called The Privacy Paradox [11]. The United States government takes this contradiction very seriously, this resulted in a just recently released factsheet[5] that presents a Plan to Protect Privacy in the Internet Age. To understand how this contradiction works in practice it is important to understand the way a user thinks and acts during privacy decision making [1]. Privacy attitude is the way a user thinks about how he or a company should deal with his privacy. Privacy behavior is the way a user deals with his privacy [9]. These two should be in balance in order for a user to make the right decision, but in practice this is not the case, users are seemingly willing to trade their privacy for (short-term) benefits [6, 3]. This might be because of reward expectation a user has [4], the research in this paper will focus on this expectation to find the boundaries of privacy decision making. With the use of previous research and a cognitive user test it is tried to find out to what extend a user is willing to provide privacy sensitive information in exchange for a short-term reward.

2. DEFINITIONS
In this section the terms that will be used in the remainder of this paper are described.

User: A person who wants to preserve his privacy.
Reward: The information or any other kind of (digital) item a user can be rewarded with.
Privacy sensitive information: Any kind of information a user may consider too personal to share with everyone. For example his location.
Stakeholder: The company and/or an organization that has interest in obtaining privacy sensitive information from users.

3. PROBLEM STATEMENT
Nowadays many people have access to a smartphone. A smartphone is a probable source of valuable information for stakeholders since a smartphone contains multiple sensors like gps-, motion-, visual- and sound sensor. The value of the data provided by these sensors may increase when it is combined with the sensor data of other smartphones. Stakeholders have only one problem: how to obtain this privacy sensitive information? Reading literature provides basis to believe that smartphone users are willing to give up this information in exchange for a (short-term) reward. The reward given to a user may vary for every stakeholder and for every service since every stakeholder works in its own field of expertise.

3.1 Research Questions
In order for a stakeholder to find a fitting business model for obtaining privacy sensitive information this paper tries to answer the following research question:

- To what extent are users willing to give up privacy sensitive information in exchange for a reward?
The main research question will be answered with the help of the following sub questions:

- What does a user consider to be privacy sensitive information?
- What does a user consider to be a reward?
- Does a users’ view of privacy change when he is rewarded for giving up privacy sensitive information?

3.2 Hypothesis
The research is built on the following hypothesis:

- Privacy awareness of a user fades away at the moment he is rewarded for giving up privacy sensitive information.

3.3 Adding aspect
This research adds to the currently existing research because it gives practical answers to practical research questions. These answers can be used for developing new business plans or adapting to existing business plans. Developers may also benefit from the results since they can adapt their applications to the answers found. Besides that, this research aims to give a good overview of current research in this area.

4. RESEARCH METHOD
4.1 Methodology
The main research question addressed in this research is a question without one fixed answer which means the question can be answered differently by different persons. In order to be able to draw some conclusions, this research will use a cognitive test. Cognitive is a term originated from the field of psychology and refers to the mental activity of processing information, learning, remembering thinking, interpreting, problem-solving and making decisions. [12]. This last mental activity is the one to be researched. The cognitive test will consist of a website emulating a smartphone with an app that needs multiple Facebook permissions from the users account in order to play a short game. The game will consist of three versions, two test groups and a control group. The actual test groups will be asked if they want rewards to get a bonus in the game. The control group will not be asked for bonuses. After finishing the game a privacy related question will be asked to see whether the users privacy decision is affected by the bonuses. Before every test a few simple questions will be asked to the user like age, gender, education etc. If there is enough time left for the research after a week the entire test will be repeated with the same users but with a little extra. The second time the users will see a list of friends who participated the first time along with their scores. This second test can be seen as both a control and (when there are enough participants) as a second test, testing how group-pressure affects the users privacy decision making.

4.2 Pre Questionnaire
In the pre questionnaire a number of statements will be presented in three categories, see chapter A.1. ‘The first category is general info like age, education, gender etc. The second category is privacy. Privacy as defined by ‘the state of being alone, or the right to keep one’s personal matters and relationships secret’ [12] describes two parts: privacy for a person as it is and privacy for matters and relationships belonging to a person. The questionnaire addresses both topics. For example ‘I feel uncomfortable near nudist people’ is a clear example of a statement belonging to personal privacy. An example for the privacy on matter is the statement ‘At night I close the curtains.’. The third and last category presents statements on rewarding. These statements are divided in statements concerning when a user wants to receive a reward and in statements determining what a user considers to be a reward. For example the statement ‘As reward I prefer getting a shoulder pad instead of an envelope with money’ can be used to see what a user considers to be a reward. The answer of a user on the statement ‘I prefer buying my clothing on the Internet over buying them in a store’ can be used to tell something on the reward preferences of a user, direct or wait for it.

4.3 The Game
The game played by the users is a simple web game combined with privacy sensitive information obtained from Facebook. The users will play a game in which they control a small plane with the mouse through a corridor. (See figure 1.) The purpose of the game is to NOT hit the wall. To avoid the wall, the user must move the mouse from left to right to move the plane within the corridor. The longer the game is played, the narrower the corridor will get. Every second the player is alive, it will get an extra point, the more points the better. The game lasts for a maximum of 60 seconds. When the time limit is reached without hitting a wall, the user is offered a bonus in exchange for privacy sensitive information from Facebook in the form of a permission for the application to access Facebook data of the user. Every time when a new permission is asked, it will be a ‘higher’ permission which means that the more permissions asked, the more the privacy of the user will be neglected. After 10 rounds the game will be terminated and the total score will be saved.

4.3.1 ‘Higher’ permissions
To determine what a higher permission is, the Maslow pyramid[10] is used. (See figure 2.) This pyramid was created by Abraham Harold Maslow, chair of the psychology department at Brandeis. It represents the needs of a human being in a hierarchical manner. Everyone needs the lowest need and when it is met it needs the need above it. So the more needs are met the better a person feels. So the first permission asked will be from the lowest level of the pyramid and each consecutive permission will be one affiliated with a higher level from the pyramid. For this

![Figure 1. The corridor game](image-url)
research Facebook permissions are mapped to each level of the Pyramid of Maslow (see table 1) to be used in the game.

![The Pyramid of Maslow](image)

**Figure 2. The Pyramid of Maslow**

### Table 1. The Facebook permissions affiliated with each level of the Pyramid of Maslow

<table>
<thead>
<tr>
<th>Level</th>
<th>Permission 1</th>
<th>Permission 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Psychological desire</td>
<td>user_about_me</td>
<td></td>
</tr>
<tr>
<td>Safety and stability</td>
<td>user_status</td>
<td>user_likes</td>
</tr>
<tr>
<td>Social desire</td>
<td>user_activities</td>
<td>user_relationships</td>
</tr>
<tr>
<td>Self-esteem</td>
<td>user_work_history</td>
<td>read_stream</td>
</tr>
<tr>
<td>Self-realization</td>
<td>email</td>
<td>user_photos</td>
</tr>
</tbody>
</table>

### 4.3.2 Bonuses

Multiple bonuses can be ‘bought’ or obtained during the game with Facebook permissions. Each bonus has almost the same effect on the score, this has been tested by playing the game multiple times and calculating averages. In total there are four types of bonuses which can be categorized as follows: **Instant information** is a type of reward that gives information instantly to the user. In the game this means that the plane will fly at a slower speed so obstacles can be seen on forehand.

**Instant bonus** is a type of reward that has instant effect. In the game this means the user gets an head start with the score.

**Future information** is a type of reward that gives the user access to information it might use in the (near) future. In the game this means the user will get an extra life.

**Future bonus** is a type of reward that gives the user a bonus in the future. In the game this means that the end score is multiplied with 1.5. Since the user only sees the names of the bonuses and not the effect this is a good way to determine the real thinking process of a user. Research on the location sharing application foursquare has shown that privacy and games go well together and represent the real privacy considerations a person has [8].

### 4.3.3 Game version 1

Version 1 of the game works exactly as explained in the beginning of section 4.3 without any changes to the bonus system.

### 4.3.4 Game version 2

The game works the same as version 1 but now the permissions are not asked between every round but instead all permissions are asked at the beginning of the game. When the user denies the game, he will never be offered the opportunity of getting bonuses. This version is chosen to see if users think better of their permissions when they are confronted with all permissions at once in comparison to asking every permission separately.

### 4.3.5 Game version 3 - control

This version of the game works the same as version 1 with the difference that no permission will be asked. The game will be played without asking permissions but with giving the opportunity to use bonuses. This version is chosen as control to see if a user’s privacy view on privacy changes after playing the game without having to think about permissions.

### 4.4 Post Questionnaire

After the game some final statements will be presented on how the game influenced the privacy awareness of the user, see chapter A.2. For example the statement ‘With the introduction of Internet, people’s privacy is endangered’ lets the user think of his general opinion towards privacy. Besides that a statement like ‘I put all my holiday pictures online’ lets the user think of his real opinion towards his own privacy. At last the questionnaire ends with the question ‘What is the answer to the sum?’ This sum was presented at the beginning of the game entirely below the privacy statement to see how many people read the statement.

### 5. RESULTS COGNITIVE TEST

Before the results can be discussed and conclusions can be drawn, it is good to look at some facts. Figure 3 shows the amount of users leaving or moving to the next part of the research. It is notable that only 11 of the original 54 users finished the entire research, later on in this chapter some reasons for this are given. The average age of all

![The flow of users during the research](image)

1All of the users were invited by email and Facebook to join the research.
participating users is 25.6 years, out of which 12 users are in secondary education and 34 users are in or finished higher education. From the 11 people who finished the entire research, 6 of them played game version 1, 2 played game version 2 and the remaining 3 were in the control group and played game version 3. In total these 11 users obtained 69 high scores. Noticeable is the distribution of used bonuses, see Table 2. Of these 11 users 5 people read the entire privacy statement because they remembered the answer to the sum written below the statement.

Table 2. The distribution of used bonuses on achieving a high score.

<table>
<thead>
<tr>
<th>Bonus type</th>
<th>Nr of times used</th>
</tr>
</thead>
<tbody>
<tr>
<td>No bonus</td>
<td>29</td>
</tr>
<tr>
<td>Instant information</td>
<td>4</td>
</tr>
<tr>
<td>Instant bonus</td>
<td>0</td>
</tr>
<tr>
<td>Future information</td>
<td>5</td>
</tr>
<tr>
<td>Future bonus</td>
<td>31</td>
</tr>
</tbody>
</table>

5.1 Results

Since approximately 75% (Figure 3) of the users did not finish the entire game the gathered data is not entirely relevant to answer all of the research questions. On the other hand the results that are gathered do say something about the users who entered the research. Since most users did fill in the pre questionnaire and left upon starting the game it is good to find out why they did not even start the game. The reasons behind this are explained in the next section. The remainder of this chapter will discuss the results of the pre questionnaire, the game and the post questionnaire.

5.1.1 Reasons to leave the game

To find out what reasons are behind the decision to leave the game, a small interview has taken place with a couple of users who left the research before starting the game. A couple of the people who were spoken to explained that they simply did not have a Facebook account. The second most heard argument was, although the invitation email clearly stated that no information will be stored from or posted on Facebook, they did not want to take the risk of the application posting on their behalf. The proposition of changing the privacy statement at the beginning of the game would not change their opinion, they said. They argued that no-one ever reads the privacy statement anyways. Upon asking them if they allow other applications from Facebook on their account they say they do not allow it. The only applications they do allow are websites with a login system based on Facebook that do not need any personal information from the user.

In the chapter Improvements some improvements on this research are proposed in order to gather better results.

5.1.2 Results Pre Questionnaire

As explained before many users left before entering the game, so it is interesting to look at the answers those users gave on the first questionnaire opposed to the answers of the people who did finish the game. To find interesting answers, an average per statement was calculated for the users who did and on the users who did not finish the game. This is possible because all the statements were rated in terms of relevance from 1 to 5 by the users. Almost half (9) of the 21 statements were, on average, answered the same for both groups. It is notable that 7 of those 9 statements were concerned with privacy, so only 2 are on rewarding. The statements with the biggest differences are shown in the top half of Table 3 and the statements both groups agreed upon the most are listed in the bottom half of Table 3. Another difference between the groups is the average age. The group of people who did play the game have an average age of 21.4. The group of users who did not play the game have an average age of 26.8. The reason for this is that some older people in this group (50, 60, 75) do not have a Facebook account, enlarging the group of non-players and raising the average age significantly.

Based on the results of Table 3, the conclusion may be drawn that people who do not want to connect their Facebook account to the game have more affiliation with computer electronics since they are more likely to buy apps on their smartphone and are more influenced by social media to respond to a friend expressed by a family member. Also they get less stressed by websites and games that ask for money for access to extra features. A possible explanation for them leaving the game is as follows: Due to this affiliation with computer electronics the user is also more aware of the risk on giving privacy sensitive information away on the Internet. This awareness makes them cautious about playing the game, resulting in the decision to leave the game. This idea is supported by the interviews held with users who left the game early. Contradicting to this idea is that on average the users who did play the game are half an hour more online per day: 7.2 hours compared to 6.7 hours. But users who have more awareness also have more electronic devices on average: 2.4 compared to 2.2 devices. As it can be seen from Table 4 more male users left without playing the game than female users. So following the previous stated idea, male users have a higher affiliation with computer electronics.

<table>
<thead>
<tr>
<th>With2</th>
<th>Without2</th>
<th>Difference</th>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.38</td>
<td>2.18</td>
<td>0.80</td>
<td>Sometimes I buy apps for my smartphone.</td>
</tr>
<tr>
<td>3.75</td>
<td>3.03</td>
<td>0.72</td>
<td>If I would get a friend book I would fill it in directly.</td>
</tr>
<tr>
<td>3.75</td>
<td>3.21</td>
<td>0.54</td>
<td>I feel uncomfortable near nudist people.</td>
</tr>
<tr>
<td>2.25</td>
<td>2.64</td>
<td>0.39</td>
<td>Through the use of social media I offer my help quicker to help my friends or family.</td>
</tr>
<tr>
<td>3.75</td>
<td>3.39</td>
<td>0.36</td>
<td>I get annoyed by websites/games that ask for my money in return for extra items / information / features.</td>
</tr>
<tr>
<td>3</td>
<td>2.76</td>
<td>0.24</td>
<td>As reward I prefer getting a shoulder pad instead of an envelope with money.</td>
</tr>
<tr>
<td>2.09</td>
<td>0.09</td>
<td>2</td>
<td>On the Internet I do not search longer than 15 minutes for information.</td>
</tr>
<tr>
<td>2.61</td>
<td>2.63</td>
<td>0.02</td>
<td>If I help someone I expect that person to help me some time.</td>
</tr>
</tbody>
</table>

5.1.3 Results Game

Although the game was not played more than 11 times, there are still some interesting details to point out. First of all, all 11 players played the entire game not stopping at any moment. This is possible because all the statements were rated in terms of relevance from 1 to 5 by the users. Almost half (9) of the 21 statements were, on average, answered the same for both groups. It is notable that 7 of those 9 statements were concerned with privacy, so only 2 are on rewarding. The statements with the biggest differences are shown in the top half of Table 3 and the statements both groups agreed upon the most are listed in the bottom half of Table 3. Another difference between the groups is the average age. The group of people who did play the game have an average age of 21.4. The group of users who did not play the game have an average age of 26.8. The reason for this is that some older people in this group (50, 60, 75) do not have a Facebook account, enlarging the group of non-players and raising the average age significantly.

Based on the results of Table 3, the conclusion may be drawn that people who do not want to connect their Facebook account to the game have more affiliation with computer electronics since they are more likely to buy apps on their smartphone and are more influenced by social media to respond to a friend expressed by a family member. Also they get less stressed by websites and games that ask for money for access to extra features. A possible explanation for them leaving the game is as follows: Due to this affiliation with computer electronics the user is also more aware of the risk on giving privacy sensitive information away on the Internet. This awareness makes them cautious about playing the game, resulting in the decision to leave the game. This idea is supported by the interviews held with users who left the game early. Contradicting to this idea is that on average the users who did play the game are half an hour more online per day: 7.2 hours compared to 6.7 hours. But users who have more awareness also have more electronic devices on average: 2.4 compared to 2.2 devices. As it can be seen from Table 4 more male users left without playing the game than female users. So following the previous stated idea, male users have a higher affiliation with computer electronics.

2Users who finished with or without playing the game.
at any permission request. This can be interpreted as follows: users who are willing to accept permissions do not care on what permission is asked as long as they get what they want. Secondly it is notable that the users achieved 6.3 high scores on average. It would be interesting to see if this average stays the same, the more people play the game and what effect the bonuses have on this number. Unfortunately there is not enough data available to make any conclusions like this. Since the 11 users granted all permissions it is not possible to look at differences in age in connection with permissions granted or what game version achieves more permissions.

5.1.4 Results Post Questionnaire

From the post questionnaire it is interesting to see what the people think of privacy after they have played the game. It is very clear what the users think of privacy on the Internet, they all say Internet is a threat to privacy (on average 3.91) and they also consider themselves to be cautious with their own information (on average 3.91). For example they are very explicit on not uploading all their holiday pictures onto social media (1.55). During informal interviews with some of the users it became clear that in reality they do upload most holiday pictures but they could not explain why their vision on paper is different than their vision in reality. The most probable cause of this, one user said, is that you feel safe with all your friends on social media so you just upload your photos without regard of what happens with the photos.

6. CONCLUSIONS

6.1 Research Questions

All conclusions are answered per research question, starting with the sub questions before answering the main research question.

What does a user consider to be a reward?
It is difficult to give a closing answer to this question but based on the used bonuses during the game (See Table 2) it can be concluded that users like a good bonus they have to wait for a little time but know will be worth it.

Does a user’s view of privacy change when he is rewarded for giving up privacy sensitive information?
The answer to this question is interesting since all 11 users in the post questionnaire say his view has not changed, but in the meanwhile all of them gave up their information on Facebook. So the conclusion, based on the few evidence that is available, is: Yes the user is less careful once it has started to give away his information but not before he has given any information.

What does a user consider to be privacy sensitive information?

The research was designed to answer this question based on the permissions a user was willing to give. But since all users who entered the game accepted all privileges it can be concluded that a user does not have privacy sensitive information. On the other hand 75% (See Figure 3.) of the users did not even start the game so in that way it can be concluded that all information, even once given name, is privacy sensitive.

Main question: To what extent are users willing to give up privacy sensitive information in exchange for a reward? Like the conclusion on the previous research questions a user is willing to give quite a lot of information in exchange for a reward but only as long as the user is willing to give anything at all. As heard in the interviews, if people do not fully trust an application or website they will not give anything. Based on the presented results it is not clear whether the reward is a relevant factor at all if a application or website isn’t trusted.

Hypothesis: Privacy awareness of a user fades away at the moment he is rewarded for giving up privacy sensitive information. The hypothesis as proposed cannot be accepted nor can it be rejected based on the gathered results. More data must be provided to draw any conclusion. But based on the results that are gathered during this research it is more likely that the hypothesis will be rejected on the basis of 75% of the users thinking carefully before giving up any information.

6.2 Improvements

When improvements are made to the research the researcher should consider very well on how he is going to test privacy in a way people are more like to participate in because it is clear that the current approach did not have the desired effect. If a similar type of research is conducted next time, it is important to add a form in which users can tell why they left the research. This way the results can better be filtered on people who do not have a Facebook account for example. Somehow a larger group of people should be reached so more people can participate in the research. The corridor game is under the current conditions not sufficient enough to draw conclusions of meaning, it can be considered to change the game to give conclusions with few responses.

6.3 Future work

A point of interest is researching what a user considers to be a reward and if this reward is of relevance upon deciding to give up privacy sensitive information. It is also interesting to look at what users consider private information on social media and what they consider private information in real life, since the post questionnaire showed that these visions are not entirely lined up.

7. REFERENCES


APPENDIX

A. STATEMENTS

All the statements are in Dutch as they were shown to the user.

A.1 Pre Questionnaire

- Ik erger mij aan nudisten.
- Ik vind dat ik het recht heb om geen last te hebben van wat andere mensen vinden.
- Ik heb het nodig dat mensen tegen mij zeggen dat ik iets goed doe.
- Door het gebruik van sociale media geef ik sneller hulp aan vrienden of familie.
- Tijdens mijn vakantie ga ik naar een rustige plek.
- Als ik overwerk wil ik meteen geld zien.
- ’s Avonds doe ik de gordijnen in de woonkamer dicht.
- Als iemand mij helpt verwacht ik dat hij/zij ook iets voor mij doet.
- Ik vind het gebruik van sociale media noodzakelijk om in contact te blijven met vrienden.
- Het gebruik van internet heeft mijn sociale leven beëindigd.
- Als ik overwerk wil ik dat later om kunnen zetten in vakantiedagen.
- Door het gebruik van sociale media geven vrienden mij sneller hulp aan vrienden of familie.
- Wanneer iemand mij helpt wil ik graag iets terug doen.
- Ik koop mijn kleren liever in de winkel dan op internet.
- Mijn vrienden zien al mijn vakantiefoto’s.
- Op internet zoek ik niet langer dan een kwartier naar informatie.
- Zodra ik de weg niet kan vinden vraag ik deze gelijk aan anderen.
- Ik koop weleens apps op mijn smartphone voor geld.
- Ik erger me aan websites/spellen die geld vragen voor extra spullen/informatie/mogelijkheden.
- Als beloning ontvang ik liever een schouderklopje dan een envelop met geld.
- Als ik weer een vriendenboekje zou krijgen zou ik die gelijk invullen.

A.2 Post Questionnaire

- Met het internet is de privacy van mensen in gevaar gekomen.
- Al mijn vakantiefoto’s zet ik op sociale media websites.
- Ik vind het niet erg dat mensen aan mijn foto’s kunnen zien waar ik op vakantie ben geweest.
- Ik zet graag een bonus in wanneer dit mij wat kost om mijn resultaten te verbeteren.