NTNU
Norwegian University of
Science and Technology

Privacy in Location aware Systems for Social Interaction

Per Anton Gransæther

Master of Science in Computer Science
Submission date: June 2008
Supervisor: John Krogstie, IDI
Co-supervisor: Anders Kofod-Petersen, IDI

Norwegian University of Science and Technology
Department of Computer and Information Science

Problem Description

One of the main assumptions in both the current trend in digital social interaction, such as instant messaging, linkin and Facebook is that users gain something beneficial without loosing, among others privacy. The ability to be always available is of particular interest in the emerging fields of Pervasive Computing and Ambient Intelligence.

This project aims at investigating how users' social interaction is affected when mediated by technology that allows users to be constantly available. We aim at investigating this by implementing a simple context sensitive messaging service in the Wireless Trondheim environment, and do empirical testing with a population of students equipped with wireless devices and the developed application.

Assignment given: 15. January 2008
Supervisor: John Krogstie, IDI

Abstract

Social network services like Facebook, and instant messaging services like MSN Messenger have gained an enormous popularity in just a few years, and are undoubtedly popular among users. What happens when these networks are combined with information about the user's location?

This master's thesis has investigated if people are willing to use systems that share the users' location for the purpose of locating friends. It is also investigated if users' of systems that shares their location behave in a different ways as a consequence of this location sharing. Finally, this thesis investigated if users of location sharing systems will get the feeling of loosing their personal privacy, and how privacy mechanisms can help the users not to get this feeling.

These questions were investigated by developing a location-tracking social network service called The FriendRadar, which was developed for usage in Wireless Trondheim. Pupils from Trondheim Katedralskole were equipped with wireless devices to test the system in the environment. The logged data of the system was analysed and the users answered a questionnaire after the test period was completed. One user also participated in an interview.

The results of these investigations show that the users did not use The FriendRadar very much, but according to the users answer to the questionnaire it seems that users are willing to use systems that share their location with others, if the benefit is that they can locate them back. It also indicates that the users do act in different ways because of the possibility to share their location. Users seem to use the fact that others can see their location deliberately to tell other their locations, but they do not avoid doing any actions. Further, it seems like spontaneous actions possibly can happen as a consequence of users seeing other's location. Users of the system did not show concerns about privacy while using the system, but they could imagine this being a problem in a system with larger user mass. The most important privacy mechanisms for a future location-tracking systems, seems to be able to turn the system off and reciprocity in location sharing.

Together these results shows that if the right amount of privacy mechanisms are implemented to a location-tracking system, the system can both be privacy preserving and useful for the users.

Preface

This master's thesis is the completion of my Master of Science degree at the at the Information Systems Group of the Department of Computer and Information Science (IDI) at the Norwegian University of Science and Technology (NTNU).

I would like to thank my co-supervisor Anders Kofod-Petersen who has been of great help throughout the work with this master's thesis. Supervisor John Krogstie has also always contributed when needed. Fellow student Gunhild Giff Bye deserves thanks for the cooperation with the development of the systems and other research. Accenture must also be mentioned, for lending me the laptop computer this master's thesis was written on.

Finally, I would like to thank teacher Aslak Bjerkvik and his pupils at Trondheim Katedralskole for participating as test persons. Their cooperation made the experiment easy to perform.

Trondheim 10. June 2008

Per Anton Gransæther

Table of contents

List of figures

List of Tables

1 Introduction

This introduction first presents the background and the motivation for this master's thesis followed by the report outline.

1.1 Background and motivation

Social network services on the Internet, such as Facebook and MSN have gained enormous popularity in the later years. As new technology makes it possible to cover entire cities with wireless Internet access and as mobile devices such as mobile phones that can exploit these wireless networks become more widespread, such social network services will naturally migrate to mobile devices. These services will probably include some context sensitive information, with the users' location as the most interesting. This will make the users of social network services more available to each other than ever before. This makes it interesting to investigate how users and their social groups react to an environment where the users' position is constantly available to the other users. It is also interesting to see if people really want to use applications that reveal their position to friends and family. Another important aspect with services where users can locate each other is how users feel about their own personal privacy in such services, and how privacy mechanisms can help users keep their personal privacy.

This master's thesis is a continuation on a project written in the autumn of 2007 which investigated the same questions as this master's thesis. The questions was investigated using *FindMyFriends*, which was a system implemented on the student house *Samfundet* in Trondheim. The users of FindMyFriends were able to locate friends currently being on Samfundet. The study indicates that users behave in a different way as a consequence of that they can see the location of their friends. To some extent they also behave different because they know that others possibly know where they are located. Further, the study proposes that people are not too concerned about privacy in FindMyFriends, but that this probably will be a much larger problem in a system used in a city environment. Following this, it is clear that some privacy mechanisms are absolutely necessary for the system to be useful for the users. The most important mechanisms pointed out in the study, is the possibility to turn the system on and off, preferably in a way that offers the users plausible deniability. The study further indicates that people seems to be interested in using a system that have functionality for locating friends in Wireless Trondheim.

1.2 Report outline

This master's thesis is divided in eight chapters and three appendices.

Chapter 1 – Introduction
This chapter presents an introduction to the study, including background and motivation and the report outline

Chapter 2 – Research agenda
The research agenda presents the research questions and the research methods used to investigate these questions.

Chapter 3 – State of the art
This chapter presents an introduction to social network services, ubiquitous computing, behaviour patterns in location based systems, privacy in P3 systems and social networks services, Wireless Trondheim and existing systems that have similar functionality as The FriendRadar.

Chapter 4 – Preliminary study
The preliminary study presents the study made on FindMyFriends during the autumn 2007.

Chapter 5 – Design and implementation
This chapter presents how The FriendRadar are designed and implemented and which privacy mechanisms that are implemented in the system.

Chapter 6 – Results
This chapter presents the results from the analysis of the usage of The FriendRadar, the questionnaire and the interview.

Chapter 7 – Discussion
The discussion presents a discussion of how the research was planned followed by a discussion of the research questions. Finally, threats to validity are discussed.

Chapter 8 – Conclusions and further work
This chapter presents a conclusion to the research questions followed by possible further work following this master's thesis.

2 Research agenda

The research agenda describes the research questions investigated through the project followed by the preparations made before the test period. Finally, the research methods used to answer the research questions are presented.

2.1 Research questions

Based upon the background and motivation and the problem definition, the following research questions will be examined through this project:

RQ-1: *Are people willing to use a system with functionality for locating and interacting with their friends and family using a mobile device connected to a wireless network?*

RQ-2: *Will users of a system with functionality for locating other users behave in a different way than they normally would?*

- RQ-2.1: *Will a user who knows the location of other users behave in a different way than she normally would?*
- RQ-2.2: *Will a user who knows that other users can know her location behave in a different way than she normally would?*

RQ-3: *Do the users of social interaction systems that share context sensitive information like location feel they are loosing their own personal privacy?*

RQ-4: *How can privacy mechanisms be used to help the users of context sensitive systems for social interaction not to loose their personal privacy?*

2.2 Preparations

This section will present the necessary preparation that was done before the test period could start.

The most important preparation of the test period was of course to implement the system The FriendRadar, called 'Venneradaren' in Norwegian. The system is implemented for this experiment only, and therefore it could be tailor made to fit the needs of the experiment. The design and implementation of The FriendRadar is described in Chapter 5.

The experiment with The FriendRadar was coordinated with another student, which also needed test subjects equipped with mobile devices connected to Wireless Trondheim. Several options were discussed when deciding which persons to pick as test users. The first option on the table was to use students from NTNU to test the system. But this option was pretty early rejected, because both the campuses of NTNU are located outside the coverage of Wireless Trondheim. This would probably lead to that the test users rarely would be given the opportunity to use the system connected to Wireless Trondheim. In addition, he NTNU students cannot connect to Wireless Trondheim without having a VPN client installed on their computer, which are not possible on the iPod Touch. When the student option disappeared, they most preferable option was to use gymnasium pupils (16 to 19 years old) from a school located in downtown Trondheim, inside the coverage area of Wireless Trondheim. All the employees of the municipality of Trondheim and pupils of the schools in Trondheim have free access to Wireless Trondheim, and are therefore ideal test persons. An e-mail was sent to the headmaster of Trondheim Katedralskole (Trondheim Cathedral School), which is located inside the coverage area. They had a subject that was meant for pupils interested in research, especially inside scientific studies consisting of pupils from Trondheim Katedralskole and Adolf Øien school, which is also located within the coverage area. The teacher of this subject (Aslak Bjerkvik) answered and said he would be interested in us using his pupils in the testing, as the research methods was of relevance for his subject.

The mobile devices chosen to perform the testing on were Apple's iPod Touch. This device was chosen in co-operation with the co-supervisor and the other master student that would use them. The most important requirement for the device that would be used in the testing was that it was possible to connect to a Wi-Fi network (Wireless Trondheim). The iPod was chosen in competition with mobile phones mainly because of its price, as they cost about half the price of a mobile phone with the same specifications. Its large screen size (3.5 inch touch-screen) was also an important factor when deciding for the iPod. Finally, the 'fanciness' of the device and the iPods' general popularity among youths, made it easy to choose this device. The cheapest version was chosen, which have 8GB hard drive. More about the specifications of the iPod Touch can be read at Apples homepage[1].

At the end of the development period six employees and students from The Department of Computer and Information Science at NTNU was equipped with an iPod each and registered in The FriendRadar. They were released inside the coverage area of Wireless Trondheim to test The FriendRadar, the positioning functionality, the iPods and the robustness of Wireless Trondheim. The testing lasted about an hour with test persons both sitting still, walking around and moving around with both bike and car.

Before the real testing could start, a user profile was created for each device, where the username was the name of each device (which was printed on a sticker on each device). Each user profile was connected with the relevant device's MAC-address, so the test users did not have to do this cumbersome work themselves. The test period started on Wednesday 23rd of April 2008, with a presentation of the experiment and The FriendRadar for the test users. After this presentation the users was handed the iPods together with a user guide, presented in Appendix C. The test users was told that they could use the iPod to whatever they wanted and that they were free to choose how much they wanted to use The FriendRadar, to get as much realism as possible.

The test period lasted for four weeks, and was completed Thursday 22nd of May 2008, when the information about the questionnaire was sent out to the pupils.

2.3 Research methods

This section will present the research methods that will be used to investigate the research question presented in the previous section.

2.3.1 Analysis of recorded data

This section will present which data that is logged by The FriendRadar, and how this data is analysed.

To make it possible to analyse the users' movements, the users' location was saved in the database every time a user gets located. A user was located every 30 seconds if she moved around and every two and a half minute if the user was at the same place. If the user was not connected to Wireless Trondheim, the system still checked the user's location every hour, in case the user would connect to Wireless Trondheim and not log into the system. The system also automatically saved each message that was sent, with a timestamp. This makes it possible to retrieve the location of the sender and the receiver when the message is sent. The content of the message was separated by the message information as shown in Figure 5.2, which is the database model of the system, to keep the user's privacy. Each message had to be marked with a tag by the sender that states what kind of message it is. The possible tags to choose among are shown in Table 2.1.

[1] http://www.apple.com/ipodtouch/specs.html

Table 2.1: Message tags

Tag	Description
inform	Information
request	Request
proposal	Proposal
confirm	Confirmation (only if answer to inform)
pos_answer	Positive answer (only if answer to request)
neg_answer	Negative answer (only if answer to request)
neu_answer	Neutral answer (only if answer to request)
accept_proposal	Accept proposal (only if answer to proposal)
reject_proposal	Reject proposal (only if answer to proposal)
not_understood	Not understood

All the data was recorded in a way that makes it unnecessary for the analyser of the data to couple actual users to the actions recorded. Each user will be identified with the help of an avatar, and not their actual names. This makes it possible to identify specific users in the data without knowing who they actually are.

The recorded data will be used to see how the behaviour of the users is affected by actions by other users of the system. The data will make it possible to see if an action performed by a user affects the actions of other users. For instance if user A sends a message to user B, it is naturally to assume that user B will answer with another action. This can be controlled using the recorded data.

2.3.2 Observational study

An observational study was planned, where one or two users would be followed for a couple of hours to see how they used the system. As it become apparent that the users did not use the system very much, the field study was cancelled.

2.3.3 Questionnaire

When the test period was completed, the test persons' teacher was asked to send out information about an online-questionnaire about the two systems (The FriendRadar and the other student's @School) the pupils had been testing. The questionnaire consisted of three parts. First, a part where the participants was asked general questions that was interesting for both systems and that together made a set of background information about the users. The second part consisted of questions about The FriendRadar. The questions of this part were developed with this master's thesis's research questions as background. Table 2.2 shows which research questions each question in the questionnaire are based on. Some questions are relevant for two or more research questions, but are in the table connected with the research question it is most relevant for. The questions of the two first parts of the questionnaire are presented in Appendix A – The questionnaire. The questionnaire was written in Norwegian, and the questions are therefore translated to English. The third and final part of the questionnaire consisted of questions relevant to the other system, and are not a part of this master's thesis.

Table 2.2: Connection between research questions and questions on the questionnaire

Research question	Questions from questionnaire
Background information	1-21
RQ1	22, 23, 25-32, 49-52, 57
RQ2.1	33-38
RQ2.2	41-44
RQ3	40, 46-48, 53-54
RQ4	24, 45, 46, 55, 56, 58, 59

The usages of an online questionnaire, which is classified as a self-administrated survey, have both advantages and disadvantages (Robson 2002). Advantages of a self-administrated survey is that they are a very easy way of retrieving information from a large set of people, and it is an efficient way of getting a large amount of data at low cost and in a short period of time. Further, an online questionnaire preserves the anonymity of the participants, which encourages a high level of frankness. Some disadvantages are that data are affected by the participants' memory, experience, motivation and personality, the questionnaire might suffer from a low response rate and the sample may not be representative. Further, it can be very difficult to see if the questions are ambiguous, and misunderstandings of the question may not be noticed. Finally, the participants may not answer the questions seriously, which is also difficult to detect (Robson 2002).

The questionnaire was produced with consideration to the disadvantages of this type of survey. To reduce the problem of low sample rate, the questionnaire was tried to be made as short as possible with short and simple questions. The two projects (this and @School) questions was merged into one questionnaire, such as the users only had to answer one questionnaire. As a consequence, the questionnaire became longer, but in total the users had to answer fewer questions because both questionnaires had some similar questions. In the e-mail the teacher sent to the pupils, it was explained that the questionnaire would take maximum ten minutes to complete. It was also explained that a gift coupon (300 NOK) would be given to one lucky winner among the respondents. The questionnaire was open for five days (22nd May to 26th May), and a reminder e-mail was sent near the end of the period. To avoid the rest of the disadvantages, some simple rules taken from Robson (2002) were followed. The language of the questions was simple, the questions were short and great care was taken with sentence structure to remove ambiguity. Leading questions and double-barrelled questions; questions that ask two questions at once, were tried to be avoided. The response alternatives was produced with care, as they were tried to be made accurate, exhaustive, mutually exclusive and kept in a single dimension (Robson 2002).

2.3.4 Interview

Interview was chosen to add more depth to the results from the questionnaire. In the e-mail the teacher sent out to his pupils about the questionnaire, he also asked if any of them could be interviewed about The FriendRadar. It was explained that it only would take about 20 minutes, that the interview was totally anonymous and that the interview would take place at their school. Two of the pupils answered that they would be interviewed. The interviews were scheduled at their school during a school period with ten minutes interval between the interviewees on 27th of May 2008. The second interviewee did never show up, so only one of them was interviewed. The interview was voice-recorded, and the purpose of the interview and the interviewee's anonymity was carefully described before the interview started.

The interviews followed the semi-structured form described in Oates (2006). This means that a template is followed, but the interviewer can rearrange the order of the questions depending on how the conversation develops, and new questions can be added when interesting subjects arise. The template followed in the interviews is presented in Appendix B. The questions asked in the interview are produced with the research questions presented above in mind. Great care was also taken in making the questions in such a way that complements the answers from the questionnaire.

Interviews as a research method has several advantages and disadvantages as described in Oates (2006). The main advantage is that they are good at dealing with topics in depth and detail. Some other advantages is that little equipment is needed and the researcher can check if the person answering is the right one for answering the questions and they have a flexible form. Disadvantages mentioned are that interviews are time consuming for the researcher and interviews requires good social skills from the researcher. The setting is artificial and the interviewees know they are speaking for the record, and a false impression can be given from that. There is also a possibility

that they can be misleading because the participants only say what they remember and think they did, which not always corresponds with reality. In this case however the most interesting part is what the participants think, and not what they did. Therefore this is more of an advantage than a disadvantage.

3 State of the art

The State of the art will start by describing social network services followed by a description of ubiquitous computing. Further, relevant literature about the behaviour of users in location-based services and privacy in P3 systems and social network services are presented. Finally, the environment of Wireless Trondheim is presented followed by a presentation of similar systems as The FriendRadar. Some parts of this chapter is retrieved form the preliminary study, as these two studies treats the same topics. This master's thesis presents the topics both deeper and broader than the preliminary study, however.

3.1 Social network services

Web 2.0 is the second generation of the World Wide Web. The main difference from early web sites to Web 2.0 are that user participation is emphasised using dynamic websites, instead of just using the web as a tool to publish static content. User can not only download and read information from the web, they can also publish and upload text, pictures, videos and etcetera to the web (O'Reilly 2005). Examples of Web 2.0 services are social network services like Facebook and wikis like Wikipedia.

Social network services have reached an enormous popularity the last couple of years. Examples of such networks are Facebook[2], MySpace[3], LinkedIn[4] and Last.fm[5] together with hundreds of others[6]. Common for all these networks are that users can search for other users and connect to them as friends or contacts. Often the networks offer some kind of media sharing among friends.

According to statistics presented on the Facebook website, Facebook have more that 70 million active users. Up to 2008, an average of 250,000 new users registers every day, and the number of users was doubled every 6 months. It is the sixth-most trafficked site in the United States. Facebook is the number one photo sharing application on the web with 14 millions photos uploaded daily. These statistics give some indication of the massive popularity such networks has.

3.2 Ubiquitous Computing

This section will first introduce the concepts of ubiquitous computing and ambient intelligence followed by a description of what context means in ubiquitous computing.

3.2.1 Ubiquitous Computing and Ambient Intelligence

The term *Ubiquitous Computing* was introduced by Mark Weiser early in the 1990s. The term literally means computers that are everywhere, which are very describing. In *"Hot-topics: Ubiquitous Computing"* (Weiser 1993), he describes ubiquitous computing as a network of fully connected devices which make information available to the user, virtually invisible, in the everyday visible world. He describes a world where you do not need to carry a PDA, since all the information you need will be available on devices in the physical environment surrounding you. He further imagines that a normal office in the future will have hundreds of little displays, replacing post-it notes, working papers, wall posting and so on (Weiser 1993). Weiser's vision has not yet fully come true, but the term ubiquitous computing is fully alive. Ubiquitous computing covers a wide spectre of computers embedded in everyday devices (cars, refrigerators etc.), but also mobile computers

[2] http://facebook.com
[3] http://myspace.com
[4] http://linkedin.com
[5] http://last.fm
[6] See a list at http://en.wikipedia.org/wiki/Social_network_service

like mobile phones and mp3 players connected with wireless networks. Internet has become an important part of ubiquitous computing as it is the network that connects these computers together.

Ubiquitous computing, pervasive computing and ambient intelligence have often been used synonymously. One can say that pervasive and ubiquitous computing actually are synonyms. For instance, if you search for 'Pervasive computing' on Wikipedia, you are automatically redirected to the article about ubiquitous computing. Ambient intelligence however, refers to an environment where ubiquitous computing is implemented. The environment consists of a number of embedded, therefore hidden computers that are sensitive, adaptive and responsive to the presence of people and objects in the environment. This environment assists the user in performing her activities in a non-explicit and smart way. While utilizing the information from the environment, privacy, security and trustworthiness are preserved (Weber, Rabaey et al. 2005).

3.2.2 Context in Ubiquitous Computing

Context in ubiquitous computing is the situation the user is in when she interacts with the computer. The context can consist of information about the position, the identity and the state of people, groups, computer devices and physical objects. Context is often used for devices to make decisions for a user depending on the situation the user and her device find themselves in (Dey, Abowd et al. 2001). In the case of The FriendRadar, the important context information is the position of the user.

Location-based services (LBS) are "*any service that takes into account the geographical location of an entity*" (Junglas and Watson 2008). An entity is either human or non-human. It is distinguished between location-tracking services and position-aware services. Location-tracking services give information about a user's location to other entities using the system. Position-aware services on the other hand, are aware of the user's location, but do not share it to other entities. It simply uses the knowledge of the user's location to provide the user with useful information concerning this particular location. The FriendRadar and FindMyFriends are typical location tracking services, and a service providing tourist information automatically to a user depending on her location is a typical position-aware service.

Systems that link people-to-people-to-geographical-places are called P3 systems by Jones and Grandhi (2005). Since LBS's uses the term entity which is both human and non-human, one can say that a P3 system is the type of LBS's concerning linking people to geographical places. The term P3 system will be used in this work, because it is considered more precise. Jones and Grandhi's article "*P3 systems: Putting the Place back into Social Networks*" presents a conceptual framework of P3 systems, which splits P3 systems into two groups, *people-centred* and *place-centred* (Jones and Grandhi 2005). People-centred systems are systems that either use absolute positioning or collocation/proximity. An illustration of systems that uses absolute positioning used by Jones and Grandhi is "*The Weasly clock*", taken from the universe of Harry Potter. This is a clock used by the mother in the Weasly family. Instead of the minute- and hour hand, this clock has nine hands, one for each of the members of the Weasly family. Instead of numerals, there are descriptions of places where the members of the family could be. So if one of the family members is at school, his hand is pointing at "School" on the clock. It is giving information of the absolute position of a person. With collocation/proximity the user's position are relative to some point, often another user. An example can be if a user has a contact list, and all the contacts that are within a kilometre of the user are shown in green text. Place-centred systems are systems that link virtual places to physical locations. Further, these systems do either use physical places or matches virtual places. The authors use another example from Harry Potter to illustrate the use of physical places. "*The Marauder's Map*" is a map that shows every detail of the wizard school Hogwarts. Inside the map there are many small dots with names on that are moving around. These dots show where every single person currently inside the school area are located (Jones and Grandhi 2005). The map is very similar to The FriendRadar, which therefore is categorised as a place-centred system. Further, P3 systems can be

either synchronous or asynchronous in terms of communication and location awareness. In The FriendRadar there is synchronous location awareness because one can only see the current location of the users. The communication however, is asynchronous; one can send a message to the other users, which are possible to read at any point after it is sent.

Grandhi, Jones et al., (2005) presents a survey executed at various places in Manhattan, with more than 500 participants. 84% of the participants were willing to share their location data (anonymously) to get information about crowding and occupancy in public places like restaurants or train stations. 77% were willing to let others know their current location in public and semi-public places; 69% to family and friends, 32% with colleagues and 17% with strangers. It is concluded that the survey suggest that a large proportion of the population considers P3 system sufficiently beneficial to let services collect their position data (Grandhi, Jones et al. 2005).

3.3 Behaviour of the user and usage patterns in location-based services

Not much research has been done on how users' behaviour is affected by location-based services. Colbert (2001) focuses the study on how rendezvousing is planned and performed. It shows that a rendezvous frequently does not occur exactly as planned. A rendezvous is any meeting with other people at an agreed time and place. Several tasks must be performed for a rendezvous to be successful; re-planning the rendezvous, seeking information about how to get to the meeting point (both travel and geographical), seeking information about other rendezvousers and about the activities following the rendezvous and communicating with other rendezvousers. Outcomes of a rendezvous are the additional stress and lost opportunities associated with the attempts to meet an agreed time and place. Mobile phones have made these outcomes less obvious, and Colbert (2001) presents a study on how a mobile device with a location-based service can make these outcomes even less obvious. It shows that 176 of the 415 rendezvous made by the participants in the study were problematic. About 30% of the rendezvous were performed without any kind of communication, and 44% was performed with a single communication. The rest was performed with more that one communication. The most important reason for an unsuccessful rendezvous was problems with the travel (traffic, delayed trains etc.), followed by overrun previous activity. The author states that the current mobile devices (2001) are not satisfactory to help rendezvousers to meet. He stresses that position-aware communication (sharing locations with others) would have solved many of the problems found in the study. Further, the study suggests that position information alone is likely to be informative. Finally, he shares some thoughts on how a location-tracking system would change the way the users behave during a rendezvous. He presents two examples, one where a mother does not know whether the father has picked their kids up at school or not. If she could see the location of the father (or even the kids), she would have known that the kids where picked up, and on their way home. Therefore she could drive home instead of stressing to the school to check. Another example is that if a user know she is early for a rendezvous with her boyfriend, she would probably be more willing to spontaneously pop into a shop while waiting, assuming that her boyfriend will know her location when he arrives. In this example, the rendezvousers are taking a higher risk, which can lead to new problems (Colbert 2001).

A recent study (Barkhuus, Brown et al. 2008)of the users behaviour when using Connecto, a mobile phone application that displays context and location information among small groups of friends, show that a P3 system can change the way users communicate with each other. Connecto is designed and tested especially for getting an understanding how location awareness would work within a peer-group of friends. Connecto has a friend list which shows the friends' name, location and ring profile. The location is obtained automatically by GSM cell towers and GSM cell fingerprints. Cell fingerprints means that each user couples an actual location (relative to up to seven cell towers) with a location name of their own choice. This location name could be geographical labels, place names, activities and hybrids of all these. Examples are 'home', 'working' and 'Amsterdam'. If users are outside a registered fingerprint location, their last location is shown

with the time since last seen there. Users could also choose to set their location manually, that is write anything they would like in the location field independent of their actual location. Their ring profile could either represent their current phone profile or any text of free choice could be written there. The study of the users' behaviour using Connecto, shows that the information was shared as story telling. The place name was mostly the user's location and the profile was mostly the user's activity. The authors propose the possibility to manually name a location as the biggest factor behind Connecto's success, as this is more interesting and telling more of a story to a friend that their actual location. Users reported to check their phone constantly to see what their friends were up to. This awareness of others location and activities made people do actions spontaneously. A user reported that he used Connecto to show his friends that he was at the shooting club, and that he hoped the others would come and join him. Two of his friends actually did join him. Users also reported not to call a friend when the friend was in some known locations. Users also reported more behaviour as a consequence of that they could see other's location; one user said he saw his roommate at home and asked him start preparing the dinner, a couple reported episodes where one asked her partner to pick something up on the way home after seeing the partner just left work and a participant that commuted to work with another participant said that it was useful for him to see when the colleague has left his home, as he knew he would show up on his house twenty minutes later. The same user also reported that he saw his friend was late, and called him to ask what was going on, only to realise that his friend has slept in. The past days' labels would be used when users actually came together. The users used the labels to find subject to talks about when they met, for example talking about the activities of their weekend. The users were actually expected to have seen the other's activities, or else they could easily fall out of the group's conversations. The study also shows that the users wrote their labels with care. They were self-conscious of what their profile and location was set to, even though they never could know who was watching (Barkhuus, Brown et al. 2008).

3.4 Privacy in P3 systems and social network services

For the last ten to fifteen years privacy in information technology has been a very hot topic. Privacy in ubiquitous computing has not received the same attention, but some good and important studies exist. Langheinrich (2001) describes why privacy is particularly important in ubiquitous computing with four properties. These are **ubiquity**; the computers are everywhere, **invisibility**; the computers disappear from our view which makes it difficult to know whether we are interacting with a computer or not, **sensing**; the sensors are becoming more accurate and can sense a more detailed picture of the environment and **memory amplification**; the ability to store large amounts of data collected from cameras and other sensors. Many of the threats of these properties are controlled by laws, both international and national (Langheinrich 2001).

The most obvious threat to think about when talking about personal privacy and ubiquitous computing, is the term *Big Brother*, described in Orwell's legendary science fiction novel *"Nineteen Eighty-Four"* (Orwell 1949). All the citizens in Orwell's world are under constant surveillance by the government, by the use of technology that is possible today. In information technology this is a problem of two classes. The first class is the intentional tampering and misuse of applications to find information about others that these individuals considers private. The other class of the problem is the unintentional intrusions in others privacy because of poorly designed systems (Bellotti and Sellen 1993). The first class is difficult to completely remove, because there will always be criminals and persons that can not be trusted. The second class however, is a problem that can be erased with the right design (Langheinrich 2001). In everyday life it is not the threat of a society like the one in *"Nineteen Eighty-Four"*, but our interpersonal interactions that is of most concern. We as users want to minimize embarrassment, protecting our territory and staying in control of our own time. We want the same amount of control in virtual settings as in real life settings. In real life,

people can not listen to conversations in a distance or look through closed doors. These properties are something the users are expecting of virtual settings as well (Palen and Dourish 2003).

Many of the problems in ubiquitous computing are related to the concept of mutual awareness. A part of mutual awareness is the problems of disembodiment and dissociation. If you meet persons in a real life setting, you can receive information in many ways including position, voice level, face expressions and direction of gaze. In ubiquitous environments these abilities to express yourself might be less effective. You may also have problems knowing what others are trying to express. In real life people normally live by the intuitive principle that if I can not see you then you can not see me. This is not always correct in ubiquitous applications. Users may no longer exactly know what information they are conveying, in what form the information is, if the information is permanent, who is getting the information and how they are using the information (Bellotti and Sellen 1993).

Bellotti and Sellen (1993) present a framework for designing ubiquitous information systems that preserve privacy with the help of *feedback* and *control*. These two issues are in the words of Bellotti and Sellen (1993) "*[Feedback and control are] fundamental to successful communication and collaboration amongst users as well as to maintaining privacy*". By control the writers mean that the users always must have the power to control what information they are showing about themselves and who can see this information. By feedback they are pointing on the need users have for knowing when and what information about them is being captured and who is getting hold of this information. In other words, control is the possibility to edit preferences about which users that **can** see what information about you, and feedback is the amount of information you receive about who is currently **seeing** what information about you. The paper further present four categories you need to have control over and get feedback about. These are *capture;* what kind of information is picked up*, construction;* what happens to information, *accessibility;* is the information public, available for certain persons or exclusive to oneself and *purposes;* to what use is the information put and how can it be used in the future (Bellotti and Sellen 1993).

Later studies do also point out similar aspects of privacy management as Bellotti and Sellen's feedback and control. Langheinrich (2001) is referring to feedback as notice, but it is basically the same concept. He explains control as choice and consent. Jiang, Hong et al. (2002) presents *The principle of minimum asymmetry* when talking about feedback and control. It says:

"A privacy-aware system should minimize the asymmetry of information between ***data owners*** *and* ***data collectors and data users,*** *by:*
Decreasing *the flow of information from data owners to data collectors and users*
Increasing *the flow of information from data collectors and users back to data owners"*

By decreasing information flow from data owners the users gets better control over the system. Increasing information flow from data collectors provides better feedback from the system. Examples of privacy mechanisms that provide control by decreasing information flow are *anonymising* or *pseudonymising* which refers to being totally anonymous or using an avatar or a nickname respectively. Pseudonymity allows users to be recognised each time they interact in the environment. Increasing location granularity and decreasing the rate which information about location is sent can be used to make the information about a user's location less accurate. (Jiang, Hong et al. 2002). Further a *self-view* which shows the user exactly the same information that other users can see about this user can be used. *Plausible deniability* give the user the ability to plausible deny that she did not want to interact with that particular person at that particular time, but make up some other excuse. If this excuse can be made ambiguous, it will have less impact on the social relationship. For instance, when you refuse to answer a phone call when you know there is someone you do not want to talk to that are calling, you can later make some excuse about why you did not answer. *Reciprocity* is an essential property for building trust and deep relationships. If you tell too much or too little about yourself, you are generally disliked. A relationship, both in real life

and in virtual life, need to have balance in the amount of information and in what kind of information revealed to each other. In awareness applications this is managed by viewing the status or location of others only to users which are showing their own status or location. Users of social networks can have nearly as many *relational selves* as they have interpersonal relationships. Therefore *grouping* of contacts, with different settings to each group, offers the users to keep better control over what to disclose to which people (Raento and Oulasvirta 2005). To get better feedback from the system one might log all access of the user's position, give notification when someone asks for the user's position or provide clear feedback over which information that is stored (Jiang, Hong et al. 2002). Some of the mechanisms mentioned above could be placed both as mechanisms to improve feedback and control, which shows that they are two tight related concepts.

The article "*Personal privacy through understanding and action: five pitfalls for designers*" (Lederer, Hong et al. 2004) describes feedback and control as the means a designer have to engender understanding and action. The article describes feedback and control as "*[Feedback and control is] the designer's opportunity to empower those processes (understanding and action), and they are the user's opportunity to practice them.*" The authors uses pitfalls which they have experienced themselves as examples of how bad privacy design can affect computer systems. The five pitfalls are split into the two categories of understanding (feedback), pitfall 1 and 2 and action (control), pitfall 3, 4 and 5:

1. *Obscuring potential information flow:*

   Systems must make clear what possible disclosures they can make. This include what types of disclosure is possible, who can receive it, which media it is conveyed through, collection of meta information and potential for unintended disclosure. Some information types of particularly interest are personae information such as passwords and e-mails, and activity information such as location and purchases.

2. *Obscuring actual information flow:*

   Systems must make clear what is actually disclosed. Users must understand what information that is conveyed and who is receiving the information. This is provided through feedback from the system.

3. *Emphasising configuration over action:*

   Privacy management should follow as a consequence of the users ordinary use of the system. This means that you should not need a load of configuration of privacy settings to maintain the desirable privacy in the system. In real life users do not explicit state which information that should be private and which information that should not be private. They change their "privacy settings" depending on which social setting they appear in. Research has proved that users tend to use the default settings of a system (Palen 1999). They do not take the time to configure their setting to fit their needs. If they actually do change the settings, they are usually too difficult to set when it comes to privacy. Users are asked to set preferences in future and unpredictable situations. What they think is their preferences in a particular situation do not always fit reality. Users also easily forget which preferences they have set in the different situations.

4. *Lacking coarse-grained control:*

   Many devices fall into the pitfall of giving a user too many choices. Often a binary on/off button is the best solution for controlling availability. Binary buttons are something every user can control with ease and everyone understands their meaning. Another solution might be a simple ordinal control like the one you find on volume controls. Binary and ordinal controls are easy to adjust and give an easy and immediate response.

5. *Inhibiting existing practice:*

   Computer systems should try to adapt existing practices in social interactions. If they fail to do

so, they might fall into this pitfall. Some of the most important issues in this field are the concept of plausible deniability. This means that the user cannot know whether the lack of response was intentional or not. A related concept is the disclosing of ambiguous information, which as mentioned above, can be use of pseudonyms or imprecise locations. Both of these concepts are often more difficult to achieve as the technology gets better.

In *"Location-Based Services: Back to the Future"* (Bellavista, Küpper et al. 2008) a future scenario of Location-based systems is described. The article appears to be written in 2012, and asks the question: *"What Was Wrong with First-Generation Location-Based Services?"*. The authors present a view in retrospective that describes the reasons why the first systems which share a user's location with others (a user or a server) did not succeed commercially. Some of the reasons described are concerning bad user experiences following technical limitations and cumbersome user interactions. They describe a change from reactive system interactions to proactive system interactions. This means that the 'new' systems anno 2012, are automatically (proactively) initiated when some predefined event occurs, and not explicitly (reactively) invoked by the user. Another change that they believe was a part of the reason for the (imaginary) revolution of LBSs, was that the systems went from single target to multi target. This is both multiple users located at once and multiple users together with other targets. The authors main reasons for the revolution however, concerns privacy in LBSs. The most important feature of the 'new' systems is user centricity. The centric management of location data is described as the main privacy concern of the early systems. It was not until the users managed the location data themselves, they started to trust the systems. The location in the 'new' systems are retrieved by a combination of GPS, Wi-Fi positioning and GSM/UMTS positioning. Each user saves their location locally and is therefore in complete control of their own location information. The data is shared directly with their friends, and only when needed and in the granularity chosen by the user. In this way the users need not to concern about how their location data is used by a central server. The 2012 analysis, also describes the protection from legitimate users as an important feature that helped LBSs to gain popularity. The mechanisms used are plausible deniability, as mentioned above, and what they call *reciprocal exchange of location data.* By this, the authors means that the exchange of location data must be symmetrical, which is the same as *The principle of minimal asymmetry* described by Jiang, Hong et al. (2002). In this occasion, the users are seen as both data owners and data collectors.

A survey from UC Berkeley concludes that identity of the inquirer of information is of greater importance that the current situation of the user, when deciding which privacy setting to use in a mobile application used for social interaction. It further concludes that designer should use identity of the inquirer as the primary index in privacy settings and situation as the secondary index (Lederer, Mankoff and Dey, 2003). These results are confirmed and further elaborated by a three-phased survey performed on 16 non-technical participants by Intel Research Seattle. This study concludes, as mentioned, that *who* the requestor of location data is, are the most important factor when deciding to disclose the data or not. Especially their feeling towards the requestor influenced the decision, for example one participant said she avoided her mother on purpose. People were most willing to share their location with their *significant other* (disclosed location 93% of requests), followed by *friends* (85%) and *family* (83%). They were much less willing to share location data with *co-workers* (53%) and *managers* (34%). Two other important factors when deciding are *why* the requestor want the user's location and *what* level of detail would be of most interest for the requestor. Another key finding was that participants either disclosed the location in the detail level most useful to the requestor, or did not disclose the location at all. This means that users very rarely disclosed less detailed location data to protect their privacy. The times they disclosed location data with higher granularity, they did it because they thought this would be of most interest for the requestor. This was done usually to requestors living in another state or country (that would not benefit from knowing the exact street address) or when the participant was on a trip in other places then their home city. If the participants did not want the requestor to know their location, they

simply chose not to disclose any location at all. The study further showed that activity and mood also influenced the participants' decision whether to disclose information or not. When people stated they where angry, they only disclosed their location 57% of the time. Surprisingly maybe, participants disclosed location most often when depressed (82%). The activity that got the highest request rate was doing household chores (96%), and the two with lowest rate was studying (63%) and talking to a colleague in person (65%). Finally some people where interviewed about which situations they rejected a location request. The situations mentioned was request from their boss after work hours, inappropriate request from friends (when socialising with others), when out on dates with significant others, when doing errands (they did not want to picks stuff up for others) and when they were trying to hide actions they should not be doing (or hide that they where not doing what they was expected to be doing) from their significant others (Consolvo, Smith et al. 2005).

Another survey is based on the actual use 350 users of Flickr with a mobile phone application called ZoneTag that supports camera phone photo sharing and organization via Flickr. Pictures can be uploaded directly from the phone to Flickr, with different privacy settings. Flickr have five privacy levels; private, family-only, friends-only, friends-and-family and public. The application automatically connects the picture to the user's actual location using mobile position techniques. Following this, a picture uploaded with ZoneTag will be tagged when viewed on Flickr. The users have the possibility to manually suppress the location data of a picture. The findings in this survey further confirm that the identity of the users that requests location information is of most importance when deciding privacy settings. Only 2% of the pictures uploaded had the location suppressed. Users decided to upload more private pictures in a more private category, rather that suppressing the location where the picture is taken and make it public. Further the authors discussed several dimensions of concern of the users, retrieved from interviews. First, the object dimension indicates that users are more careful when it comes to pictures which include other people than with pictures of only themselves. Several interesting points were raised from the interviews. Some security concerns were expressed, especially by mothers that described it as "*a roadmap for sexual predators*". Concerns dealing with the identity of self and others were also an issue, for example one user did not want to be seen on a gay parade and some users where worried about HR departments searching for their name. Social disclosure was also an issue in both negative and positive ways. One user published a photo so his friends would know where he was, but on the other side some were worried that someone that was not invited would see the picture and get hurt. When it comes to location privacy, the participants expressed little to no concern with the fact that the application collects and exposes location data. One user said that he would not publish photos online if he was trying to hide his location from someone. Two users expressed concerns about advertisers using their location information combined with the content of their photos (Ahern, Eckles et al. 2007).

All studies presented so far agree that privacy, especially location-privacy, is of great importance in ubiquitous computing and that users of location-based services are in great danger of loosing their privacy feeling. Later field studies of the usage of implemented systems (and some surveys) however, indicate that this privacy concern might not be as big in reality as it is in theory. It all boils down to a tradeoff between the usefulness of the service and the users' privacy concerns while sharing their location. Barkuus and Dey (2003) concludes from their results (that shows that 11 of 16 users are not concerned) that people are not overly concerned about their privacy when using location-based services. They also found that users are more concerned about location-tracking service than location-aware services, and since they find both types of services equally useful, they suggest that location-aware systems should be emphasized (Barkhuus and Dey 2003). These results are from a diary study of fictional systems, and only presents what users imagine can be a problem. Junglas and Watson (2008) on the other hand, argue that location-tracking systems should be the focus of development, since they offer a greater usefulness to the users. The results from their study also show that users had a mixed feeling of enthusiasm and concern towards such systems (Junglas

and Watson 2008). Another field study (Barkhuus 2004) performed in a closed environment (The University of California, San Diego) with the system Active Campus also suggest that the 'coolness' and usefulness of a system, could undermine the users' focus on privacy issues. This is however no reason for not to implement privacy mechanisms to future systems, as users must know who can and who cannot see their location to be able to accept the system. To be able to turn a system off is important, and a system would be easier to accept if it is in a closed setting, either physical or closed user groups (Barkhuus 2004). The users of Connecto (Barkhuus, Brown et al. 2008) had several privacy mechanisms implemented. For instance it had a possibility to manually set your location, independent on where your actual location was. This function could be used to achieve plausible deniability by lying on your location, but it was not used this way. It was used to give the friends a better understanding about their actual location instead of lying about it. For example if a user was in another town, the area was too big to register to a location, so she only wrote the city's name manually. The system was not possible to turn off, but since the users had to write in the location themselves, they had the possibility to be in unknown areas if they wanted to. They could also blur out their location name, for example just write 'restaurant' instead of a particular restaurant's name. None of the users expressed any concerns about privacy in interviews after the project was finished, not even when they were explicitly asked about it. The authors think that the usefulness of the system, the practical use and the awareness of the system outweighed these privacy issues (Barkhuus, Brown et al. 2008).

3.5 Wireless Trondheim

Wireless Trondheim is a project that covers the downtown of Trondheim with wireless Internet connection available for anyone to use. Students and employees of NTNU, employees in the municipality of Trondheim and pupils of the high schools of Trondheim, have free access to the network. Everyone else must buy a cheap ticket, which gives them access to the network for twelve hours. Figure 3.1 shows the areas in Trondheim which is covered by wireless network. As the figure shows, the entire downtown of Trondheim is covered by the network. Some areas however are shielded from the signal, especially indoors it is difficult to connect to the network. The markers in the map in Figure 3.1 are indoor locations (cafés and shopping centres) that have Wireless Trondheim hotspots.

The transmission technology used is Wi-Fi hotspots, backed with fibre-cables. This gives a signal reach of about 60 metres from each hotspot. In the near future the plan is to integrate WiMAX technology in Wireless Trondheim, which will offer a signal reach of about 10 kilometres from each transmitter (Andresen, Krogstie et al. 2007).

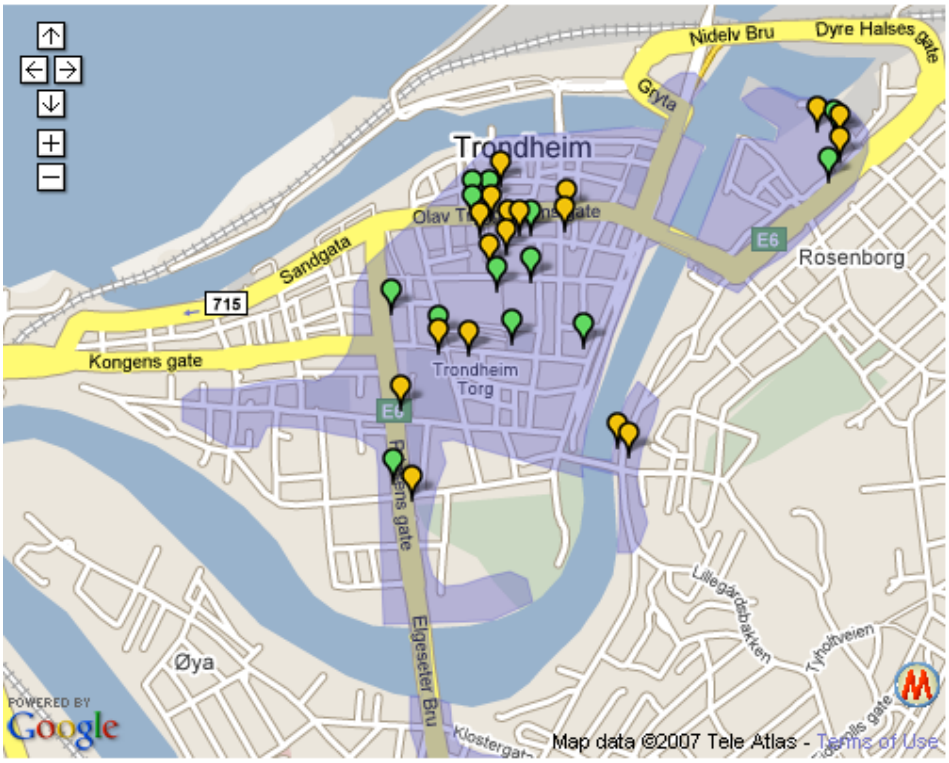

Figure 3.1: Coverage of Wireless Trondheim

3.5.1 Geographical Position Service

Geographical Position Service (GeoPos) is a position service for Wireless Trondheim. GeoPos has a web service interface that offers connections to the Cisco Location Appliance. Input to the GeoPos service is the MAC-address of the device which you want to retrieve the location of, together with some certification-data. From this follows that you can locate any device, both your own and any other. The response from the service is the user's location in XML format, together with some other parameters. An example of the response from the server is presented in Figure 3.2. The <X> and <Y> elements is the position of the device in Wireless Trondheim. The <Longitude> and <Latitude> elements is position of the device in Universal Transverse Mercator (UTM) coordinate system, and the <geoLongitude> and <geoLatitude> elements is the position in the longitude/latitude coordinate system. Google Maps uses the latter coordinate system, and the coordinates can therefore be used directly in Google Maps. The <changedOn> element is the time the user's location last changed, in milliseconds from January 1st 1970. If the device is located outside the area of Wireless Trondheim an <ErrorList> element is filled with a specific error response.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<GposResponse>
    <ResponseHeader sessionID="NOT-SET"/>
    <ResponseBody requestID="reqIdNotImplemented" version="1.0" locationType="CURRENT">
        <XYPosition>
            <X>1666.92</X>
            <Y>300.06</Y>
            <Longitude>569620.0</Longitude>
            <Latitude>7033449.0</Latitude>
            <geoLongitude>10.394750213485754</geoLongitude>
            <geoLatitude>63.42273795639271</geoLatitude>
            <changedOn>1208936530977</changedOn>
            <FloorId>12</FloorId>
            <Elem>Sone14</Elem>
            <Elem>Sone14</Elem>
            <Elem>Midtbyen_Group</Elem>
            <Elem>Midtbyen</Elem>
    </XYPosition>
    </ResponseBody>
</GposResponse>
```

Figure 3.2: Response from GeoPos

3.6 Existing systems

This section will present systems that offer similar functionality as The FriendRadar. First, FindMyFriends will be presented followed by the Norwegian system mBuddy and Navizon.

3.6.1 FindMyFriends

FindMyFriends is a project developed by Accenture for UKA-07 that allows people to locate each other at Samfundet. "Studentersamfundet i Trondhjem", or just Samfundet for short, is a student society in Trondheim that is student driven. Samfundet arranges concerts and other social activities for the students, with the student festival UKA as the biggest happening every second year. Samfundet has 1200 volunteers and over 8000 members. The name Samfundet is also used for the building where the society is located. It is a very big red and round house, which was built in 1929.

It is a known problem among students in Trondheim that it is difficult to find each other inside Samfundet. Accenture was one of the main sponsors of UKA-07, and had the idea of promoting the technology behind FindMyFriends during UKA-07 by making it easier for the participants on a party to find each other. The system was particularly aimed towards the workers of UKA-07, to make it easier for the workers to keep track of each other.

Users of the system registered a user profile on the website[7]. After a user had registered her profile she could start connecting with the other users, much like the concept behind Facebook and other social network services. Just before UKA-07 started, the users received their tag used for positioning. The tag had to be registered by the user, to connect the user to the tag. There were placed user terminals at Samfundet, which allowed the users to log into the system. When a user moved around Samfundet wearing the tag, the user's friends could log on the website or one of the terminals to check out the user's position. A user can only locate the users that have accepted to be friends with her. The system generates statistics based on the user profiles, which allows the users to see which rooms that have most girls, the average age of the users in a room, where you should be if you want to meet most single boys and similar statistics. Users could also send avatars to each other, that is a little icon that represents a meaning.

[7] http://findmyfriends.no

The website offered the users to register as a member of FindMyFriends and make a user profile. After registering the users could search for other users that they wanted to be friends with, and ask them to become friends

To log in on a terminal at Samfundet, the users have to carry her tag and 'show' it to the terminal. Then a welcome screen appears where a pin code must be entered. This means that a user have to carry the tag to be able to locate someone through a terminal. Users can log in on the website from wherever they want without using the tag. On the terminals the users can locate their friends on the map and check the statistics. To become friends or to send avatars to other users, one has to be logged in on the website.

The users are able to locate their friends on the map shown in Figure 3.3. This screenshot is taken from one of the terminals, but the map is similar on the website. The user logged in on this figure has two friends currently on Samfundet, both in *Bodegaen*. One of her friends is shown as a pacman avatar (the yellow one) and the other one are shown as normal.

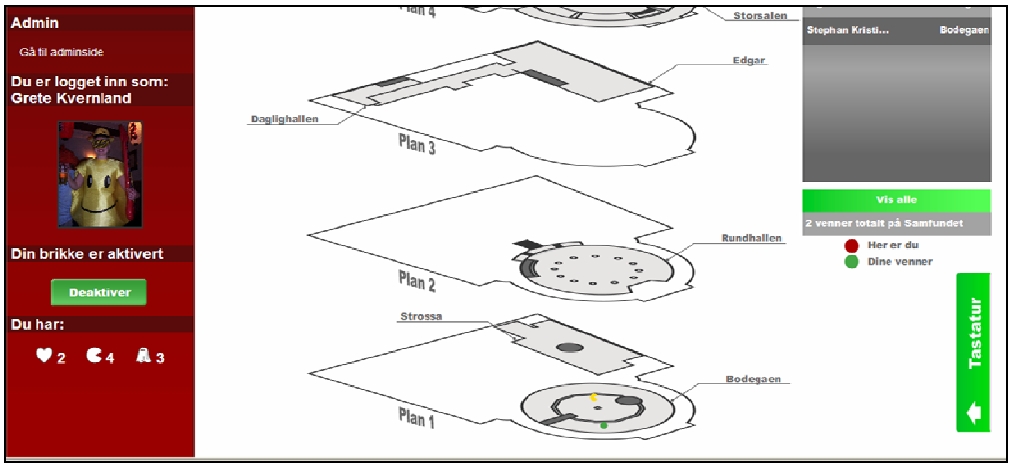

Figure 3.3: The map from a terminal (Picture: Accenture)

The technology used for positioning of tags inside Samfundet is *Ultrasound indoor positioning system* (IPS). Ultrasound makes it possible to locate users precisely by room using wireless detectors and tags as the one shown in Figure 3.4. Each tag has its own unique identification sound, which is transmitted periodically or by moving. This sound is detected by one of the 63 detectors ("microphones") spread around in the rooms of Samfundet.

The advantages of this technique are that the sound does not penetrate solid walls, which makes location per room easy, ultrasound waves are mechanical and therefore immune to interference and it is difficult to eavesdrop the communication link.

Figure 3.4: The tag used for positioning

3.6.2 mBuddy

The Norwegian mobile company *NetCom* released a service called *Buddy* in 2001, where users could send an SMS to a server and receive the position of the requested friend on SMS with information as for example "Gjøvik Sentrum, 42 kilometres away, direction north" (ITavisen 2001). Today, CellVision has a service called *mBuddy* that is a continuance from NetCom's Buddy. It has about

20,000 users in Norway. It uses GSM positioning to locate users anywhere in Norway, which give a position-accuracy of a couple of hundred metres in urban areas and a couple of kilometres in rural areas. A user can only locate her own buddies; someone who previously have accepted being a buddy of that user. Members of the service are charged 29 Norwegian kroner each month. Users can localise buddies either by a SMS, on the website or on WAP. SMS positioning and positioning through the website cost 2 kroner and WAP positioning is free. The WAP positioning graphical interface is shown in Figure 3.5. About 10% of the times a user is localised a notification SMS is sent out to avoid misuse of the service. Users can choose to 'hide' whenever they want by sending an SMS to the service (mBuddy 2007).

mBuddy got criticised by the manager of *The Women Shelter* in Norway in an article at NRK where she warns about the use of such systems. She says that The Women Shelter has experienced that controlling men uses mBuddy to keep their partner under surveillance. She further asks The Data Inspectorate in Norway to stop the system, to avoid such surveillance. The Data Inspectorate answers in the article that it is important that these kinds of services are closed until the users manually open them by for example accepting buddies (NRK 2007).

Figure 3.5: WAP interface of mBuddy (mBuddy 2007)

3.6.3 Navizon

Navizon is an application for mobile devices and laptop computers. It will display the users' location on a map and find restaurants, sights and other things around. These things are user edited so any user can add *Geotags*, which are physical places connected to the map. Geotags are notes with a name, location, description and tags for searching. Users can later find these Geotags by searching. For instance if a user is interested in the closest pizza restaurant, she can search for 'Pizza' in the program and the application shows a list of pizzerias nearby as shown in Figure 3.6. Users can also just check any tags that are close (Navizon 2007).

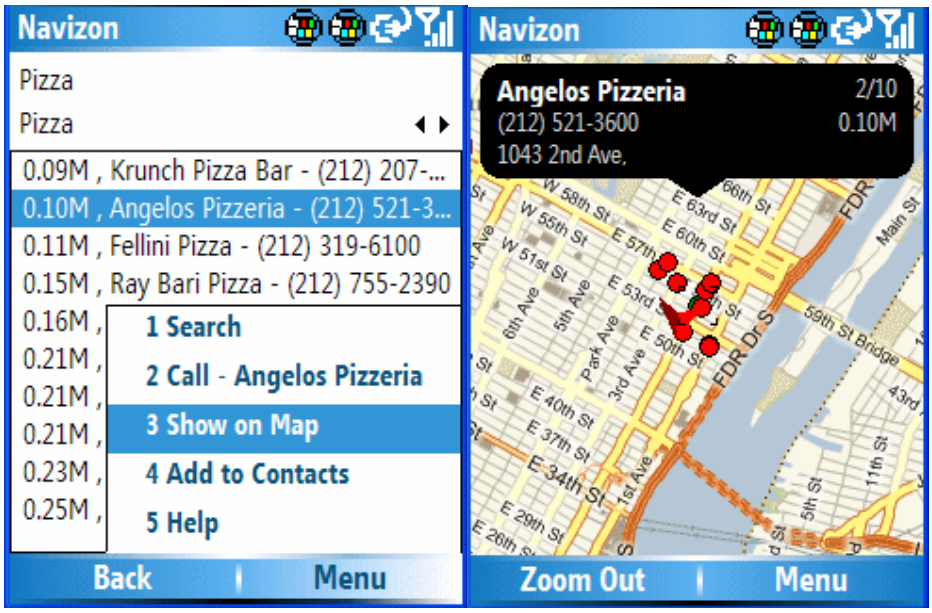

Figure 3.6: Navizon pizza search (Navizon 2007).

This functionality is complemented with the possibility to start or join groups of users. Groups can be started by anyone, and can be public or closed. Within in these groups it is possible to locate other users; a functionality called *Buddy Tracker.* A user can locate all the users that are member of any of the groups she belongs to. The user keeps a list of the users possible to locate, and one can choose to locate any of those users. The users must manually make their location available to the other by checking a menu choice called 'Send location'. If this is checked the location is shared with other user, unchecked the location is private. The left part of Figure 3.7 shows how users can choose to locate any of the users that belong to the same groups as themselves. The right part of the figure shows the users on the map. Users can also choose functionality to log their own position for later retrieval (Navizon 2007).

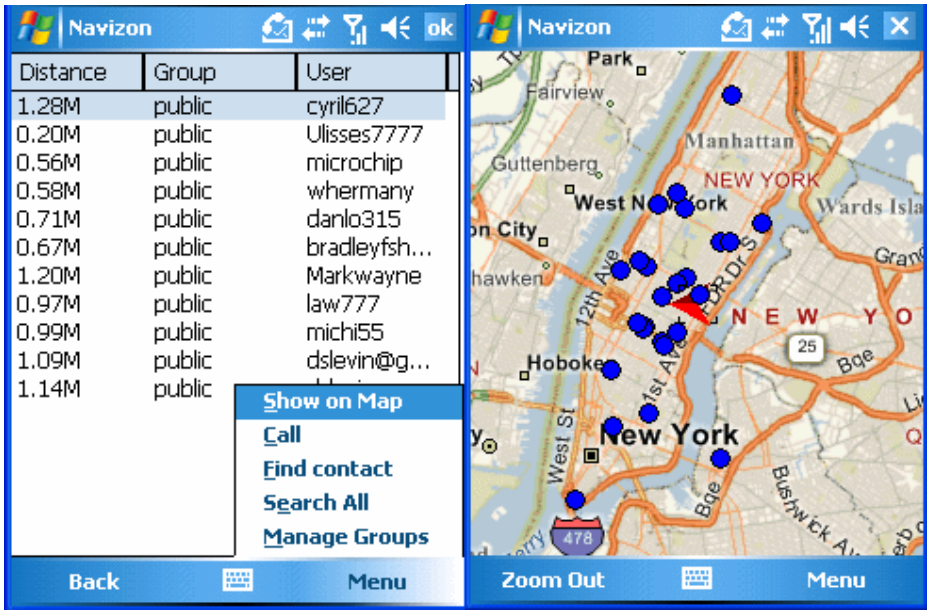

Figure 3.7: Navizon Buddy Finder (Navizon 2007).

Navizon use GPS to locate its users, but they also be located using a device without GPS. This is done using something Navizon calls *VirtualGps*. When users with a GPS device uses Navizon, they are at the same time located using WiFi hotspots and GSM triangulation. These two locations are synchronised and stored and by this way GPS user build the Virtual GPS environment while they walk around (Navizon 2007). In other word, if nobody with a GPS device and Navizon active has visited a location, a user cannot be located at that position with VirtualGPS.

Navizon costs USD 24.99 to download and are available in every country. *Navizon Lite* is free, but this version only uses GSM triangulation for positioning (Navizon 2007). No data was found about the number of downloads of Navizon.

4 Preliminary study

This chapter will summarise the preliminary study performed on the system FindMyFriends, presented in Section 3.6.1, during the autumn 2007. The preliminary study had the exact same research questions that this master's thesis, and was performed and written by the same student as this thesis. First, the research methods used and the results found in the preliminary study will be presented. Further, the conclusions are presented and finally further work from the preliminary study will be presented.

4.1 Research and results

To be able to study the behaviour of the users of FindMyFriends the systems stored data was analysed, an online questionnaire was sent to the users and some users were interviewed.

FindMyFriends had 2769 registered users, but only 1661 registered tags. Only those with a registered tag are actual users. 62% of the actual users were males and about 34% of the users were workers at UKA-07. The average number of friends for all registered users was 12.55.

An e-mail was sent to all the 2769 registered users, where they were asked to answer an online questionnaire. 207 users answered the questionnaire, which accounts for 7.5% of the registered users. The questionnaire had relatively few questions (20) and took only a couple of minutes to complete. The questionnaire was designed with the research questions as a basis, and designed with consideration to the disadvantages of this type of survey. The gender and worker/non-worker distribution of the respondents of the questionnaire indicated that the participants from the questionnaire are a representative selection of the actual user mass.

The results of the questionnaire shows that users said that they used their tag 'always' or 'most of the time', while they was at Samfundet, and that users with many friends used their tag more often than the users with few friends. Further, the results shows that about 75% of the users checked their friends' location at a terminal at least once and almost 80% did the same using a computer located outside Samfundet. 55% of the participants said that they would use a similar system as FindMyFriends made for positioning users in the entire city, which are analogous to The FriendRadar developed in this master's thesis. The participants were also asked to substantiate why or why not they was interesting in using such a system. The by far most common answer (56 answers) in the 'No' category was that they felt it would be like surveillance and that they would not like that everyone could be able to see their location. Other common answers was that they did not see the need of such a system (12 answers) and that they might would have used it if the system could be turned off (8 answers). Most of the users that was positive to a city environment system, substantiated this with they thought it would be funny or exciting to use such a system (25 answers), that they only would use it if the system or its location functionality could be turned off (22 answers) and that they thought this system would make it easier to find their friends (20 answers).

The results also showed that over 50% of the users tried to find their friends at least once after locating them on a terminal and that about 10% of the users went to Samfundet as a consequence of seeing some of their friends at Samfundet from a computer located outside Samfundet. Seven participants, or 3.38 %, postponed a trip to Samfundet as a consequence of checking the map on the website where they found few of no friends. Seven people also cancelled a trip to Samfundet after doing the same. Only two users thought that the tag made them act in a different way than normally because of wearing the tag, and only three users felt that the tag disturbed their personal privacy. Five users left their tag at home on purpose, because they did not want their friends to see that they were at Samfundet or where at Samfundet they were located. A total of eight people obstructed the tag on purpose because they did not want to be located at least once. On of these did it more that five times. Further, the results indicates that there are a connection between the privacy feeling and leaving the tag at home, but that the same connection did not exist between privacy

feeling at obstructing the tag. Finally, 10% of the users said that they would probably have lied about their location if possible, but most of these users said that they would only do it because it would have been fun. Many users were sceptical to such functionality, manly because they did not see the purpose of it. Twelve users stated that this would ruin the whole point of the system, because the location credibility would be lost.

To add more depth to the questionnaire, interviews were chosen. An e-mail asking if the user wanted to participate in an interview was sent to the 15 users of FindMyFriends who sent most avatars, which is a type of message, during UKA. Two of the users who were asked, answered positive to that request, one of each gender and both was workers during UKA. Each interview lasted for about half an hour, and followed a semi-structured form which means that a template was followed but the order of the questions could be rearranged depending of how the conversation developed. The interview template was designed such as the question answered the research questions and complemented the results from the questionnaire.

The male participant, called 'John', was 23 years old and had about 45 friends in FindMyFriends. He visited Samfundet about 20 times during UKA, but wore the tag only about three times. The main reason for this was because he forgot it and because he felt it was big and clumsy. The female participant, called 'Jane', was 21 years old and had 64 friends in FindMyFriends. She visited Samfundet about 15 times during UKA, but only wore the tag at the night, not at daytime. Both interviewees would use FindMyFriends if it was possible next time UKA is arranged and both would use it if it was a permanent system. Jane however, said that she would not always wear the tag, because of its inconvenient size. Both interviewees used the terminals to check their friends' location, John four times and Jane about ten times, but only Jane used them to physically find some of her friends. None of the interviewees felt that they had behaved in any different way because of the location functionality the system offered. John was not interested in a similar system used in a city environment, but Jane admitted that she probably would have used it if her friends started using it. John would use it if all privacy issues were dealt with, but would have had very few friends. Jane also said that she would be a lot more careful about whom she would accept as her friends. When the interviewees were confronted to some of the privacy mechanism mentioned above they were negative to most of them in FindMyFriends, but positive to most of them in a city-scale system as shown in Table 4.1 and Table 4.2.

Table 4.1: Interviewees' attitude towards privacy mechanisms in FindMyFriends

Mechanism / **User**	**Plausible deniability**	**Turn positioning off**	**Notice when located by others**	**More coarse-grained positioning**	**Group friends, and have different privacy settings for each group**
John	Probably	Maybe	No	No	Probably
Jane	No	No, but if I had a stalker	Maybe	No	Probably

Table 4.2: Interviewees' attitude towards privacy mechanisms in city-scale system

Mechanism / **User**	**Plausible deniability**	**Turn positioning off**	**Notice when located by others**	**More coarse-grained positioning**	**Group friends, and have different privacy settings for each group**
John	Definitely	Definitely	Yes, as a log	Definitely	Definitely
Jane	Yes	Sometimes	Maybe, but it makes people too aware of the system	Yes	Yes

4.2 *Conclusions from the FindMyFriends research*

The results from the research presented in the preliminary study suggest that people in fact do want to use a system like The FriendRadar, and that it mainly will be used as a party tool for locating friends when out partying. However, the results shows that the users' privacy concerns are greater in a city scale system, than in FindMyFriends, and that sufficient privacy management are essential to get people to use the system.

The results further showed that users did act in ways they would not have done if they could not locate their friends. Users tried to find their friends after locating them on Samfundet, users both delayed and cancelled their trip to Samfundet because they saw that few or none of their friends were at Samfundet and users went to Samfundet as a consequence of that they saw some on their friends on Samfundet through the website. On the other hand, the results indicate that users of FindMyFriends did not act in a different way because they knew they could be located by others. It seems that the system did not hinder people in doing things they did not want other people to know, the users just hindered the system to show they were doing it.

Further, the results indicate that privacy was not a big problem in FindMyFriends. The users seemed to be aware of the possibility to block the tag's signals, so they could not be localised. The users did disturb the system in ways that allowed them not to be localised instead of letting the system disturb their own personal privacy. The users indicated however that privacy could be a bigger problem in a city scale system than a system used at Samfundet.

The results from the questionnaire and the interviews show that users are aware of privacy mechanisms and are willing to use them. In fact, many users state it as an explicit requirement that some privacy mechanism are included if they should use the system. Especially the possibility of turning the system on and off is required. It also shows that some users used privacy mechanism even though they were not implemented in FindMyFriends, for instance by physically blocking the signals. This clearly indicates that there are needs of those mechanisms.

4.3 *Further work suggested in the FindMyFriends research*

The further work presented several suggestions of how a city scale system should be implemented. It was proposed that the system should offer the users functionality that give the users sufficient feedback over what they are conveying and control over their privacy settings. The most important mechanisms to be implemented are functionality to turn the system on and off, preferably in a way that offers the users plausible deniability. Other functionality that should be implemented is grouping of friends with different position accuracy and reciprocity in the form of that users only can locate others when they themselves can be located. Further privacy mechanisms must be considered in the implementation of the prototype, for instance notification to the users when they are being localised by others could be a useful functionality. Further, it was proposed that the prototype must be tested by possible future users in Wireless Trondheim. An observation study would probably be an appropriate testing method, together with interviews of the prototype users.

5 Design and implementation

This chapter describes the design and implementation of the prototype system developed in this master's thesis. The system is called The FriendRadar ('Venneradaren' in Norwegian). First the overall functional requirements of the system will be presented followed by the systems architecture and implementation. Finally, the privacy mechanisms implemented (and not implemented) will be described.

5.1 Overall functional requirements

This section will present the most important functional requirements for a social network service with location functionality in Wireless Trondheim. Basic requirements are requirements that make it a social network service, location requirements makes it a location based social network service and privacy mechanisms explains what level of privacy mechanisms that should be implemented to the service.

5.1.1 Basic requirements

FR1: The system should be developed as a website.

FR2: The system should allow user to register a user profile, with various information about the user.

FR3: The users should be able to connect with other users, to form a friendship.

FR4: The users should be able to send each other messages.

FR5: A message must be marked with a message type before it can be sent.

5.1.2 Location requirements

FR6: Each user profile must have at least one mobile device connected to it.

FR7: The system should be able to find a user's location in Trondheim, when the user's registered mobile device is connected to Wireless Trondheim.

FR8: Each time a user is located in Wireless Trondheim, the location should be saved in a database.

FR9: A user should be able to see the location of the user's friends that are currently located in Wireless Trondheim.

5.1.3 Privacy mechanisms

FR10: When connecting to a friend, a user must be able to choose between three privacy levels; map, nearby and blocked.

- FR10-1: The map privacy level allows the friend to locate the user on a map.
- FR10-2: The nearby privacy level allows the friend to know if the user is nearby her own location (Within 200 metres).
- FR10-3: The blocked privacy level does not allow friend to see the user's location at all.

FR11: If each part of a friendship has chosen a different privacy level, the strictest privacy level applies for both parts. That is, if one user choose map as the privacy level and the other one choose nearby as the privacy level, both parts of this friendship can only see if the other one is nearby.

FR12: A user can only see the location of her friends, when she herself can be localised by the system.

5.2 Architecture and implementation

This section presents the architecture of The FriendRadar. Figure 5.1 shows how The FriendRadar application is connected to GeoPos and to the database. GeoPos is as mentioned in Section 3.5.1, a service which takes a device's MAC-address as input and gives the device's location in Wireless Trondheim as an answer in XML format which need to be parsed by the application. The database makes a persistent storage for the users' location after it has been parsed. This makes it simple for any user to retrieve any other user's location, without calling GeoPos. The database also holds the information found in user profiles, friend connections and messages. Section 5.2.1 will describe the database design in detail. The FriendRadar component consists of business logic (controller), data model and a view that is a normal website accessible form any web-browser. This component is implemented in Java and JSP and will be further described in Section 5.2.2 and Section 5.2.3.

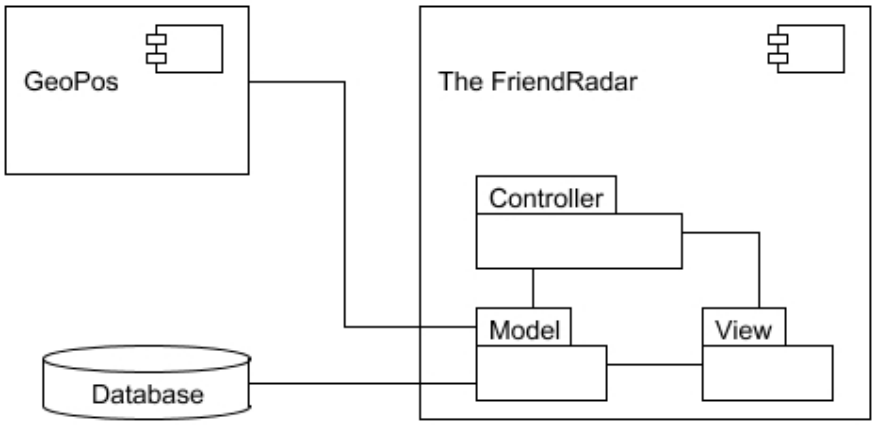

Figure 5.1: Overall structure of The FriendRadar

5.2.1 The database

This section describes the design and implementation of the database. The database is designed in such a way that sensitive data are protected when data will be analysed for research purposes. Figure 5.2 show the database model for the system, and Table 5.1 show the system's database schema. 'Usertable' contains all the relevant possible information a user can change in their profile. Nickname and pass (password) are mandatory attributes needed to log in to the system. The other attributes are information that can be added to make a profile more interesting for the other users. 'Avatar' inherits from 'usertable' and contains the gender and the date of birth of the user. This inheritance is done because gender and date of birth are attributes that are interesting when analysing data, but none of the attributes in 'usertable' are. This is also the reason why 'message_content' and 'message' are divided into two different tables. The information stored in 'message_content' is the actual message text together with its header. These values are of great interest for a user that sends or receives a message, but of no interest for the researcher analysing the data. But it is still valuable for the researcher to have some idea of what the content of a message is. Thus, 'message' has an attribute where a message type, which is selected by the sender, is stored. This makes it unnecessary for the researcher to actually read each message to know what they contain. This will also help keeping the messages private to only the sender and the receiver. The different message types are described in detail in Section 2.3.1. Each 'message' has one sender and one receiver. The attribute rd is a Boolean field that states if the message is read or not. The 'message' table has a connection to itself. This connection is represented by the answer_to attribute, that contains the id of the message that the current message is an answer to. The 'position' table

contains the longitude and latitude of every positioning done by the system connected with an avatar. The 'device' table keeps information about all the devices registered in the system. Each avatar typically has one device, but it is possible to register multiple devices to each avatar. The 'avatar' table has a many-to-many connection to itself. This connection represents a friendship connection between the users. A friendship must be two-ways to be an actual friendship. This means that for user 1 and user 2 to be friends, two tuples in the table are necessary; one where user 1 is the owner and user 2 is the friend, and one where user 2 is the owner and user 1 is the friend. The status (privacy setting) with the lowest granularity is the current privacy setting of the friendship.

The database is implemented using the MySQL server available for all students at NTNU.

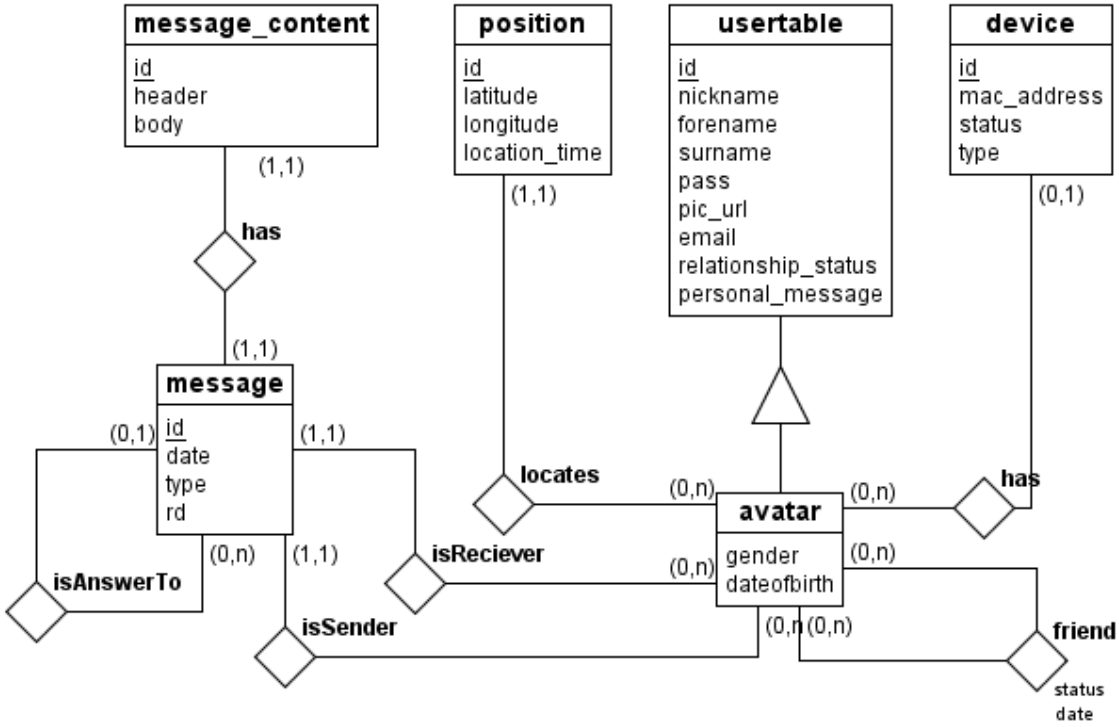

Figure 5.2: Database model for The FriendRadar

Table 5.1: Database schema for The FriendRadar

usertable (id, nickname, forename, surname, pass, pic_url, email, relationship_status, personal message)
avatar (id, gender, dateofbirth)
device (id, mac_address, status, type, user)
friend (owner, friend, status, date)
position (id, latitude, longitude, location_time, user)
message (id, date, type, sender, receiver, rd, answer_to)
message_content (id, header, body, message)

5.2.2 The FriendRadar component

The architecture of this component follows the common model-view-controller design pattern (MVC) as shown in Figure 5.3. The principle of this pattern is to separate the domain model and the business logic from the user interface that presents model. The manipulation of the model is

controlled by the controller, based on actions by the users performed on the view. MVC is very commonly used when developing web applications.

The model and the controller are developed in plain Java, and the view is implemented using JSP, HTML and CSS. The application is build using Maven2, and deployed on an Apache Tomcat 5.5 web server installed on a Windows Server 2003 machine placed on NTNU Gløshaugen campus.

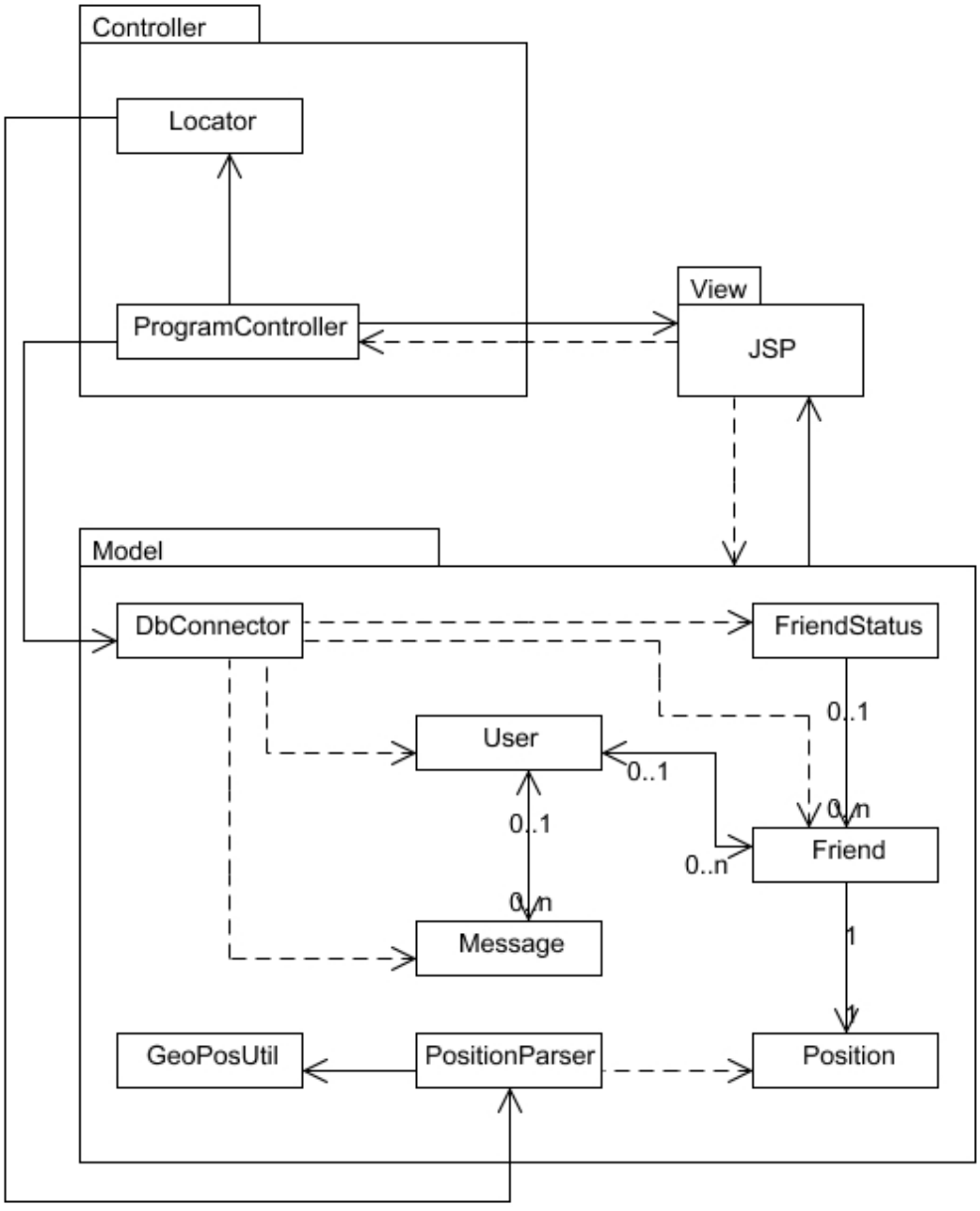

Figure 5.3: The architecture of The FriendRadar component

The domain model classes are JavaBeans consisting of various variables and getters and setters of these variables. The DbConnector class connects to the MySQL database using JDBC. This class does all the communication to the database, both instantiating domain objects from the stored data

and manipulating the database with the changes done to the objects by the application. The GeoPosUtil class does all the communication with the GeoPos server. This class delivers the raw XML data to PositionParser, which collects the relevant data and places it in Position objects. The ProgramController controls the execution of the application. One controller exists per session. All of the JSP pages interaction with the rest of the application goes through the ProgramController. The controller is instantiated when the user tries to log in to the system through the webpage. If the username or password is wrong, the ProgramController delivers an exception back to the view. When the login is successful, as shown in Figure 5.4, the ProgramController instance uses the DbConnector to retrieve the relevant User from the database. Further, the ProgramController uses the getOwnPositionStartThread method in the Locator to get the position of the user. This method first asks PositionParser for the user's location, which again asks GeoPosUtil for the location. GeoPosUtil delivers a XML answer to PositionParser, which is parsed to form a Position object. This object is stored in the database through DbConnector, before it is sent back to the Locator instance. The Locator then starts a thread in the Locator class which keeps going until a newer thread with the same user is started. If the user's location keeps changing, the thread will locate the user every 30 seconds. If the location is the same as the last time the user was located, the thread will locate the user every two and a half minute. If the user has no location (not connected to Wireless Trondheim), the thread will check for the user's location every hour. Every time a user is located by the system, the location is stored in the database. After the Locator instance has started the thread, it passes the Position object back to the ProgramController. Then the controller sets the Users location, and the user that started the interaction is now logged in and ready to use the system.

The login sequence presented above and in Figure 5.4, is just an example of how the ProgramController controls how the user interactions will affect the rest of the system. Every interaction from the webpage to the data objects passes through the ProgramController, and vice versa. Some controlling tasks are however done in the JSP pages. This was done both because it was more convenient at the time of development, and because some of the task was better suited to be performed in the JSP pages.

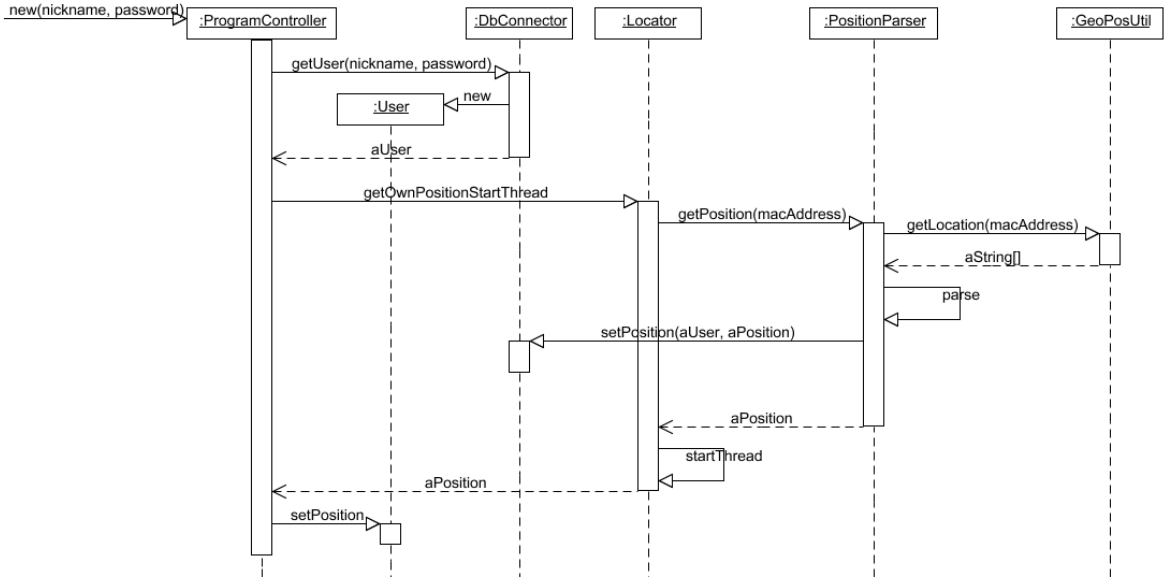

Figure 5.4: Successful login

5.2.3 Implementation of the JSP pages

As mentioned above, the view was implemented using JSP[8] (with JSTL[9]) HTML and CSS, and to some extend JavaScript. This section will show screenshots of the website and explain the functionality they offer.

Figure 5.5: Log in screen of The FriendRadar

The first screenshot, Figure 5.5, shows the log in screen of the application. It is accessed using any web browser with http://vr.idi.ntnu.no/vr as the URL. A user must be registered to log in to the system.

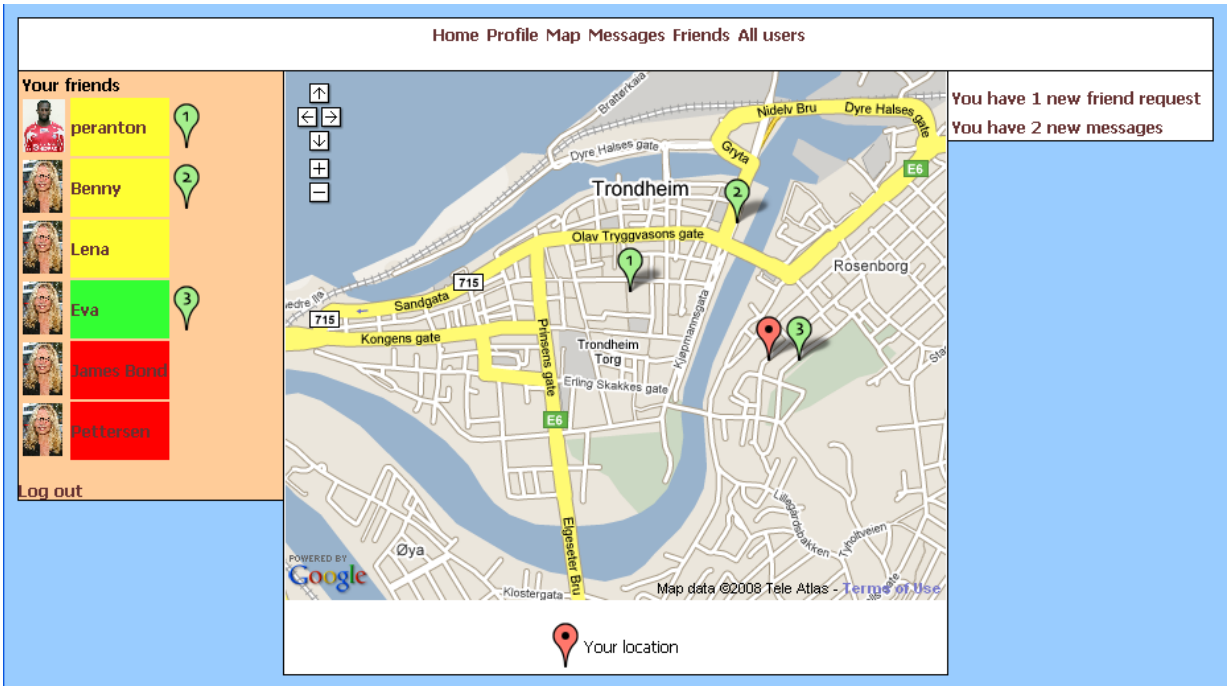

Figure 5.6: The map on The FriendRadar

Figure 5.6 shows the Map page in the website. The map used is taken form the Google Maps API, which is chosen because it is relatively easy to implement in a custom website. The red pin on the map is the logged in user's location. The green pins with a number on are plotted on the location of the user's friends, or more exactly; the location of the friends' devices. The number corresponds to the number shown on the pin behind the friends' names in the friend-list in left-menu. A friend either has a red, yellow or green background. The red background means that the friend is not possible to locate, that is; the user's device is not connected to the Wireless Trondheim network. If a

[8] http://java.sun.com/products/jsp/
[9] JavaServer Pages Standard Tag Library

friend has a green background it means that the friend's device is connected to Wireless Trondheim, and that its location is nearby the location of the logged in user's device. Nearby is within an area of approximately 200 metres. Friends with yellow background are connected to Wireless Trondheim, but are positioned on a location that is not within the nearby boundary. In this particular example, Eva is the only friend close enough to be marked as nearby. Lena is not shown on the map as a consequence of that either she or the logged in user (or both) has chosen the 'nearby' privacy setting in their friendship. If Lena had been nearby, she would have had a green background as any other user. The other three friends that are currently connected to Wireless Trondheim are shown with a pin on the map, because both parts in the friendship have chosen 'map' as the friendship's privacy setting. If a logged in user not are possible to locate in Wireless Trondheim, the user will see all her friends with red background, and the map will not be shown.

Figure 5.6 also gives an impression of how the user interface of the system is designed. The left-top- and right-menu is the same in every display when a user is logged in. The top-menu works as a normal menu, which allows users to navigate through the different pages. The right-menu shows the number of new messages and friend requests the user has received. The friend requests and messages can be clicked and the user is taken to the friend acceptance display or to the message inbox respectively. The left-menu works as a friend-list and shows every user that is friend of the logged in user as mentioned above. If a friend's name is clicked, the user is taken to the friend's profile page, as displayed in Figure 5.7 where Eva's name is clicked.

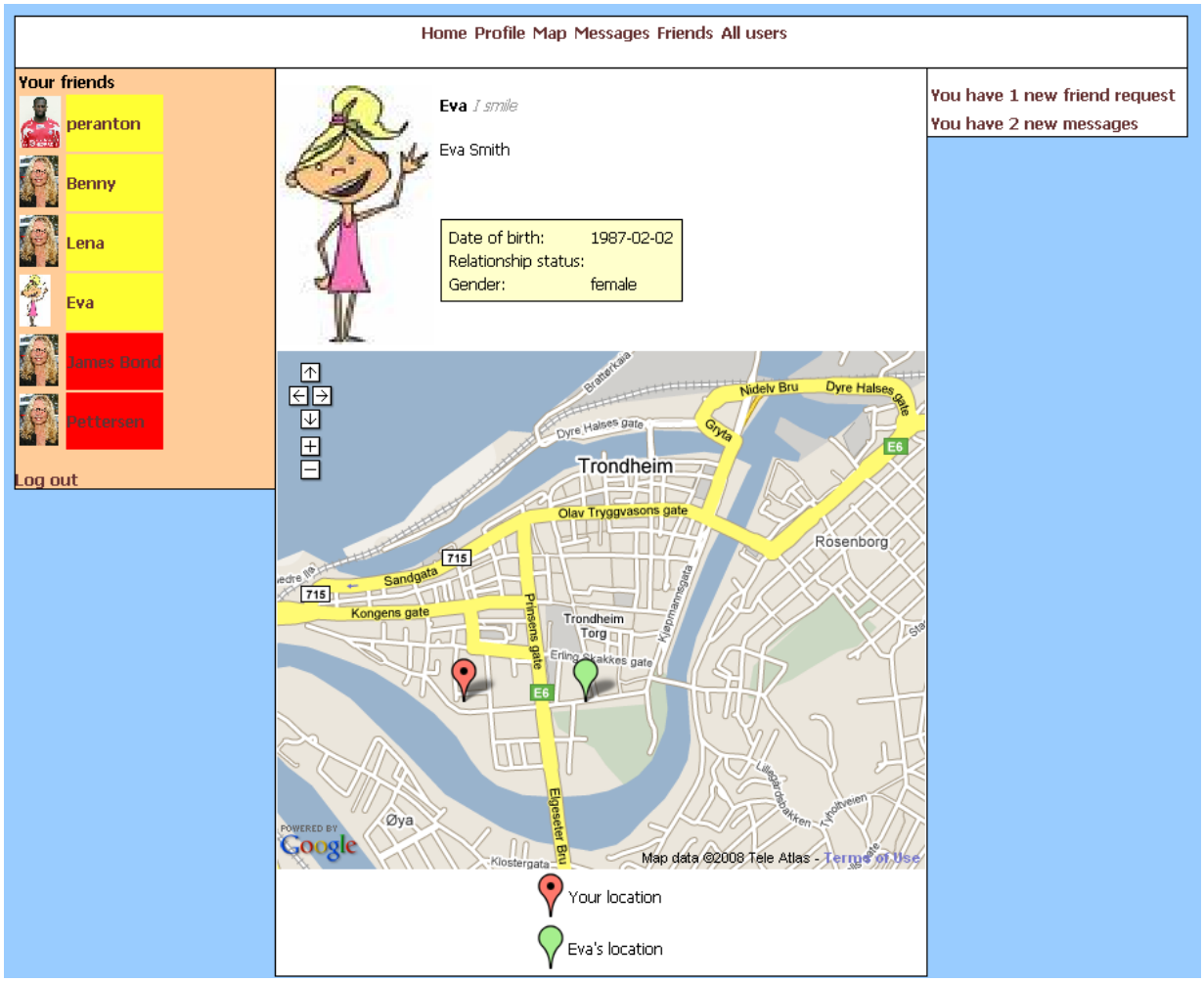

Figure 5.7: Eva's profile page

The profile page in Figure 5.7 shows Eva's nickname, her picture, a personal message, her full name and information about her birth date, gender and her relationship status just as any other social network service would have done. The profile page in The FriendRadar however, also shows a map where Eva's location is plotted together with the logged in user's location. This is beneficial if a user is only interested in a single friend's location. Notice that the friend-list to the left is still visible, but without the numbered pins behind which are only visible when the map page is shown. If the privacy setting in a friendship not allows the user to see the friend on the map, no map is shown at all. This also applies if the friend is not possible to locate or if the logged in user's device is not connected to Wireless Trondheim.

5.3 Privacy mechanisms in The FriendRadar

This section describes which of the privacy mechanisms mentioned in the preliminary study's further work that has been implemented to the system and which that has not.

5.3.1 Plausible deniability

It was concluded in the preliminary study that the mechanism that seemed most important is the possibility to turn the positioning functionality on and off, preferably in a way that offers plausible deniability. The FriendRadar has this functionality. A user has to manually connect her registered device to the Wireless Trondheim network to be localised by the system. This also offers plausible deniability; a user can say that they forgot to connect to the network or that she were in no need of the network at the current time. Another aspect that strengthens the plausible deniability part is that the Wireless Trondheim network has some weak spots. Some restaurants, cafés and shopping centres in the city have Wireless Trondheim coverage, but most of them do not. Thus, a user can say that she was inside a café or a store without coverage if someone wonders why she could not be localised. A third aspect that strengthen the possibility of plausible deniability is that the area a user can be localised are limited to a restricted area, namely the downtown of Trondheim. A user can simply say that she was outside the coverage area.

5.3.2 Friend based privacy settings

When users connect to friends in the system, they are asked what privacy setting they would prefer towards this particular friend. A user can choose between 'map' and 'nearby'. If a user not wants the friend to be able to see her on the map, she can use the setting 'nearby'. It is also possible to block friends. A user that has blocked a friend will appear disconnected to this friend at all times.

5.3.3 Proximity

If a user chooses the 'nearby' privacy setting, both parts of the friendship are only able to know if the other user is nearby or not. This is described as proximity, and can make it easier to accept more friends than they would have done without this privacy mechanism. This is, as mentioned above, implemented in the system as a privacy setting choice.

5.3.4 Positioning reciprocity

In The FriendRadar users can only locate their friends when they themselves can be located. If a user is not connected to Wireless Trondheim, and therefore impossible to locate using the system, then she cannot locate any of her friends. This also applies in the privacy settings in a friendship. If a user refuses a friend to be able to locate her on the map, the user cannot locate this friend on the map either.

5.3.5 Minimal configuration and standard settings

A problem described in existing literature on social systems, is the users resistance to complex privacy settings. In this system the users are only asked for privacy settings when connecting to friends, and there it is only one choice a user has to take; whether or not to be shown on the map. This privacy setting has no standard setting, because the user has to choose it before being able to connect to the friend. Therefore the user is forced to take a stand to this question.

5.3.6 Grouping of friends

Another mechanism mentioned in the preliminary study, is the possibility to group friends and have different privacy setting for each group. This is not implemented in The FriendRadar. The main reason for this is that the test user group probably would have been placed in the same group, since all the participants are classmates. Another reason is that the users are offered a privacy setting towards each friend rather then toward a group of friends. When there exists only one privacy setting, it is not of much effort to configure this setting towards each friend, rather that towards a group. It would have been more preferable to use a grouping mechanism if the privacy setting between friends had been more complex.

5.3.7 Feedback when localised

Another issue discussed both by other authors and in the preliminary study, is the importance of being notified when localised by other users. This is not implemented in the prototype, but could be a possible mechanism to be implemented in a commercial system. The main reason why it is not implemented is that the users usually localise many of their friends at a time, and every user may not be interesting. Therefore, a user can get an irrelevant notice about she is being localised. A possible solution could be that a user gets notice if a friend opens her profile and from there can see her location.

6 Results

This chapter will first present the results of the analysis of the logged data from The FriendRadar. Further the results from the questionnaire will be presented. Finally, a summary of interview will be presented.

6.1 Analysis of logged data

This section will present data of the actual usage of the system, extracted from the database and the log of The FriendRadar. 23 pupils did receive an iPod and agreed to participate in the experiment. Only 17 of the pupils did actually log into the system at least one time, and only these 17 pupils are considered to be a part of the experiment. Thus, all the results presented in this section are collected from the 17 actual users. Table 6.1 presents the 17 users' usage of the system. *Number of logins* is the total number of times a user has logged in to the website, both from the iPod's and from any other computer and independent on which network they were connected to. *Number of times located* is the total number of times a user's request to GeoPos returned an actual location in Wireless Trondheim. As mentioned earlier, the positioning functionality uses a thread that asks GeoPos for a location in a periodical interval. *Number of times connected to Wireless Trondheim* represents the approximated number of times a user connected to Wireless Trondheim. This number is calculated clustering a user's consecutive locations responses in groups, and counting the total number of groups for each user. From this, if a user connected to Wireless Trondheim after she received the iPod, and continued to be connected through the whole test period, she would have an extremely high number of times located, but would only be connected to Wireless Trondheim one time. The number is approximate because it can take maximum one hour before a user is localised by the system after connected to Wireless Trondheim. Therefore connections that last less than an hour could be missed in this statistics. Friend requests out are the number of other users the user has asked to be their friend, and friend requests in are the number of other users that has requested the user to be a friend. Registered friends are friend requests (both ways) that are accepted by the other part, and therefore the number of friends the user has in their friend list and the number of friends they can localise. The user IDs presented in the table is not the real IDs from the database, and is only used in this document.

Table 6.1: Statistics per user in The FriendRadar

User	Gender	Number of logins	Number of times located	Number of times connected to Wireless Trondheim	Friend requests out	Friend requests in	Registered friends	Msgs sent	Msgs rec.
1	female	1	40	2	9	11	8	0	0
2	female	6	0	0	9	10	9	0	0
3	male	1	97	6	7	13	7	0	0
4	female	5	0	0	14	10	9	0	0
5	male	3	38	3	11	12	11	3	2
6	female	10	33	4	14	11	10	4	4
7	female	2	6	2	3	8	2	0	0
8	female	2	1	1	0	8	0	0	0
9	male	2	5	2	14	14	13	0	0
10	male	1	0	0	13	13	11	1	0
11	female	4	58	6	13	13	11	4	3
12	male	4	107	5	15	15	14	0	1
13	male	2	5	3	7	10	6	1	3

14	male	3	11	1	13	13	11	0	0
15	female	2	46	6	8	4	3	0	0
16	male	1	211	6	0	1	0	0	0
17	female	3	2	1	16	0	0	0	0

6.1.1 User information

Figure 6.1 shows the gender distribution of the users in The FriendRadar. There were nine females and eight males. All the users are pupils in the second grade of a class that are mixed from two different schools located in downtown Trondheim. This means that the users are normally either 17 or 18 years old. These differences are not significant for the data, and are not included in the statistics. Another reason for this is that not all the users have written a birth date.

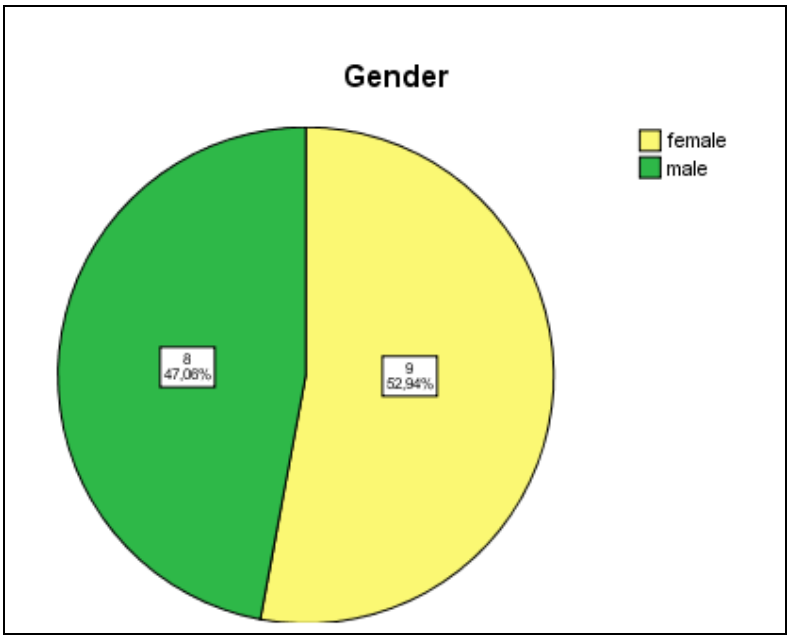

Figure 6.1: Gender distribution of the users

6.1.2 The user's usage of the system

Table 6.2: Statistics of logins, times located and connections to Wireless Trondheim

	Mean	Median	Mode	Standard Deviation	Variance	Min	Max	Sum
Number of logins	3.06	2	2	2.304	5.309	1	10	52
Number of times located	38.82	11	0	55.667	3098.779	0	211	660
Number of times connected to Wireless Trondheim	2.82	2	6	2.270	5.154	0	6	48

The users logged in to the website a total of 52 times, which gives a mean of 3.06. The median was 2 times and the mode, with five users, was 2 times. 52.9 percent of the users logged in either one or two times. One user however (user 6), logged in 10 times. The system did not log if the login was from the iPod or not. Table 6.2 shows summary of the statistics of logins, times located and the user's connections to Wireless Trondheim. Figure 6.2 shows the distribution of the users based on number of logins. The females logged into the system more frequently than the males, as Figure 6.3

strongly indicates. A female user logged in to the system in average 3.89 times and a male logged into the system an average of 2.13 times, which is a quite significant difference. The male user that logged in the most times logged in only four times, while there is four females that logged in four times or more. The tendency is also clear at the other end of the scale; three boys logged in one time, while only one girl did the same.

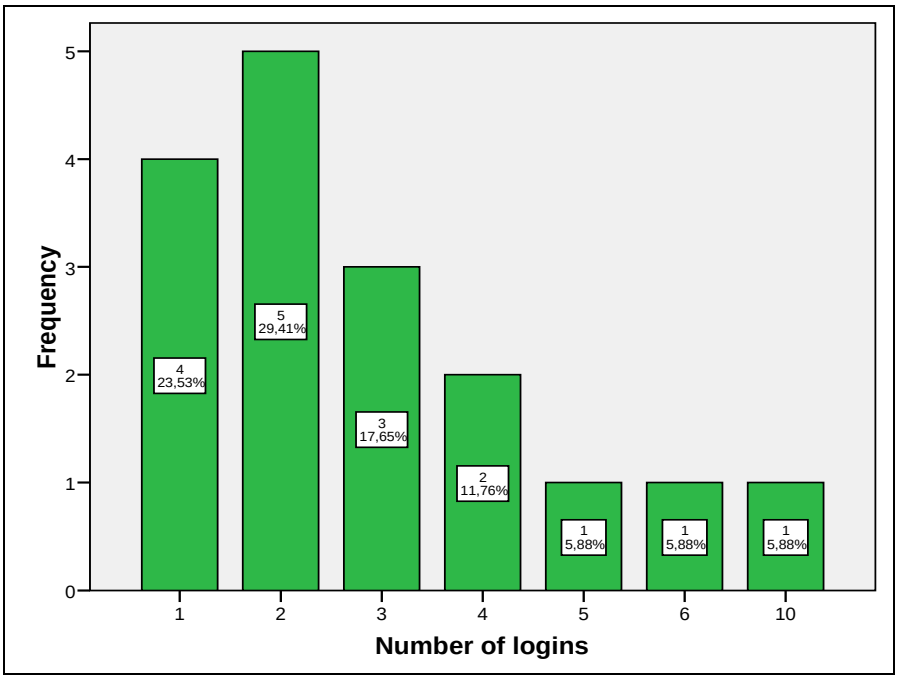

Figure 6.2: Number of logins to The FriendRadar

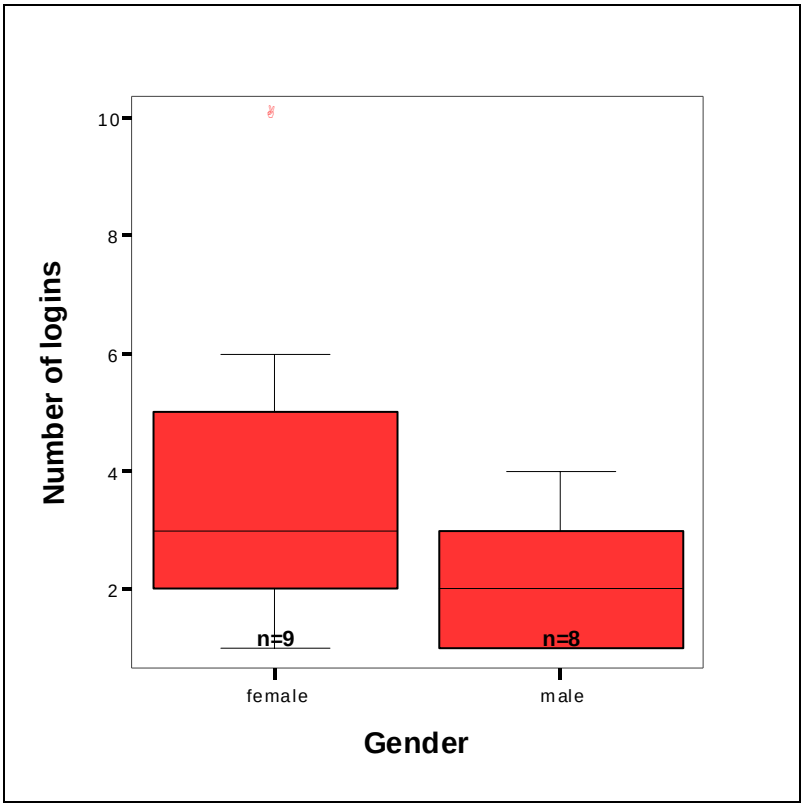

Figure 6.3: Number of logins based on gender

Total number of times located indicates how long time the users has been connected to Wireless Trondheim. There were a total of 660 successful positioning attempts through GeoPos (There was 13077 requests to GeoPos that did not return any location). Each user was located on average 38.82 times and the median was 11 times. It was however an enormous variance. Table 6.1 also shows that some users never connected to the network, and some users were located many times, with 211 as the most. Since the locating requests are executed with an interval of either 30 seconds or two and a half minute, the user which is located 211 times can be assumed to have been in connected to Wireless Trondheim between 105.5 minutes (1 hour 45 minutes 30 seconds) and 527.5 minutes (8 hours 47 minutes 30 seconds). The number of times connected to Wireless Trondheim represents an approximate number of times the users has successfully connected to Wireless Trondheim. The users connected to Wireless Trondheim 48 times, which gives an average of 2.82 times per user. As shown in Table 6.1, only three users did not connect to Wireless Trondheim at all.

Figure 6.4 show box plots of number of times located and connected to Wireless Trondheim distributed by gender. The tendency is opposite compared to number of times the users logged in to The FriendRadar; male users were more frequent users of Wireless Trondheim compared to the females. Of the tree users that never connected to Wireless Trondheim, there were two females and one male. The male user (user 10) with no connections only logged in to The FriendRadar once, while the females that did not connect to Wireless Trondheim logged in to The Friend Radar as much as six (user 2) and five times (user 4), which are second and third most times respectively.

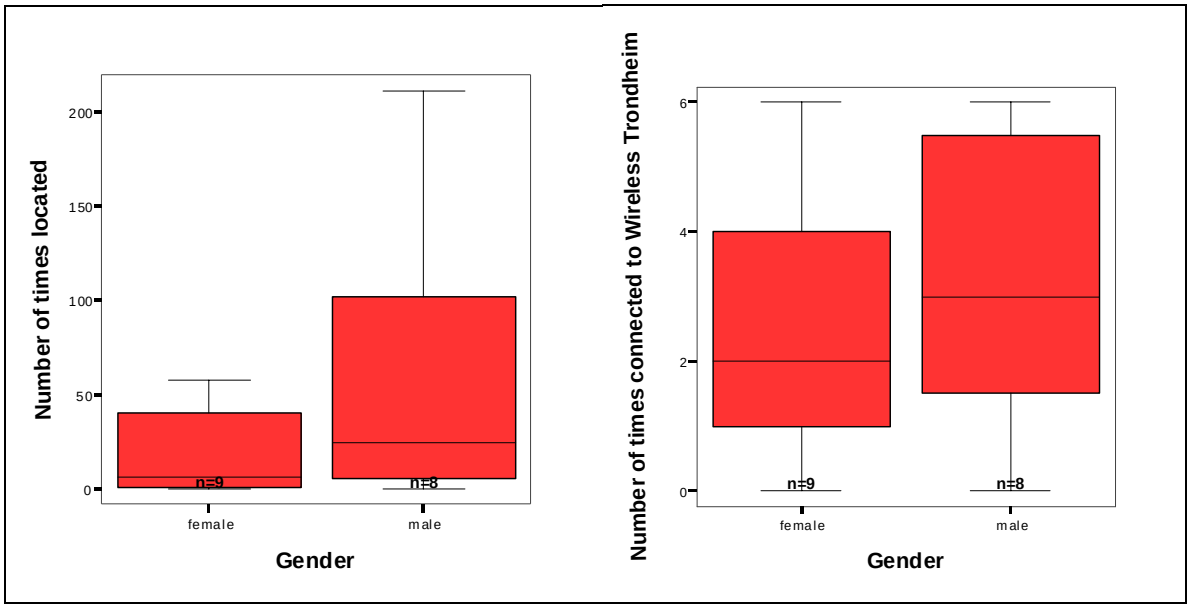

Figure 6.4: Number of times located and times connected to WT based on gender

Even though some users have been connected to Wireless Trondheim a considerable number of times and occasionally over quite long periods of time, it has only happened three times that two or more users has been connected to Wireless Trondheim at the same time. One of the times there were three users connected at the same time, the two other times there were two users connected at the same time. In two of the three occasions the users that was connected simultaneously was friends, which means that they theoretically should be able to see each other on the map. Table 6.3 show information about these occasions, with the numbers of users that participated in an occasion, if they was friends or not, if any message was sent between the users during this time, which users that was involved, the length of the period they was connected at the same time and which date it happened. The first occasion, that happened 25th of April, includes three users which all were friends with each other. User 5 and 11 was located at the same spot during the whole occasion (at the school). User 14 seemed to be moving away from the two others.

Table 6.3: Users that were connected to Wireless Trondheim at the same time

Num of users	Friends?	Message	Users ID's	Connection	Duration	Date
3	Yes	No	5, 11, 14	Probably (5, 11)	1 hour	25.apr
2	Yes	No	6, 15	Probably	30 minutes	30.apr
2	No	No	8, 12	No	1 minute	03.may

In the second occasion (30th April) the two users was located in the same area. Figure 6.5 shows their movements placed on a map during the time they were able to be located simultaneously. Both of the users started at the same location (a famous recreation place called "Marinen"), but at different times. User 15 started at one part of Marinen, and moved to another place before user 6 arrived. They was however both at Marinen in the same time. User 6 was first located at the spot where user 15 started, but seven minutes after user 15 has been located at another place at Marinen. User 6 kept on the same location the whole time (20 minutes), while user 15 moved around in the area around the user (from 50 to 200 metres) which indicates that there probably is a connection between the locations of the two users. The locations of user 6 around Trondheim Torg (which is next to most of the users' school) are not a part of the occasion, since they are made over an hour after user 15 was disconnected from Wireless Trondheim, but are still interesting since this is the place where user 6 could have seen user 15 for the last time. It is not possible to establish if their

movements are affected by the system or not. The third occasion shown in Table 6.3 did not involve users that were friends with each other, and are not being further analysed.

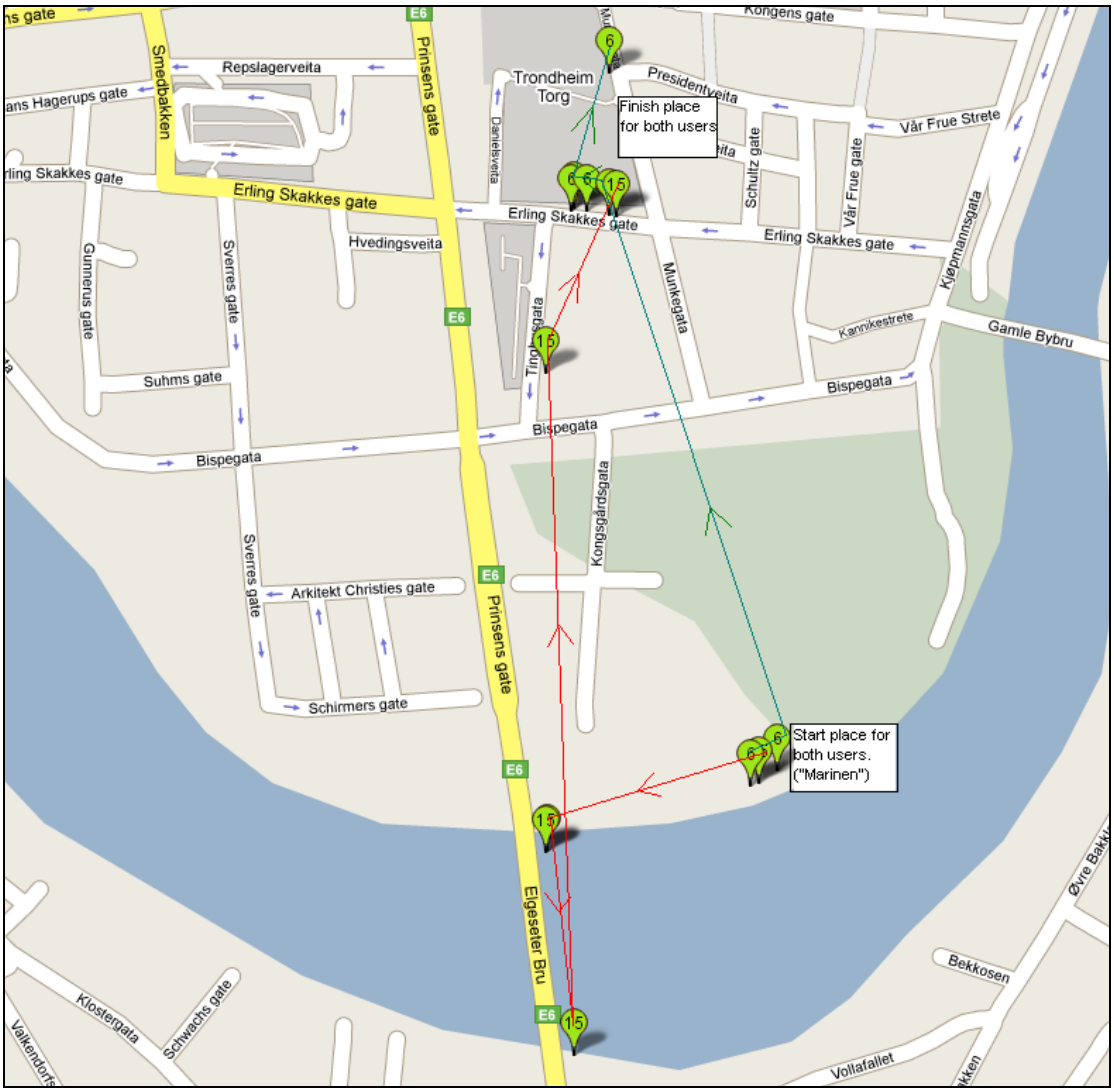

Figure 6.5: The users' movements when logged on simultaneously

6.1.3 Friends

Each user had an average of 7.35 friends in The FriendRadar. Three users had no friends, which pulls the mean down. Male users had an average of 9.13 friends and a median of 11 and the females had an average of 5.78 friends and a median of 8, even though the girls logged in to the system more often. All friend connections had the privacy setting 'map', which means that there was no users that either not allowed a friend to only be able to locate them approximate or blocked their friends. Figure 6.6 shows that boys and girls sent about the same number of friend requests to other users (or accepted others), but the boys had definitely received more friend requests. The middle graph of Figure 6.6 shows one outlier in each gender. User 16 and 17 registered in the system late, and it seems they did not have enough time to connect to friends. This also affects the rest of the friend statistics. The rightmost graph in Figure 6.6 shows that the boys had more friends than the girls, as mentioned earlier.

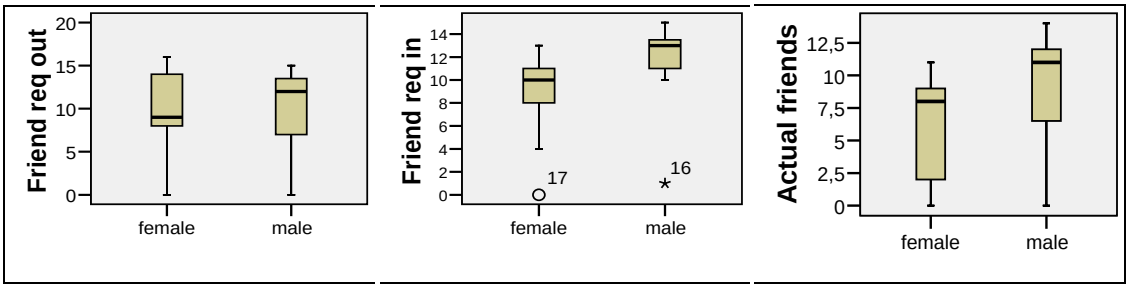

Figure 6.6: Friend requests and actual friends based on gender

6.1.4 Messages

It was sent a total number of 13 messages in the system, split over five senders and five receivers. Nine of the messages were read, and six of them were answers to other messages. None of the messages appears to be related with the registered locations of the users. Table 6.4 shows details about all the messages sent in the system. Notice that all the messages was sent within the first week of the test period, and 10 of 13 messages was sent during the first day.

Table 6.4: Messages sent in The FriendRadar

id	date	type	sender	receiver	rd (read)	answer_to
1	23.04.08 10:57	request	5	11	1	0
2	23.04.08 10:57	request	13	6	1	0
3	23.04.08 10:59	request	5	13	0	0
4	23.04.08 11:00	request	5	6	1	0
5	23.04.08 11:04	inform	10	12	1	0
6	23.04.08 12:50	Neg_answer	11	5	1	1
7	23.04.08 12:52	inform	11	6	1	0
8	23.04.08 16:15	Pos_answer	6	5	1	4
9	23.04.08 16:16	confirm	6	11	1	7
10	23.04.08 16:16	inform	6	13	0	0
11	25.04.08 13:47	request	11	6	1	9
12	25.04.08 14:14	request	11	13	0	0
13	29.04.08 18:47	Pos_answer	6	11	0	11

6.2 Questionnaire

This section presents the results from the questionnaire.

6.2.1 Participants

The information about the questionnaire was sent out to all the 28 pupils of the subject where the test persons were collected from, both the pupils that participated in the testing and those who did not. This lead to 16 responses, where 9 was from females and 7 was from males. 14 of the participants answered that they received an iPod and participated in the testing of the system. This question (14) was somewhat double-barrelled; it both asked if the users had received the iPod and if they have participated in the testing of the system. As shown in the previous section, it was actually six users that received the iPod, but never logged in to The FriendRadar. Figure 6.7 shows however, that there were five users that never logged in to the system from the iPod and two that never logged in from a regular computer, but only one that never logged in at all.

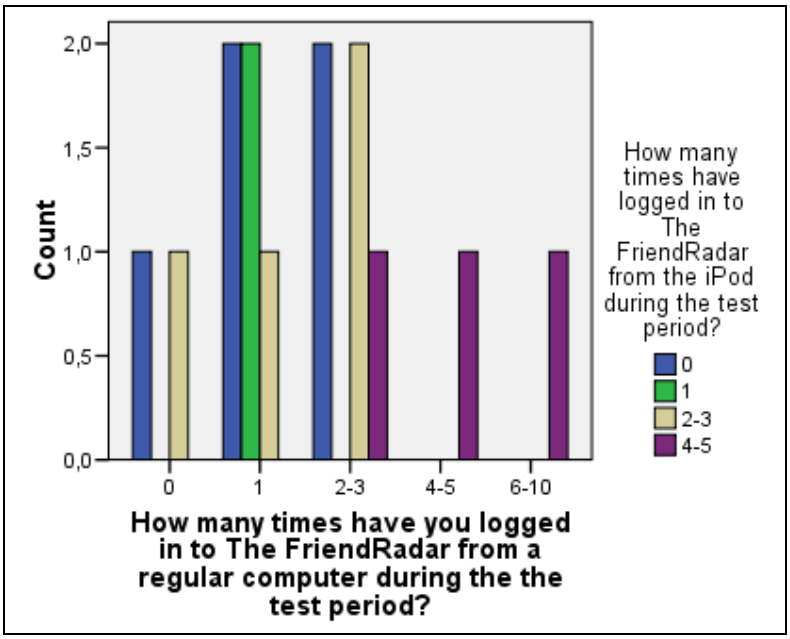

Figure 6.7: Times the participants has logged in to The FriendRadar.

All the participants own both a mobile phone and an mp3-player. 10 of the participants own a laptop and one of the participants owns a PDA. Four participants said they have some other mobile devices in addition to those mentioned here.

All 16 participants had a profile on Facebook, and Figure 6.8 shows the number of friends the participants had on Facebook (left) and how often the participants log in on Facebook (right). The figure shows that the participants are very active users on Facebook, since more than half of the participants have 200 friends or more and only two of the participants log in more infrequently than daily. There seems to be no connection however, between the number of friends and how often the users log in since users with fewer friends logs in both frequent and infrequent (in this scale) and the other way around. Four of the users state that Facebook is an important part of their life. Three of these four has given a reason for it:

"Because there is always something that happens there"

"Share pictures with friends"

"Keep in touch with people and keep myself updated. I feel 'social' in a way."

There were no large differences between the genders in the number of friends and in how many times the users logged in to Facebook. There was a significant difference however between the genders of the users that stated Facebook as an important part of their life. All four users that feel that Facebook is an important part of their lives are females, which mean that four of nine girls feel this (Almost 45 percent). All seven boys stated that it is not an important part of their lives. Most of the users have given reason for why they have a profile on Facebook, which was often described with what they used it for, which is a later question. These two questions are however closely related, and Table 6.5 summarises what users said they were using Facebook for. No categories are mutually exclusive, which means that a user can be registered in several categories. In addition to what Facebook is used for, two users said that they are registered because their friends are registered. When the users was asked why they felt that Facebook was not an important part of their life, almost everyone said that it was a nice thing, but it was not a necessity of their life and

that other things like school was more important. They used it however like a tool to keep in touch with others, both local and distant friends and family members.

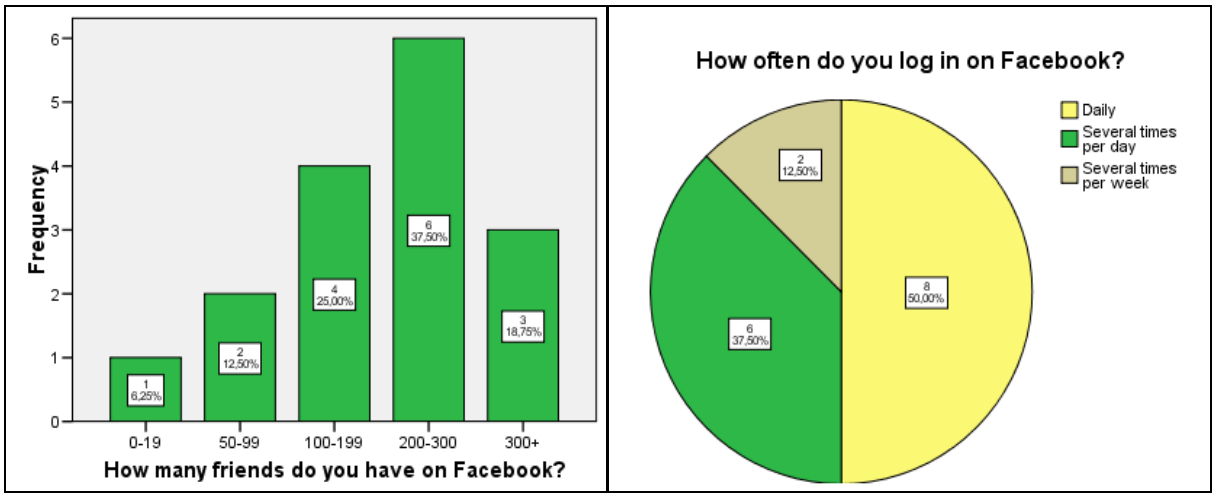

Figure 6.8: Friends and log in frequency on Facebook

Table 6.5: What is Facebook used for?

Category	Reason	Frequency
1	Communicate (talk) with friends	14
2	Watch pictures	12
3	Keep updated	6
4	Share pictures	4
5	Get to know new friends	1
6	Nose around	1
7	Play poker	1

The participants were asked what they think about privacy in Facebook, and not everyone had a lot to say. Three participants said that they are satisfied with Facebook's privacy and six participants said that they feel it is not good enough. Examples are:

"There are some users that have had some unwanted things published about themselves on Facebook. This is sad, and I don't think many users are aware of the consequences it can have to publish pictures of others that you have been told not to publish."

"I think that one is vulnerable, but I don't care, it's not that important."

6.2.2 Usage of the iPods

When it comes to usage of the received iPods, six of the users stated that they have used it a couple of times, two stated that they have used it fairly much and six clamed that they have used it a lot, as shown in Table 6.6.

Table 6.6: How much the participants have used the iPod

Category	Frequency	Percent
Used it a couple of times	6	37.5
Used it fairly much	2	12.5
Used it a lot	6	37.5

When asked to range how much they have used it at home, at school and other places (on a 1 to 5 scale), at home got slightly higher score than other places. It was used least at school. All three places had a fairly high average value however, with 3.14, 3.07 and 2.50 respectively. When asked what they used it for, the different activities are ranged in Table 6.7. It shows that, not surprisingly, listen to music was the far most popular activity. In fact, 8 of 14 users rated listen to music to 5 on the scale. It also seem that 'everyone' used the iPod to surf the web, as all except one user has rated this activity to 2 or higher at the scale.

Table 6.7: Activities the iPod was used for

Range	Activity	Average value
1	Listen to music	4.49
2	Surf the Web	2.93
3	Watch saved videos	2.14
4	Be at YouTube	2.14
5	Use The FriendRadar	1.64
6	Other things	1.50

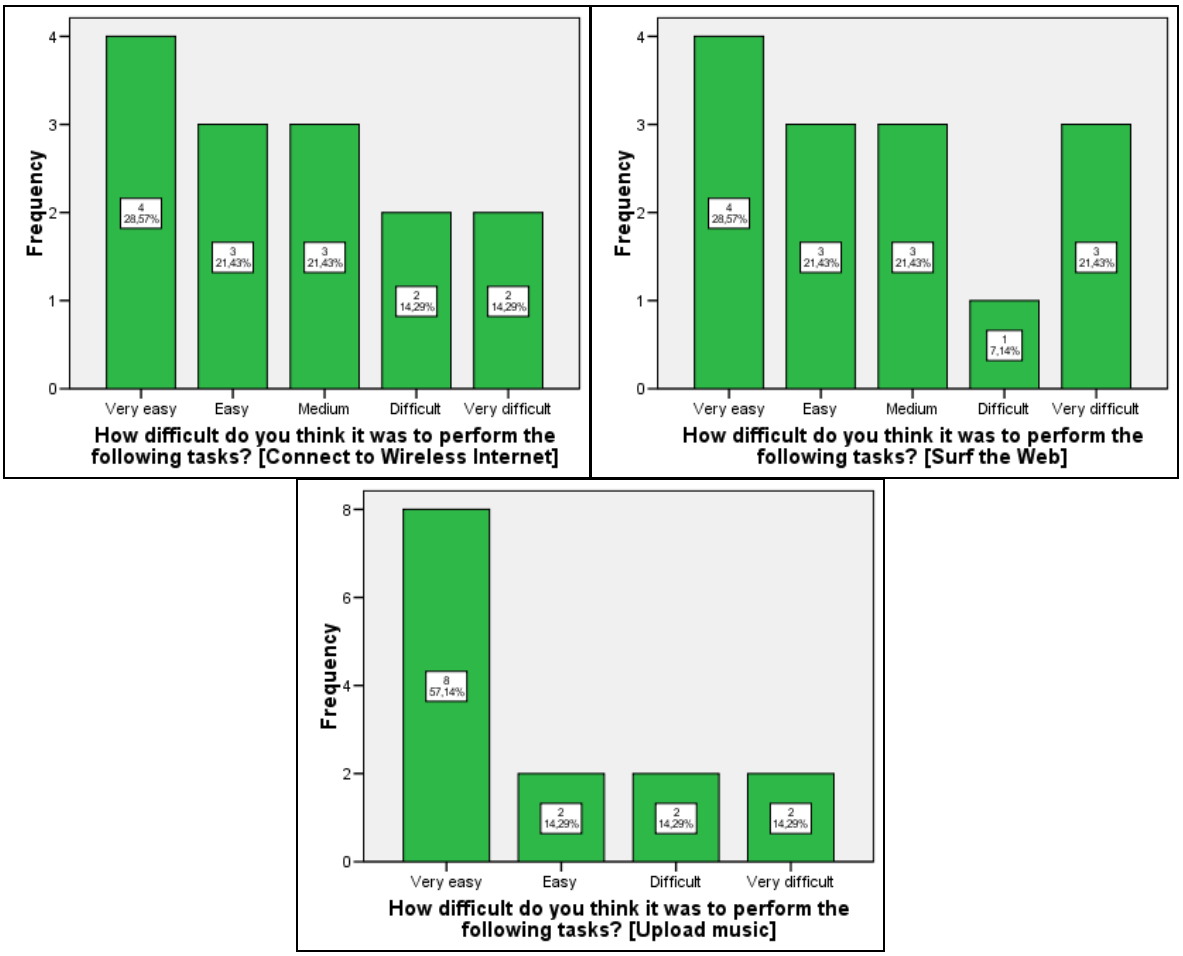

Figure 6.9: Difficulty the users had in using the iPod

Figure 6.9 shows how difficult the users found the tasks of connecting to wireless internet, surf the web and upload music to the iPod was. In general, the users seemed to find all tasks quite easy, especially uploading music. Each task had only four users that found the task either difficult or very

difficult. The users that find it difficult to connect to wireless internet are the same users that find it difficult to surf the web, which is quite naturally. One user thought all tasks was very difficult, and the three others that thought uploading music was difficult were spread from very easy to medium on the two other tasks. Figure 6.10 shows how difficult the task was distributed on gender. The clear tendency of the graphs in the figure is that the males thought the three tasks were easier to perform than the females.

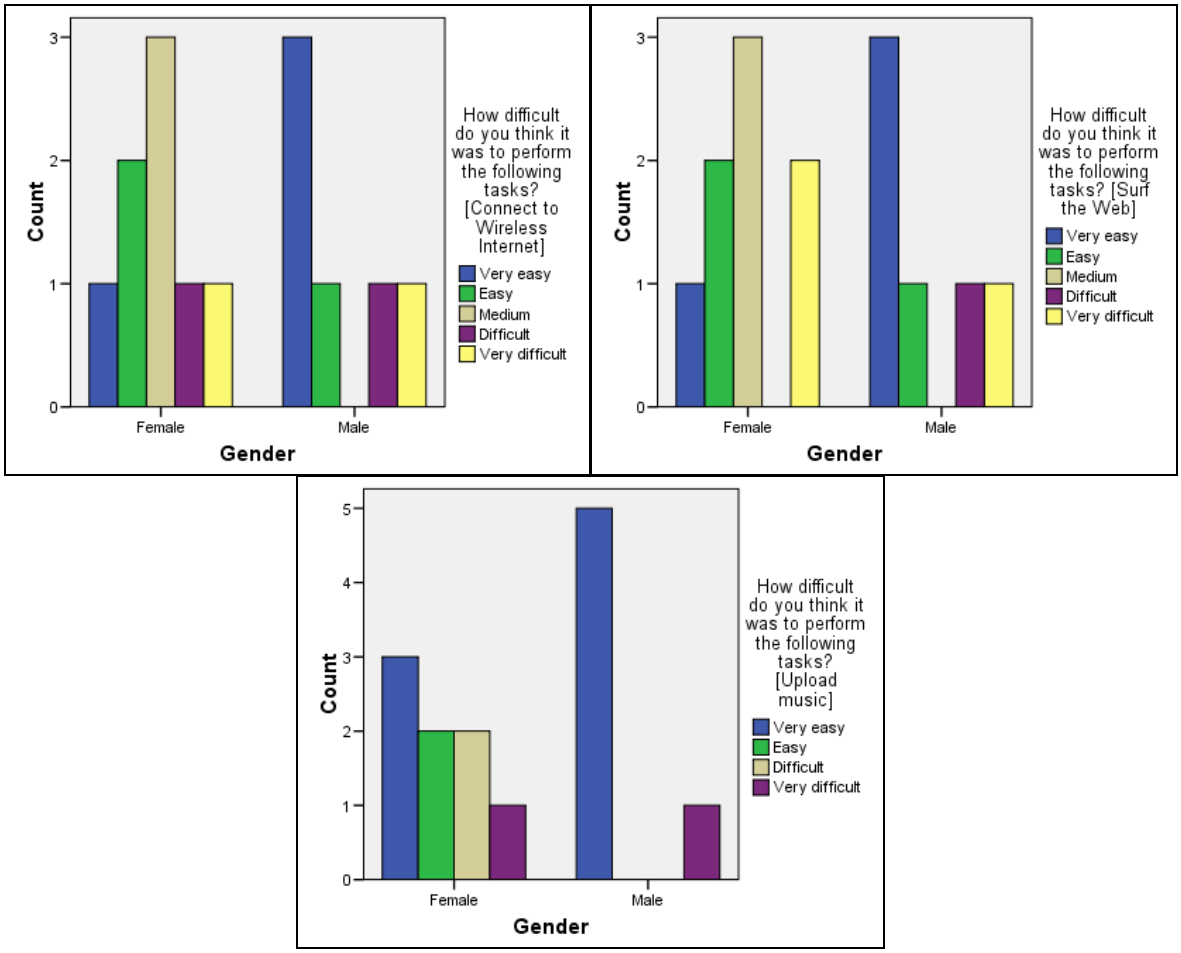

Figure 6.10: Difficulty the users had in using the iPod based on gender

Figure 6.11 shows that users tried to connect to Wireless Trondheim more times than they actually managed to connect to Wireless Trondheim, which is natural. But the differences here are so obvious that it is clear that users had difficulties with connecting to Wireless Trondheim. As Figure 6.12 shows, the users that have never managed to connect to Wireless Trondheim have tried to connect between four an ten times. The only participant that has managed to connect as many times as tried to connect is the user that had tried to connect the fewest times, namely 2-3 times. The impression that the users had difficulties with connecting to Wireless Trondheim is further strengthened by the answers of question 21, where 13 of the participants felt that the coverage of Wireless Trondheim was too bad to be used in practice. The three remaining users said that they did not know if the coverage was good enough, and two of these had not received any iPod. In this case there were no significant differences between the genders, both the males and females tried and managed to connect to Wireless Trondheim in the same extent. One notable thing about the data presented in the right graph in Figure 6.11, is that the participants of the questionnaire has in average connected to Wireless Trondheim fewer times than registered in the actual data. Either the

population from the questionnaire did not include those that used Wireless Trondheim the most, or users had an impression that they actually managed to connect to Wireless Trondheim more rarely than they actually did.

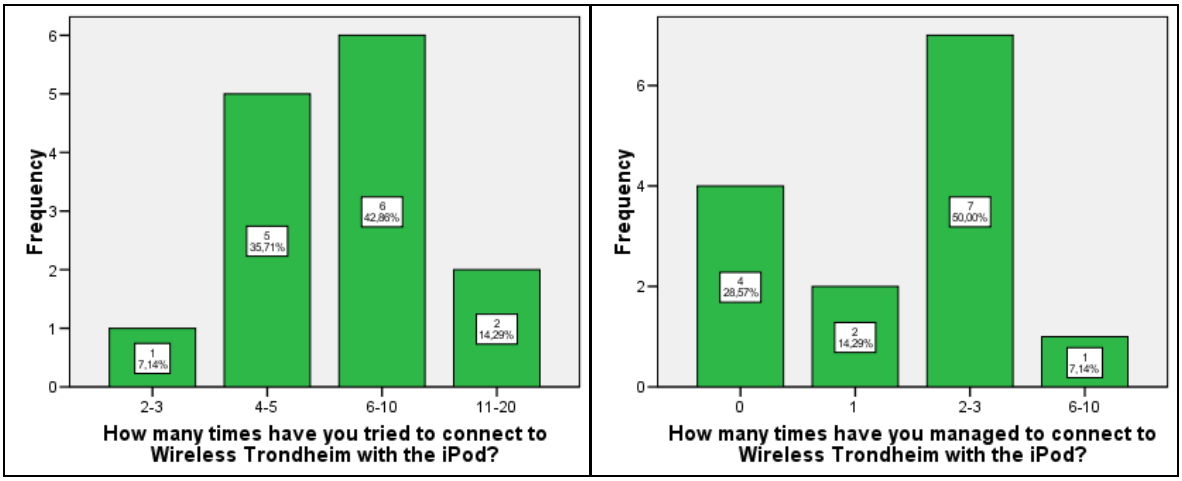

Figure 6.11: Tried and managed to connect to Wireless Trondheim

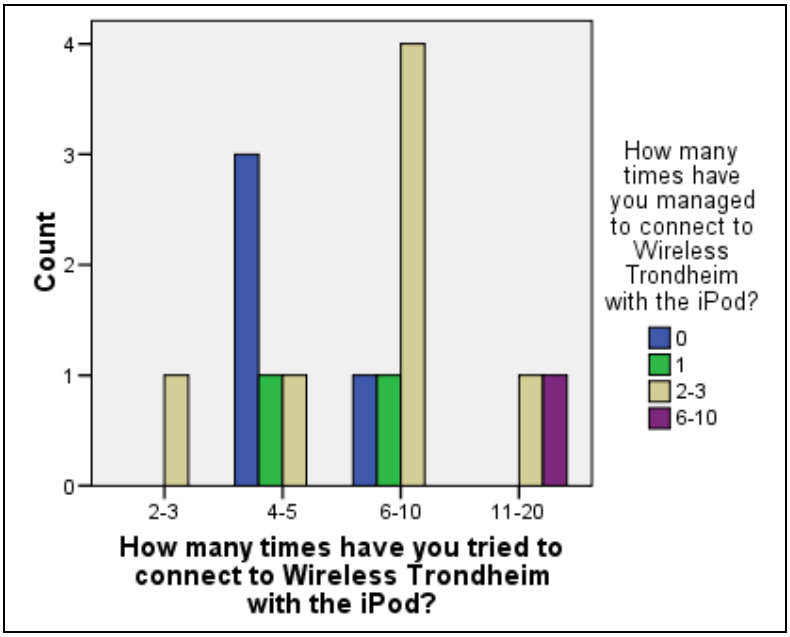

Figure 6.12: Managed to connect to Wireless Trondheim based on times tried

6.2.3 Usage of The FriendRadar

The actual usage of The FriendRadar has been logged and is presented in Section 6.1. The data presented here are based on what the respondents remember, and are not as accurate as the information in Section 6.1. Here however, the answers from various questions can help drawing lines between factors and identify which kind of users that want to use the system and which that will not use it. Answers that are substantiated by text answers can also give a sense of not only what the users do, but why they do it.

Figure 6.13 shows how many times the users have logged in to The FriendRadar from the iPod and from a regular computer. It shows that five users never have logged in to the system from the iPod and two users have never logged in from a computer. The users that actually has logged in from the iPod however, have logged in more often from the iPod than from a computer. Figure 6.7

shows a graph that combined the times users have logged in from a computer and from the iPod. It shows that one of the respondents have never logged in at all, in addition to the two respondents that did not receive an iPod. One user has logged in from the iPod (2-3 times), but never from a computer and four participants has logged in from a computer (two 1 time and two 2-3 times), but never from the iPod. The remaining eight respondents have logged in both from a computer and from the iPod. The users that have logged in most from a computer are the same users that has logged in most times from the iPod.

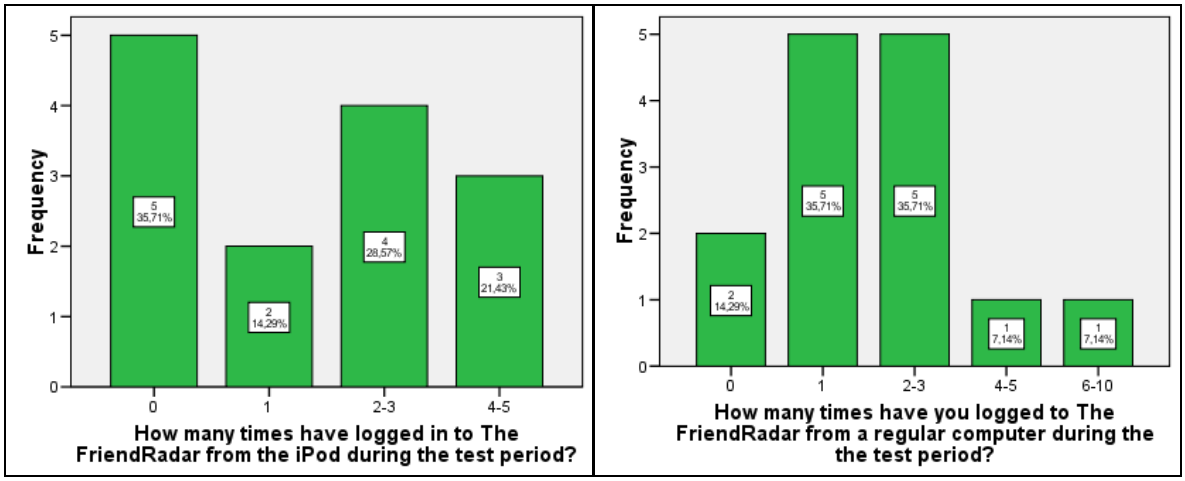

Figure 6.13: How many times the users logged in to The FriendRadar from the iPod and from a regular computer

Figure 6.14 (left part) shows how many friends the respondents stated they had on The FriendRadar, and it shows that it corresponds fairly well with the real numbers of friends registered in the system. The right part of Figure 6.14 shows that the two participants with no friends, never logged in to The FriendRadar from the iPod and that the three participants that logged in with the iPod 4-5 times all had 11 or more friends. The tendency is therefore that the more friends a user have, typically over ten friends, the more often the user logs in with the iPod.

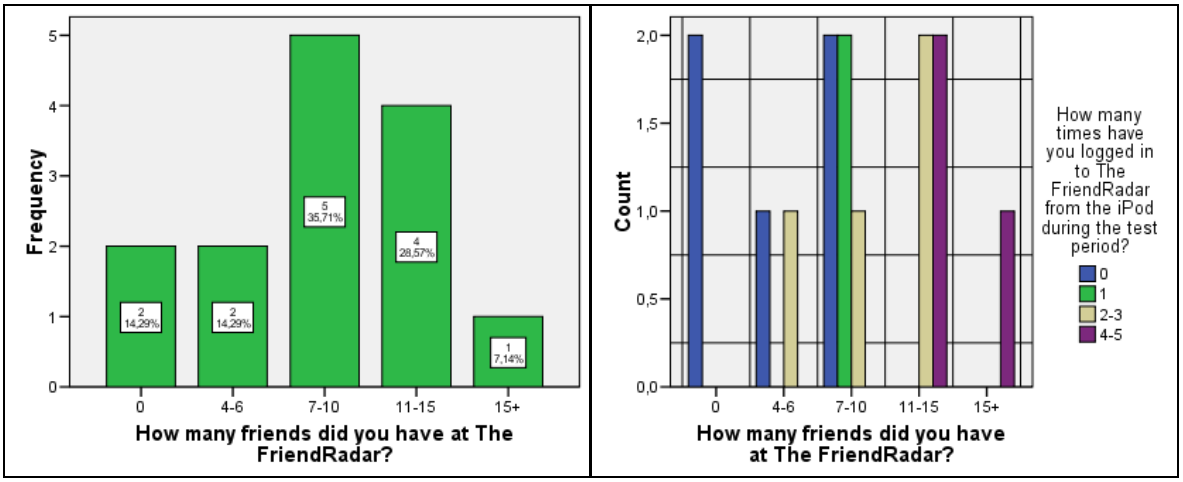

Figure 6.14: Friends in The FriendRadar

Figure 6.15 shows six of the respondents logged in to The FriendRadar with the intention to check their friends' location. Of these six, two states that they checked one time, three states that they checked two times and one states that she or he checked five times. The five participants that never logged in from the iPod are of course among the eight participants that said they never

logged in to The FriendRadar to check their friends' location. The graph to the right in the figure shows a tendency that more of the respondents with many friends (except the one with more than 15 friends), have tried to check their friends location. The participants that stated that hey never had logged in to check their friends' location was asked to substantiate why they did not do it. Seven of the eight that answered no, gave an answer and all of these seven blamed technical problems as the main reason. Wireless Trondheim was mentioned by all the users as the main problem. A couple of interesting answers are:

"*Because I rarely am inside the coverage area of Wireless Trondheim*" (7-10 friends)

"*I can imagine that it would be of more interest to log in to The FriendRadar if I had more friends (like MSN or something) where there always is someone logged in, but since nobody was logged in each time I checked, I lost the interest. Another thing is that even if all the test persons was downtown, the network was very bad, and almost none of the users managed to log in on Wireless Trondheim*" (More than 15 friends)

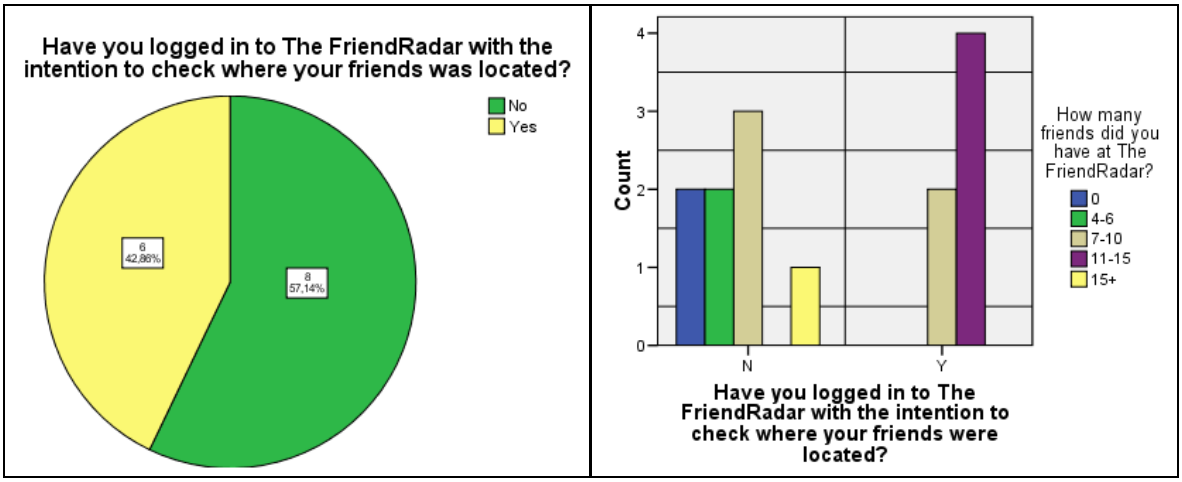

Figure 6.15: The numbers of times users has logged in to check their friends location

As shown in Table 6.3, there were five users that had the possibility to see some of their friends on the map during the test period. Figure 6.16 shows that of the participants that answered the questionnaire, five of them said that they have found some friend on the map of The FriendRadar, which make it probable that all the users that actually have seen some other users on the map has answered the questionnaire. The users blamed, with one exception, either Wireless Trondheim or their own incapability to log in as the reason for not finding any friends. The one exception said however: "*Because nobody has been logged on when I was.*" which is blaming the low user mass that probably is a consequence of the technical issues concerning Wireless Trondheim. Of the five users that have seen some of their friends on the map, two stated that they have tried to find them physically after locating them with The FriendRadar and one of these two has actually managed to find one of the friends. The one participant that did not manage to find the friend, answered when asked to write why she could did not find the friends that "*I have not tried*". This means that only one of the participants tried to find the friend, and this participant succeeded in doing it. The users that did not try to find the friend(s) they located on the map, and gave a reason for it, gave the following reasons:

"*I did not have the energy to do it at the time.*"

"*The opportunity has not been there.*"

"Because I haven't had the need to do it."

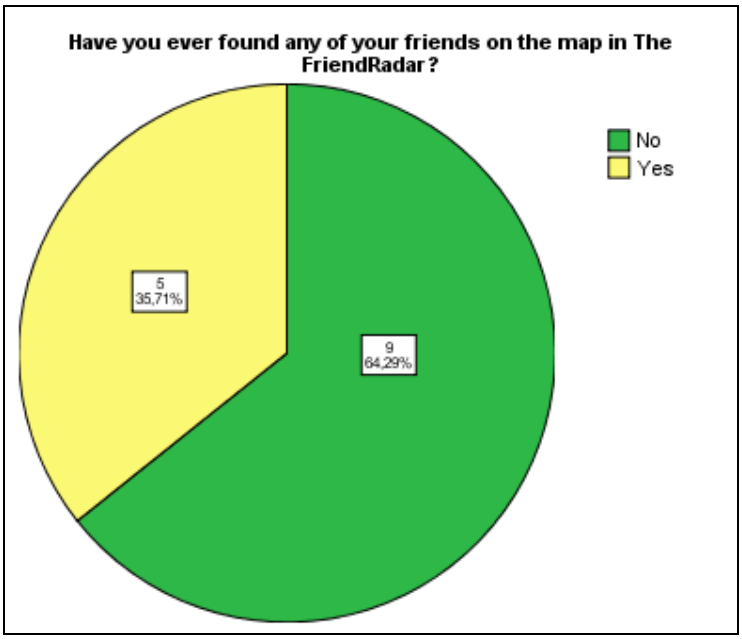

Figure 6.16: Have users seen some of their friends on the map?

Question 50 asked the users if they wanted to use a similar system as The FriendRadar if all the shortcomings of the system were fixed. Figure 6.17 shows that 13 of the participants stated that they would use such a system which are over 80 percent of the users. Two of the three that was negative to such a system had received an iPod, which implies that one of the positive ones did not receive an iPod and did not participate in the experiment. All the three participants that answered no to use a similar system was females and surprisingly, as Figure 6.18 shows, two of the users that would not use a similar system stated that Facebook is an important part of their lives. There were not significant differences between the yes and no answers to question 50 when it comes to number of friends on Facebook, friends on The FriendRadar and number of times logged in to The FriendRadar.

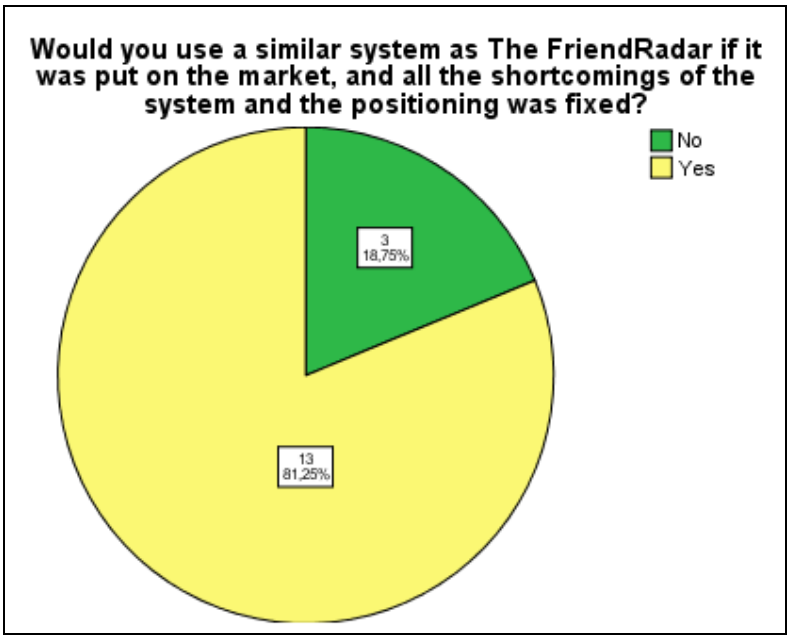

Figure 6.17: Will the participants use a similar system?

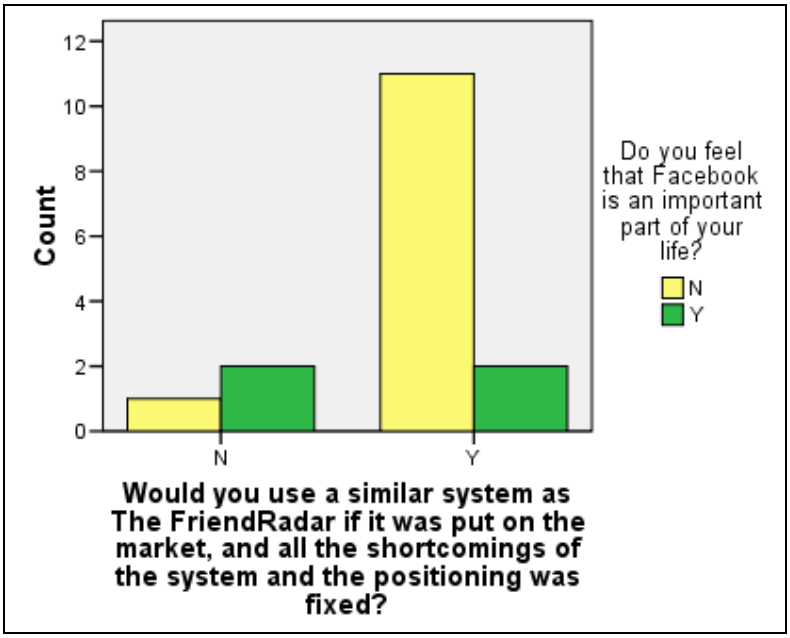

Figure 6.18: Facebook importance based on interest in a future system

The participants were further asked to write what they thought of the concept of The FriendRadar, and the possibility to locate their friends. Everyone that answered yes to question 50 answered the question and was naturally positive to the concept, except one respondent that said "*it was tiresome and unnecessary*". Only one of the respondents that said they would not use a future system answered, and the answer was: "*Okay opportunity for those who want it*". Some of the other positive answers were:

"*I think the concept is exciting, original and fun.*"

"*Very good! Great that one can find each other and that one can turn it off if one want to.*"

"It is a nice concept for finding your friends, but I think it will be used more by parents that want to know the location of their children."

"I think it is a very interesting concept, I don't know if it is any reason why you have to be connected to Wireless Trondheim, but it would be cool if one could be connected to any wireless network because Wireless Trondheim is not good enough."

In general, the answers of the respondents showed great enthusiasm about the idea and concept of be able to locate their friends. The participants were also asked if they had any other comments concerning The FriendRadar. Many users used this field to express dissatisfaction with the quality of Wireless Trondheim:

"It was kind of boring that Wireless Trondheim never worked on my iPod."

"Wireless Trondheim did not have good enough coverage. It was slow and it did not work on my school (Katta[10])."

One user also said it was too few users on the system:

"I can not say how it was to use the system in practice, because too few users had the possibility to connect to it."

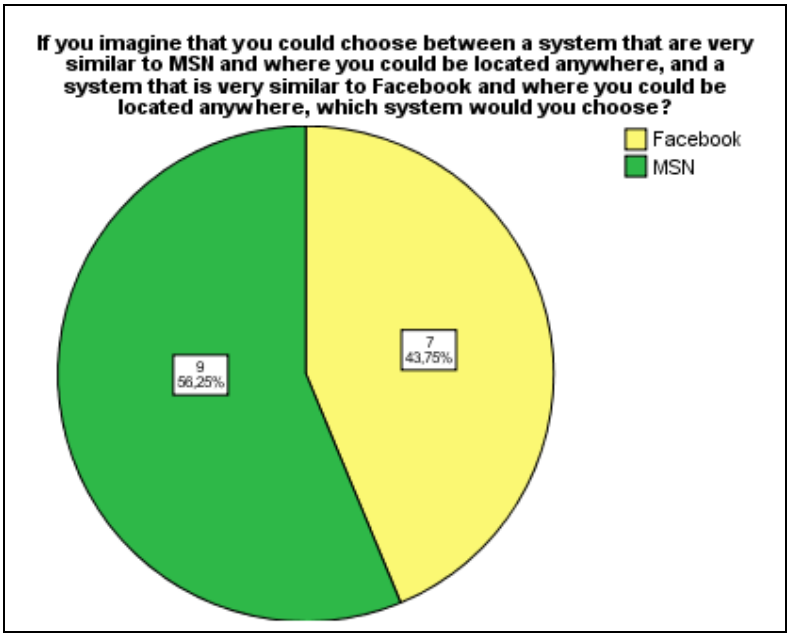

Figure 6.19: MSN or Facebook like system

In question 57 the users was told to imagine a future system where one could be located anywhere, and asked whether they would prefer a system that was very similar to MSN Messenger or a system that was very similar to Facebook, both of course with the positioning functionality. Figure 6.19 shows that MSN would be the preferred system by nine of the respondents, and seven would prefer a system with Facebook's functionality. A strange thing is that eight of the nine users that answered the MSN system, chose to substantiate their choice with a textual answer. Only one

[10] 'Katta' is a slang word for Trondheim Katedralskole, where the test subject was collected from.

of the seven that answered Facebook did the same. The users that answered Facebook wrote: *"It is about the same for me, but I use Facebook more often"*. Most of the respondents that answered Facebook were clearer about why they chose it, but they had very different reasons:

"Easier to communicate directly, that is what it is most need for."

"It is more 'social'."

"If one is going to be localised anyway, the MSN system I better, because it is more private."

"I feel that the MSN system is better. You don't need any web browser and I feel it demands less effort to log in there. It is just to turn on the computer, and you're logged in:"

"Have used MSN the longest, and feel safer with it."

Two more users said it was because it was better with direct contact, just as said in the first quote. One final user that said that she would prefer MSN said the following:

"Here is my answer in reality a mixture of the two systems. Where you could send direct messages to the users that are currently logged in, and a system that makes it possible to send messages to users that is not logged in , such as the person received the message the next time he logs in."

The left part of Figure 6.20 shows that the proportion of respondents that would prefer each system is almost the same in both genders, with one more respondent preferring MSN in each gender. The right part of Figure 6.20 shows that among the respondents that uses Facebook several times per day, Facebook is definitely the most preferred future system. Only two of eight respondents that state they use Facebook daily would prefer Facebook as the new system, and both respondents that use Facebook rarer than daily would prefer MSN.

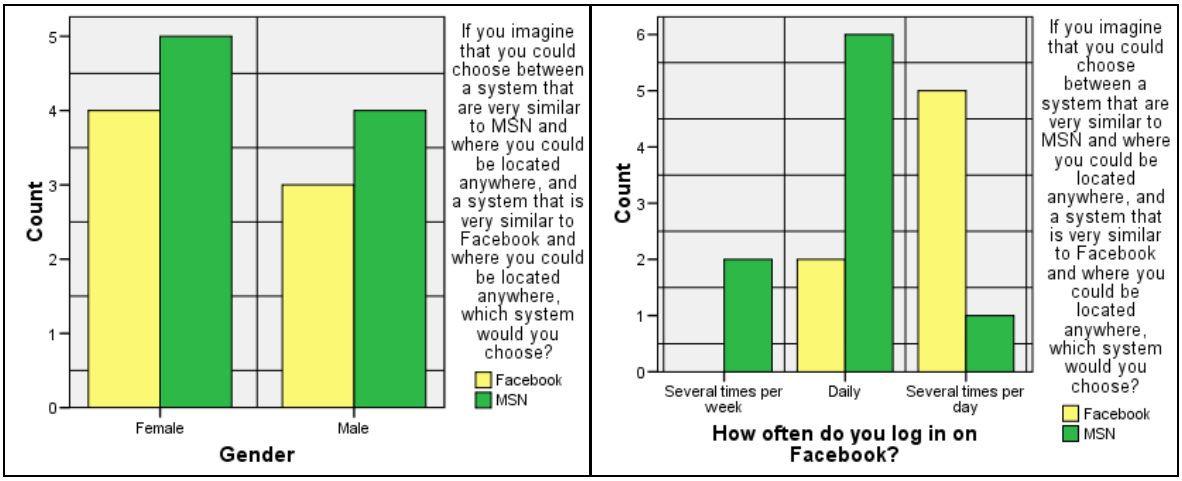

Figure 6.20: MSN or Facebook preference distributed in gender and usage of Facebook

Results from question 29 and question 30 which asked how many times the participants had tried and managed, respectively, to find themselves on the map of The FriendRadar are not presented because the results show that the respondents had clearly misunderstood these questions. The purpose was to get to know how many times the users had spotted themselves on the map, but many users said that they had spotted themselves fewer times than they have spotted others, which is impossible following the way the system was implemented.

6.2.4 The FriendRadar's influence to its users

As mentioned in the previous section, five users found their friends on the map at least one time. One of these users actively tried to find the friend(s) physically, and the user succeeded in doing so. This is a behaviour that is affected by The FriendRadar. The users that did not try to find their friends either said that did not have the opportunity, did not have the energy or that they had no need to do it at the present time.

Another way the system can influence the users' behaviour, is if the users do something they normally would not do as a consequence of their knowledge of that others can locate them (Research question 2.2). Question 41 of the questionnaire asked the participants if they have behaved different when their iPod was connected to Wireless Trondheim. None of the respondents said they had behaved in a different way. When asked how many times they deliberately avoided connecting the iPod to Wireless Trondheim because they did not want to be located, all the respondents said that they never had done it. When asked if they had left the iPod somewhere else deliberately to let others think they were located at a place they were not, all the respondents answered, not surprisingly, that they have not.

6.2.5 The users' privacy feeling in The FriendRadar and the need of privacy mechanisms

None of the participants felt that the iPod combined with the positioning-functionality of The FriendRadar had disturbed their personal life during the test period (Question 40). One respondent stated that he was afraid that the system administrator or others would use location information or other information about him to something he was not aware of (Question 47). When asked to explain what he was afraid of, he wrote: *"I don't know, I just remember that I thought about it"*.

One of the privacy mechanisms that were implemented in The FriendRadar was that users only could see their friends' location when they themselves could be located by others. In other words, the users' iPod had to be connected to Wireless Trondheim to see their friends' location. Question 25 in the questionnaire asked the participants if they would have used the system more, less or the same if they could see their friends' location independent on which network they were connected to. Figure 6.21 shows that five users would use it more and nine users thought that they would use it about the same as they did now. Notice that no users thought that they would use it less than they did now. Figure 6.22 show which users that have answered they would use the system 'The same' and which that have answered that they would use the system 'More' to question 25. The top left graph shows that it is generally the male respondents that will use the system more, as it is only one female user that says she would use it more. In fact, among the respondents that said they would use it about the same there are 78 percent females and among the respondents that said they would use it more there are only 20 percent females. The top right graph shows that it is the users that used the iPod the most, which stated they would use the system more if the friends could be located regardless of network. The bottom right and the bottom left graph shows that it is also the users that actually managed to use the iPod that would use it more, if they could locate their friends even if they were not connected to Wireless Trondheim themselves. The graph showing the same data with how much users has logged in to The FriendRadar from a regular computer are not shown, as the distribution in that case was fairly equal between both cases, which means that there was no differences between the respondents that said they would use it more and the respondents that said they would use it about the same. As mentioned earlier there was a field in the questionnaire where the users was asked to write any comments about The FriendRadar. One of the users that did not receive an iPod wrote: *"It is a great opportunity that you can deactivate The FriendRadar, such as it won't show. In addition is it great that one cannot see others when deactivated in such a way that espionage are avoided"*.

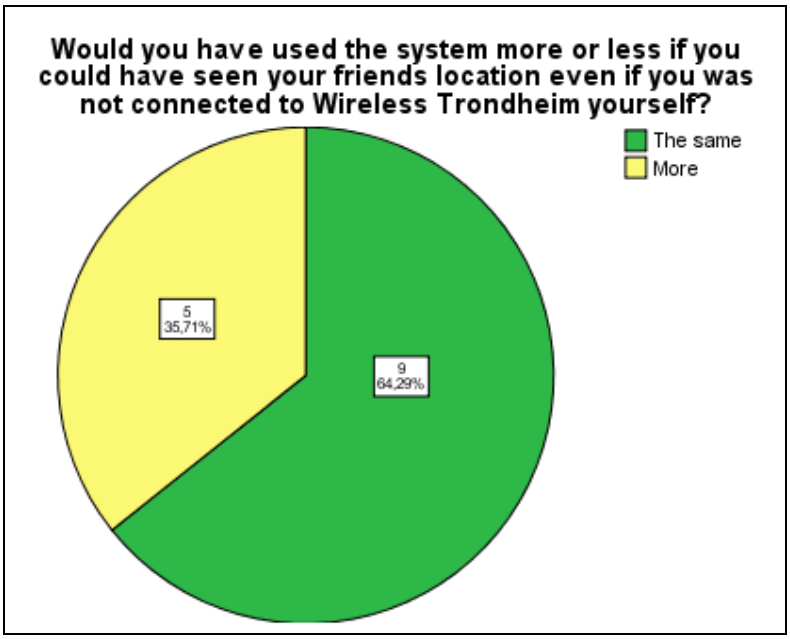

Figure 6.21: Would the system be used more or less if users could see friends' position regardless of network

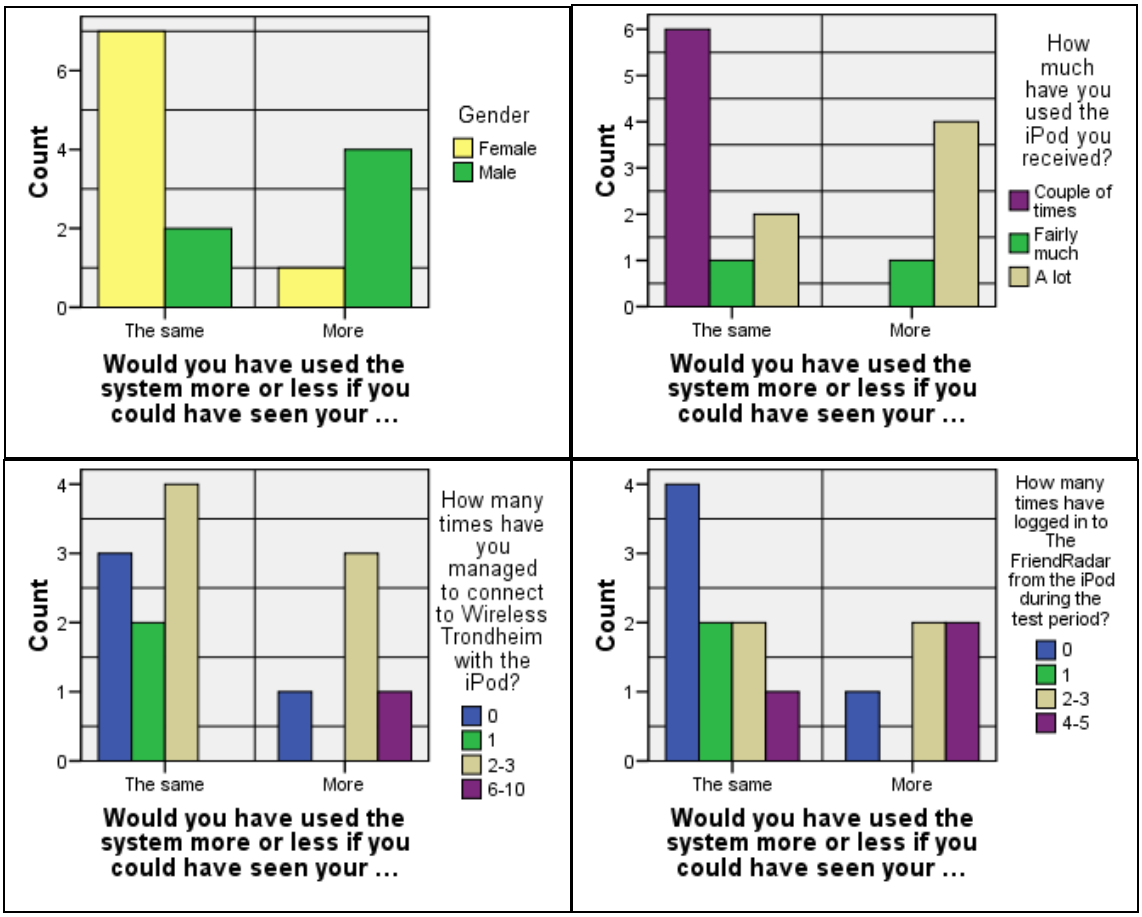

Figure 6.22: Various questions based on if the system would be used more or less if the user's friends could be positioned regardless of the user's network

Another security mechanism that was implemented in The FriendRadar was the possibility to choose the map privacy setting between friends. As described in Section 6.1.3, all the users chose the setting 'map' in all their friends connection, which means that all users allowed all their friends to see them on the map. Therefore as expected, all the respondents answered 'No' when asked if there were any friends they did not allow seeing on the map. The users had the possibility to comment this answer, and two users chose to do it:

"I can't really see any problems with that people know where I am."

"I did not have anything against that they could see where I was, since they only could see me in the city centre."

Figure 6.23 shows the number of users that thought they would use a 'lie' functionality if it was implemented in the system, which means that the users could say they were located at a different place than were they actually was (This was also explained in the Norwegian version of the question). Two users claimed that they would use it and six users said they would not use it. The remaining six did not know. The users had the possibility to comment their answer to this question. One of the users that answered yes commented and wrote: *"It would be fun to fool somebody"*. None of the users that answered that they did not know chose to comment, but all six that answered no commented their answer:

"Then it isn't 100% true. What's the purpose of The FriendRadar then?"

"If I did not want them to see me, I would just have logged off the network."

"Don't see any reason to lie about where I am located in the city centre."

"I can't see the problem with people knowing where I am."

"I can't see the problem. If I don't want people to know where I am, I could log off the network."

"Can't see any use of this functionality."

To summarise, five of the respondents felt that there was no use of this kind of functionality and one felt that this would ruin the concept of the friend radar.

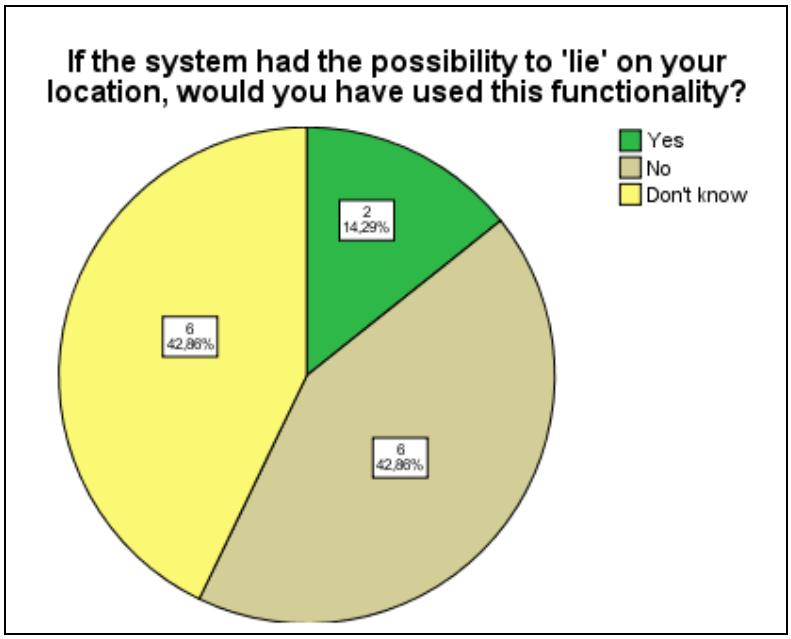

Figure 6.23: How many users that would use a lie functionality

Question 53 asked if the users would have used The FriendRadar more or less if the system would locate the user everywhere, independent of which network the user was connected to. It is important to note the difference between this question and question 24 which asks if the user would use The FriendRadar more or less if she could see her friends' location independent on whether or not she was connected to Wireless Trondheim. Question 24 is asking about if the users want location reciprocity implemented. Question 54 is asking if the users would use it more or less if they, and their friends, could be located anywhere in the world. The result of this question is shown Figure 6.24. One user would use it less, six would use it more and seven would use it about the same. The one user that would use it less substantiated this with: *"One needs a private life"*. It was four comments from the ones that would use it more:

"Then you could actually use it (the system)."

"It had given it a new dimension."

"If one didn't have to only use Wireless Trondheim. If one could see everyone on every network I would have used it more."

"I am not often inside the limits of Wireless Trondheim, so I would have used it more if it could be used in the entire city."

The comments from the users that said they would use equally much as today was:

"A little scary that it could not be controlled by me."

"Then I probably would not have allowed the same kind of friends to see where I was."

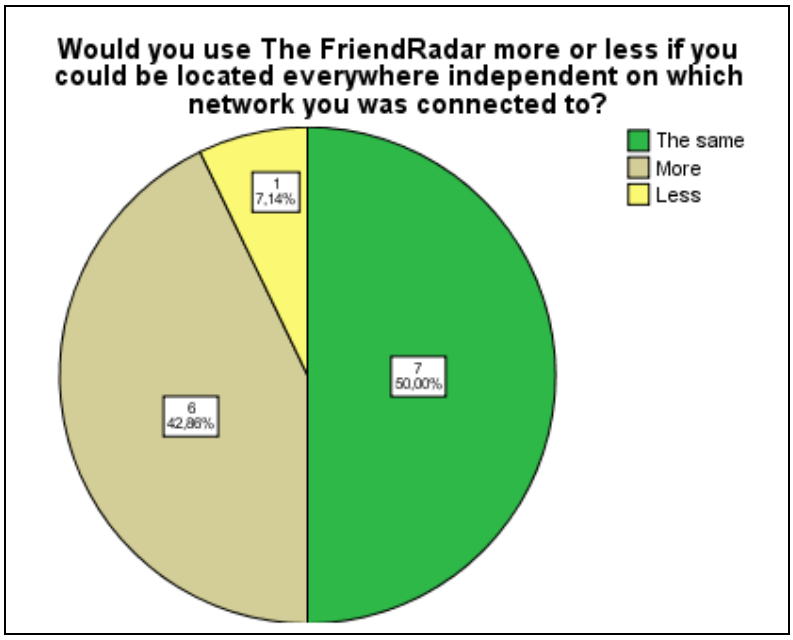

Figure 6.24: Would you use the system more or less if you could be located independent on network?

Figure 6.25 indicates that there is no connection between the answers of the users in question 24 and question 54. In fact, the only user that said he would use it less if one should be localised anywhere, would use it more if he could localise his friends in Wireless Trondheim, independent if he could be localised by them or not. Figure 6.22 showed four diagrams that showed what kind of users that answered what to question 24. The tendency is the same for all questions presented in Figure 6.22 when compared to question 54, except one: Figure 6.26 shows that the majority of the users that would use the system more have never logged in to The FriendRadar from the iPod, which was not the case with question 24. The figure also shows that the male users was dominant among the users that would use it more, and that the only user that would use it less also was male.

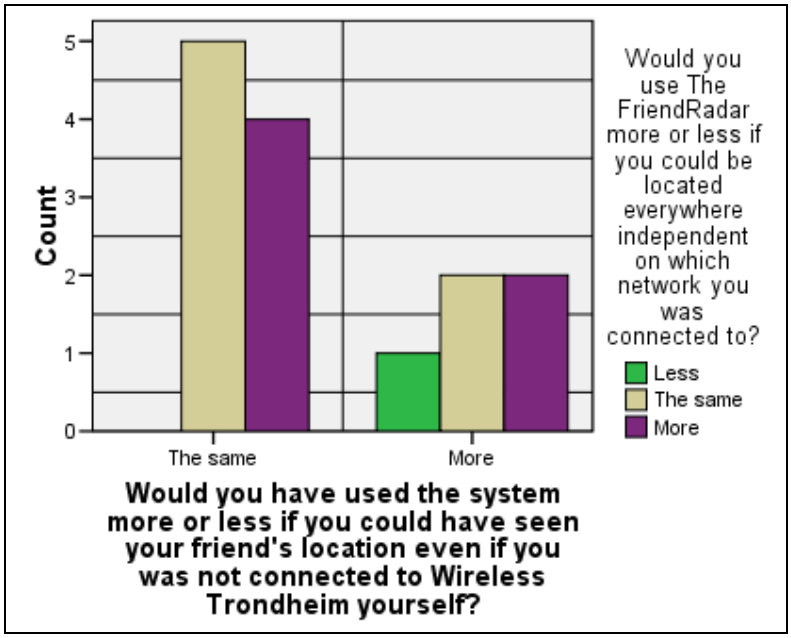

Figure 6.25: Crosstab between use the system more or less if located everywhere and locate without connected to Wireless Trondheim

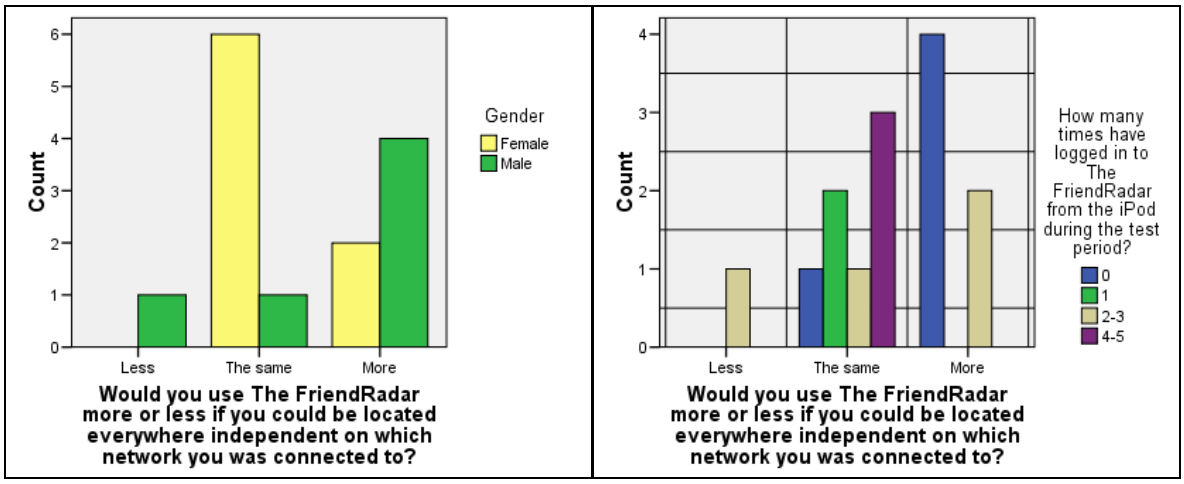

Figure 6.26: Gender and how many times the users that would use the system less, more or the same have logged in to The FriendRadar

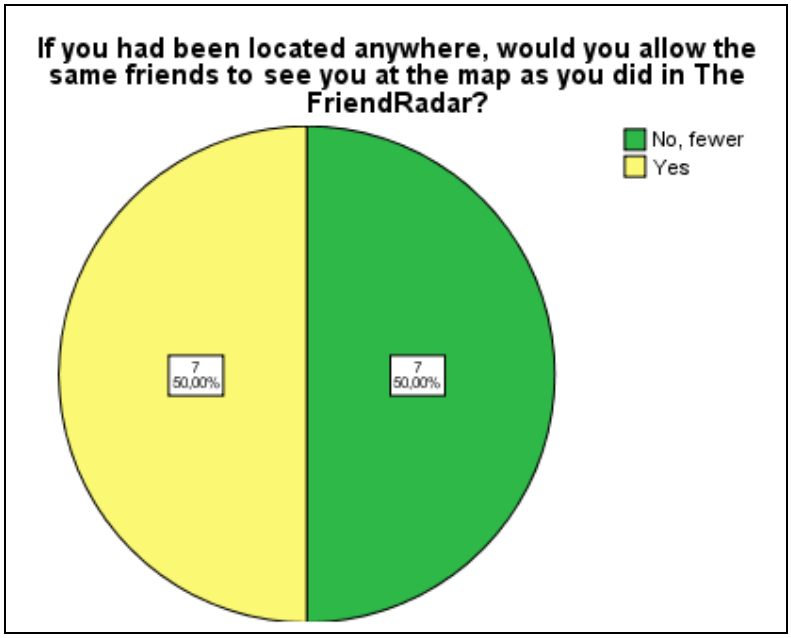

Figure 6.27: Allow the same friends to see you on the map?

Figure 6.27 shows that half of the respondents would have allowed the same friends to see them on the map in a system where you would be localised anywhere, and half would have allowed fewer friends. No respondents would, as expected, have allowed more friends, which in practice only were an alternative that was included to cover all possible answers, which made the alternatives exhaustive. The left diagram in Figure 6.28 shows that females are very dominant among the respondents that would have allowed fewer friends to see them on the map, as six of seven respondents were women. The opposite tendency is shown among the respondents that would have allowed the same friends. The right diagram in Figure 6.28 show that the proportion between the users that would prefer Facebook or MSN with positioning functionality is complete opposite in the two categories. The respondents that would allow fewer friends were dominated by MSN people, and the respondents that would allow the same friends were dominated by Facebook people.

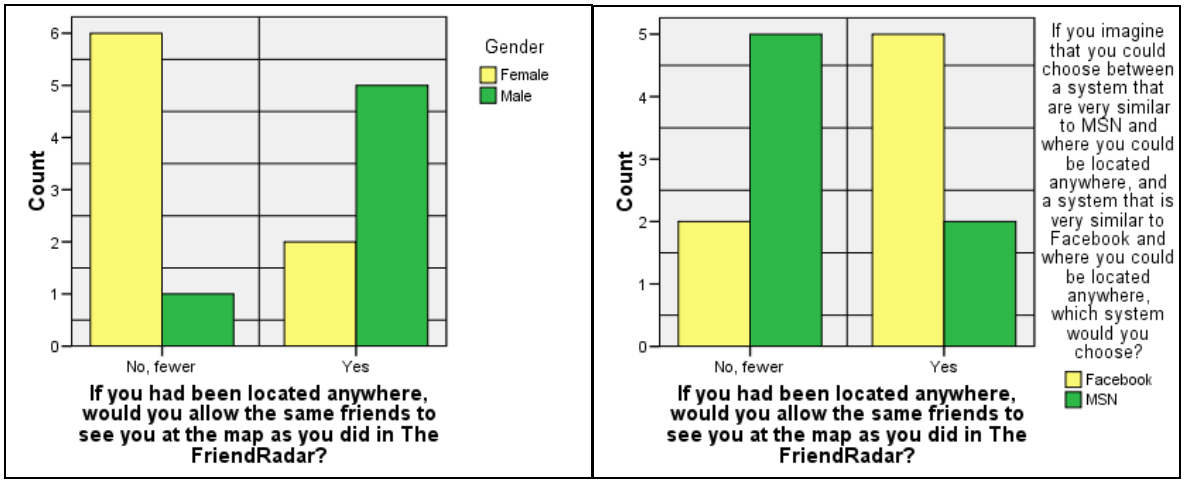

Figure 6.28: If users would allow the same friends to see the map split in gender and Facebook/MSN preference

Figure 6.29 show that if one could be located anywhere, 11 users (73 percent) think they would have used a lie functionality. This is in contrary to the number of users that thought they would use a lie functionality in The FriendRadar, which only was two users. By an unfortunate mistake was 'I don't know' not an alternative in this question, as it was in the lie question about The FriendRadar (Question 45). However, as shown in Figure 6.30, four of the 'No' respondents from the question about The FriendRadar have changed to 'Yes' in this question and only two are still 'No'. It is impossible to know how many of the 'Don't know' respondents that had answered 'Yes' to the first question if they were forced to, nut it is probable that they actually did not care since none of them wrote any comment with the answer. It is however probable that more users would have answered 'Yes' to this question than to the first one even if they had not been forced to make up an opinion, since many in fact changed their opinion from 'No' to 'Yes'. One of the ones that answered 'No' substantiated the answer: *"I still can't see any places where I can't stand for being"*. Three of the respondents that answered 'Yes' commented their answer. Their answer to question 45 is written in the parenthesis:

"For safety." (No)

"To fool someone." (Yes)

"I think maybe someone would use it for not showing at places they are a little embarrassed over or to show that they for instance not are at home all the time." (Don't know)

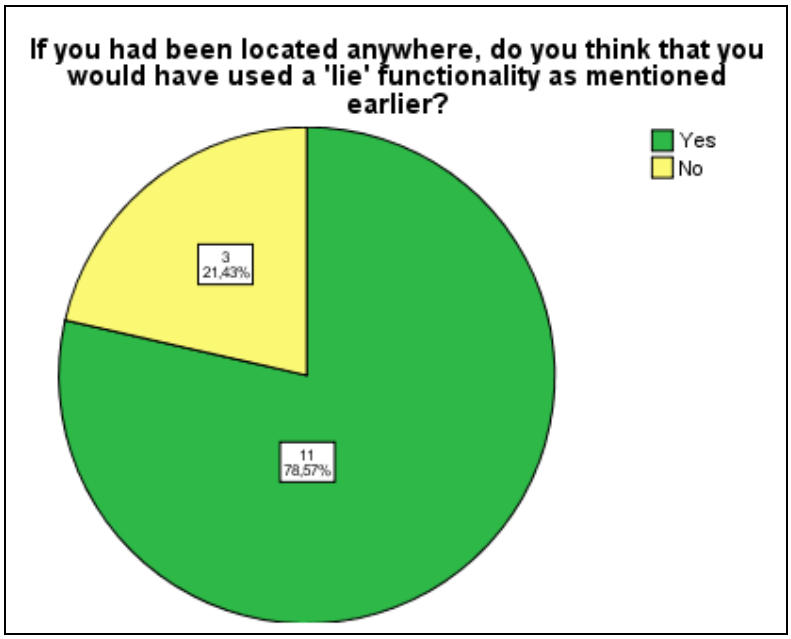

Figure 6.29: Would you lie if you were located everywhere?

When asked if they would use a turn-off functionality in a system where you would be located everywhere, 13 participants said that they would use it and only one participant stated that he would not use it. This one participant is one of the participants that said he would not lie in both of the lie questions. He also used the same comment when he substantiated his answer: *"I still can't see any places where I can't stand for being"*. Six of the no respondents added a comment to their answer:

"To hide."

"In some situations where you want to be left alone."

"So people can't locate me at any given time." (Two almost similar comments)

"I would might use this functionality if I was downtown and saw someone I know was nearby that I don't want to meet, so this person would not try to go and see me."

"It is more secure, it can be 'fake' profiles on The FriendRadar also."

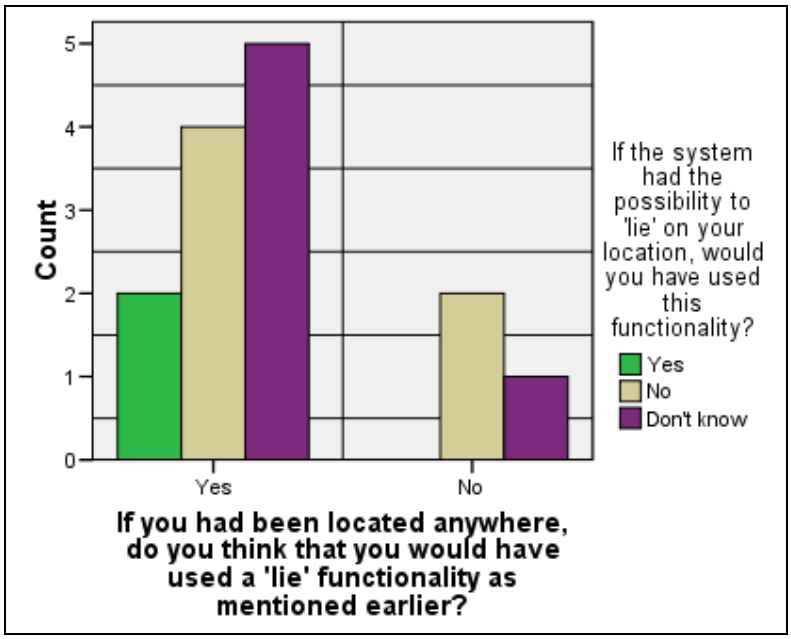

Figure 6.30: Comparison of the 'lie' questions

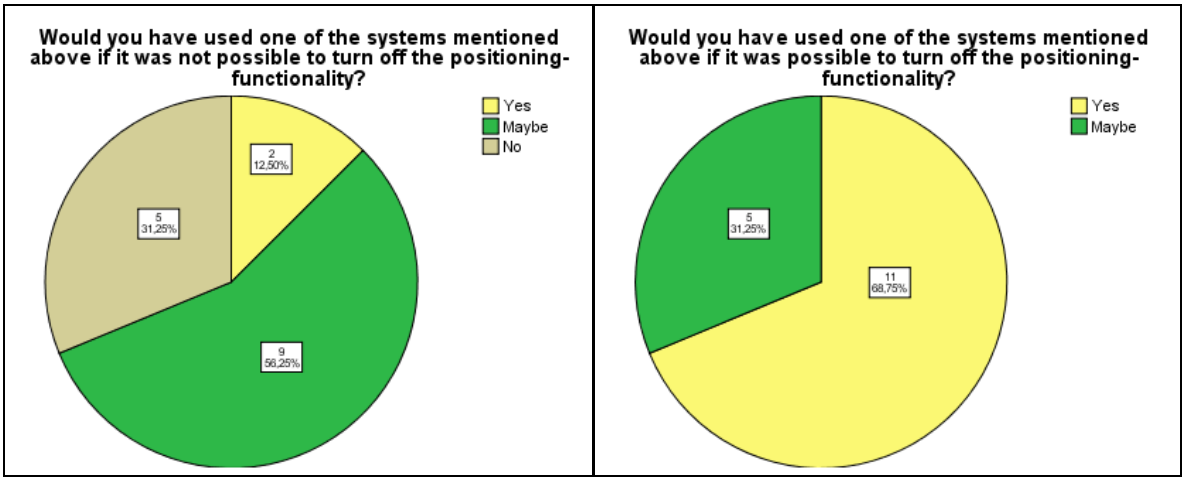

Figure 6.31: Number of participants that want to use the system with and without the possibility to turn off the positioning

The left chart in Figure 6.31 shows the amount of users that want to use either the MSN or Facebook system with continuous positioning functionality if it is not possible to turn the positioning off. Five users said they would not and two said that they would use it. The right graph shows the number of users willing to use such a system if it is possible to turn the positioning off. It shows that eleven users stated that they would use it and five where unsure. No users said that they definitely were not going to use it. Figure 6.32 shows that seven users went from 'Maybe' to 'Yes' and two users went from 'No' to 'Yes' when the possibility to turn the positioning off was introduced. Three users went from 'No' to 'Maybe'. The left chart in Figure 6.33 shows that a higher amount of the participants that would prefer the system most similar to MSN was sceptical to use the system without the possibility to turn the positioning off. The right chart in the same figure shows that when this possibility was introduced, the positive and unsure users were almost evenly distributed between the two systems.

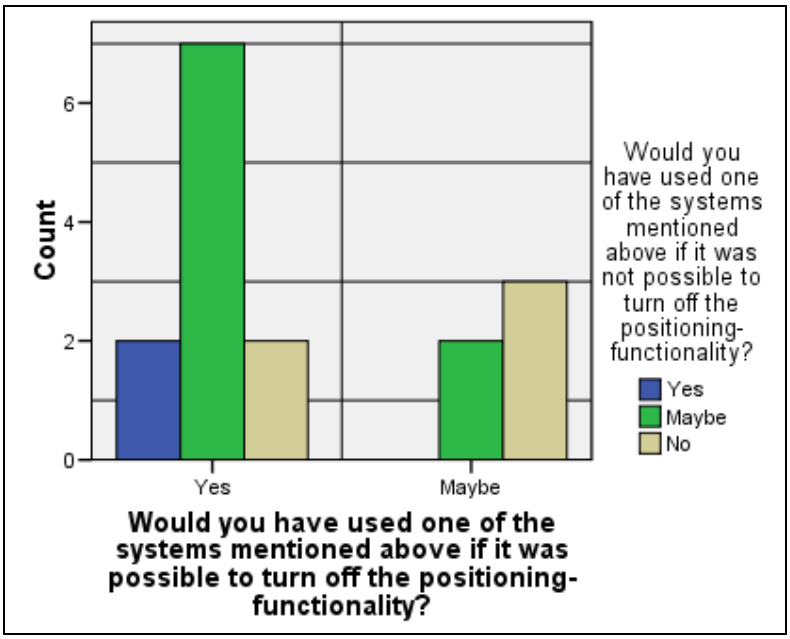

Figure 6.32: Combined results of thought usage with and without possibility to turning off positioning

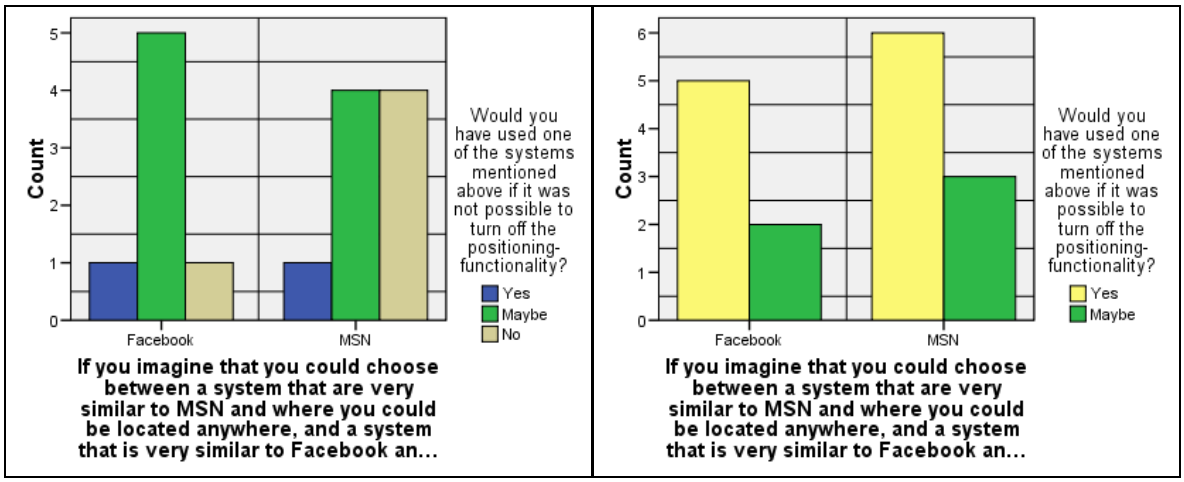

Figure 6.33: With or without positioning distributed on MSN/Facebook preference

6.3 The interview

The one interviewee that was interviewed is a male and is 17 years old. He was a part of the experiment and received an iPod. He carried the iPod with him almost always and he used it mostly for music and videos, but also The FriendRadar sometimes. He had another iPod from earlier, but used this one because it was newer. When asked what he thought about the iPod he answered:

> *"I thought it was stylish. I haven't seen any others that have touch screen like that. It was fun to use it since it was something new. I was a little disappointed with the capacity of the hard drive, but there exists versions with larger capacity."*

He further was asked if he thought it was simple to connect to wireless network with the iPod:

"At home there were no problems, but here at school and in the city it was a little problematic because of some networks that are password protected. In Wireless Trondheim, I thought we would have access, but it did not work right away. I don't know why, but we had to go and re-establish the user profile and write a new password and stuff and then it worked after a while. At home I have the password so it worked right away. In Wireless Trondheim was a little problematic that you could not move around. I connected to Wireless Trondheim about five times I think."

He felt that the web-browser (Safari) of the iPod was quite easy to use. When asked if he thought the iPod was a suitable device to use for testing the system he answered:

"Absolutely suitable! A mobile phone would have smaller screen. I would have been sceptical to a mobile phone because of the screen. It would have been difficult to get the overview."

He has had a profile on Facebook for about half a year. He uses it about once a day and has between 150 and 200 friends. He was asked what made him decide to register to Facebook:

"A big reason was because I knew my friends had it. I was a little against it at first, the arguments was that one could keep in touch with old friends and stuff. The first thing I though was that I have contact with the friends I want to be in touch with anyway. But then I finally created a user because my brother moved to Holland. So I thought I could keep in touch with him, and it led to that I accepted friend request from others. Then it just escalated from there."

What he uses Facebook for and what he thinks is good and bad with Facebook:

"Mostly to check if someone has added pictures from things I have been participated in. Check if people I don't have daily contact with have written something in my inbox or on my wall and upload pictures and stuff myself. A little chat since that has arrived now. I think it is a lot with that privacy stuff about who has the rights to the pictures and stuff. When I read that you don't have control over your own pictures I totally freaked. It seems like, what should I call it, humbug, with things that not are as safe after all when you publish it. One has to be careful not to publish things you don't want others to control. Beside that I feel that it is a simple way to keep in touch with people around you with all you can share and stuff. Haven't had any problems with the system."

He has had MSN Messenger much longer than he has been registered on Facebook. He is logged as long as the computer is turned on, except when he really needs to concentrate on other things. Even if he is logged on constantly, it will not say that he is always active on MSN. He can be away from the computer for hours and still be logged on. He has more friends on Facebook than on MSN, because it is not so much direct communication on Facebook. The contacts on MSN are closer friends, and he thinks he has all his MSN contacts as friends on Facebook. He thinks MSN are the more important of the two systems, because he has been registered on MSN longer than Facebook.

He logged in to The FriendRadar about five times from the iPod and one time from another computer. He had about 15 friends in The FriendRadar and they were his friends because they were a part of the project. Many of the friends were his friends from earlier, but not everyone even though he knew everyone a little from before. He said that he would not have all the friends from The FriendRadar if it had been a system out on the market. When he was asked about what he thought about The FriendRadar he answered:

"First time I heard about it, I had never heard about something like this, it was original! I have not quite thought about how much use I could get from the system or not, for me it take some time to get in and get it as a part of the agenda in a way. But I thought it was fun. I thought it was much more fun at first than

what I found out when I used it. Interviewer: But if it had been easier to connect to Wireless Trondheim? -A*bsolutely, I think that would have improved it a lot!"*

He thinks that his classmates had about the same impression as him about the system, and had never heard about anyone that thought it was just stupid.

He managed to locate himself on the map every time he logged in with Wireless Trondheim. He found some of his friends when they went in actively to try and find each other to check how the system worked, but he never logged in just to check if some of his friends were nearby. He did not act in a different way because of The FriendRadar, but imagines he could do if it was more a daily routine to use the system. He never felt that The FriendRadar disturbed his private life, but he could imagine it would if it was a big thing. As he says, he knows about people that turn off their mobile phones because they do not want to be disturbed. He both received and sent messages in the system, and thought it worked fine.

When asked if he missed anything in The FriendRadar he said that it would be cool with profile pictures on the map, instead of the ordinary marker. He did not think that it would be important to share photos and videos, but it could be cool to link them to the map. He thinks that a functionality that showed the last known location of his friends together with a timestamp could be useful, so you could call them if they had been nearby recently. When confronted with the implemented privacy mechanisms he answered:

a. Choose if you want to show on the map or not with each friend: "*This thing is for finding your friends, so I think it would be strange to remove them. Would rather not accept them as a friend."*

b. That it is only possible to see other location when they can see yours: "*It makes it fairer like you can not snoop on people."*

With possible privacy mechanisms:

c. Grouping of friends with different setting: "*It could make it easier to get an overview, but not for privacy."*

d. Get a notice when localised by others: "*Yes, that would have been nice!"*

e. Lie about you location: "*Only for fun, but I would rather log off if I did not want people to see me."*

He said he would use The FriendRadar as it is if it was put on the market, but it had to be better connection with Wireless Trondheim and one had to be able to move and not loose the connection. He would be a little more sceptical if he could be localised anywhere and anytime. He would have limited his friends (contacts) to only his nearest friends (classmates and family). Only people it would be normal to hang out with on his spare time.

For a future system with positioning functionality he would choose a system that was more like Facebook than MSN, because he is used to that Facebook has all kind of different functionality already. He points out that he wants it to be possible to turn off the positioning functionality even though he is logged in on Facebook. He would definitely have a map instead of showing just the distance of his friends or a written location and he would finitely have fewer friends in such a system.

Then he was confronted with privacy mechanisms in a system that localised his mobile phone or mp3-player anywhere and anytime, and asked if he wanted them in such a system. He said that the possibility to turn the positioning functionality off was essential. He would not have used such a system if it was not possible to turn off. He also thought that it was great that you only could see your friends' location when you could be located yourself. He thinks grouping of friends (with

different privacy settings) would be ok, but not very important. To get notice if others localises would be a great functionality but not essential, and he also imagines in a system where you always will be located, it could be situations where he could use the lie functionality. If all his wishes of privacy mechanisms were granted, he would definitely use the system. He also states that he probably would be willing to pay for it, but it depends both on the price and how great the system actually is. Finally he was asked if he had other comments:

> *"I think it was very fun to be a part of this experiment, I'm very happy for it. It is because I am interested in such things myself. I thought the system was a great idea, I have never heard about anything like it. I know GPS, but not combined with Facebook and stuff."*

7 Discussion

This chapter will first present the discussion of how the research was performed through the project. Further, it will treat the research questions of this master's thesis. Finally, threats to validity will be discussed.

7.1 The research

This section will discuss all the areas about the way the experiment in this master thesis has been planned and performed.

One of the requirements of this master's thesis was that a system with positioning functionality that uses mobile devices connected to Wireless Trondheim should be developed. Therefore, there was not any discussion about which positioning technology that would be chosen, as Wireless Trondheim already had GeoPos implemented. GeoPos worked well however, so there would be no reason not to use GeoPos. It was easy to implement, and the positioning accuracy was better than for instance GSM triangulation. This was not the case when it comes to Wireless Trondheim. Wireless Trondheim seems to work excellent if you are sitting on a bench with a laptop, or any other mobile device with Wi-Fi connection, and want to check your e-mail or read a newspaper online. But as soon as you start moving problems appear. The experiences from the pre-testing of the system, with the six students and employees from NTNU were mixed. On one hand it was a satisfying feeling to see that the system worked, and that the users actually were able to locate each other. On the other hand it became apparent that Wireless Trondheim easily could cause problems for the test persons. The persons that participated in the pre-testing showed both great enthusiasm about the system and the fact that they actually could see the location of the other users, but at the same time great frustration about Wireless Trondheim. The problem was mainly that when moving, the network connection was lost. This is apparently not satisfying to a system which is focused on locating users moving around with small mobile devices. Many of the actual test users also expressed dissatisfaction with Wireless Trondheim in the questionnaire. Figure 6.12 shows that every user except one tried to connect to Wireless Trondheim more times that they actually managed to do it. This shows that the network was not only insufficient when moving, but it was also difficult to connect to Wireless Trondheim in the first place. The six persons that participated in the pre-testing all either are studying towards a master degree in computer science or has studied computer science, so one can say that they are above average skilled with computers, but even they had troubles connecting to Wireless Trondheim. Table 6.1 shows there four users that never managed to connect to Wireless Trondheim and Figure 6.11 shows that everyone tried at least 2-3 times. Many of the textual answers presented form the questionnaire also shows that there is a frustration about Wireless Trondheim among many of the respondents. Also the interviewee talked about troubles with Wireless Trondheim, and since he said he was quite interested it these kind of things, there must be assumed that he also has an above average knowledge about computers. The users complain about the coverage, about the speed, the fact that you could not move around and that it did not work at the school. Trondheim Katedralskole is at the edge of the coverage area, and it was known that it would cause some troubles connecting to the network at the school, which can cause some parts of the frustrations. Wireless Trondheim does not work at most indoor locations either. However, it is pretty obvious that Wireless Trondheim is not yet suited for this kind of usage.

When it comes to the choice of the mobile devices, the iPods seems as a great choice. Table 6.6 shows that most of the participants stated that they used it fairly much or a lot, and listen to music was the far most used activity. This is also an important feature, as the Wi-Fi connection at the iPod shuts down after a while of inactiveness. But if it is used, for instance plays music, it will not shut down. Figure 6.9 shows that in general, the users thought it was pretty easy doing tasks as connect to wireless network, surf the web and upload music. That indicates that the iPod was user friendly

enough for the test users. Finally the interviewee stated that he though the device was fun to use since it was new and that it looked great. He also was very satisfied with the large screen, and felt this was a more suitable device than for instance a mobile phone.

Finally, the test persons were chosen, as mentioned earlier, because their school is located inside the coverage area and because they already have access to Wireless Trondheim. In retrospective, the test persons seemed to be the right choice. It would of course had been better if the school area had better coverage, but the school's location led to that the pupils had to be downtown each day anyway. The pupils was also in an age group that would be one of the probable users of such a system, and many users also showed happiness of being able to borrow the iPod for a month. They also had a very helpful teacher that made the process easier, so it would probably be difficult to get better test persons.

7.2 RQ-1

RQ-1: *Are people willing to use a system with functionality for locating and interacting with their friends and family using a mobile device connected to a wireless network?*

This research question asks basically if people are interested in locating their friends and family and communicate with them trough the same device. A requirement that must have been fulfilled before you can be able to locate your friends and family, is that your friends and family must have shared their location with you. Therefore this research question also asks if people are willing to share their own location information in exchange for the ability to locate their friends and family.

Judging from the usage of The FriendRadar, one could say that it seems like users are not interested in systems where they can locate their friends. The users did only log in an average 3.06 times during the 29 days long test period. If this number is compared with the test persons self declared use of Facebook, it is a very small number. 14 of 16 of the respondents of the questionnaire said they logged in on Facebook daily or more (Figure 6.8). This would probably lead to an average of about 30 logins per user on Facebook during the same period. The user that had registered definitely most logins to The FriendRadar during the period had only 10 logins. This is clearly an indication to that the users were not very interested in using the system, at least not compared to Facebook. It is however probable to assume that this low log in rate can, at least partly, be explained by the difficulties the users had with Wireless Trondheim. Even though most of the test users said that they used their iPod fairly much or a lot, they have only connected to Wireless Trondheim an average of about 2.82 times during the test period, which seems fairly correct according to the number of times the users claimed that they connected to Wireless Trondheim (Figure 6.11). This indicates that even though the users has an available network that they could use free of charge in the downtown, they have not used it. This is confirmed by the negative comments about Wireless Trondheim both by the interviewee and the respondents of the questionnaire. Two questions from the questionnaire that was meant to give an answer on how the users would react if some mechanism was removed that in theory would give them less privacy when using the system, can actually be helped to illustrate how hampering Wireless Trondheim was for the usage of The FriendRadar. The first question was if the users would use the system more or less if they could locate their friends that were connected to Wireless Trondheim, even if they themselves were not connected to Wireless Trondheim. Five users answered that they would use it more and the remaining nine answered that they would use it equally much as they did now. In practice this could have made the user experience even worse, because this could lead to that nobody would ever connect to Wireless Trondheim, which again could lead to that nobody shares their location and therefore nobody could ever be located. Anyhow, it shows that Wireless Trondheim was inadequate. Another question was if the users would use the system more or less if they could be located everywhere independent of which network they were connected to. Six would use it more,

seven the same and one user would use it less, as shown in Figure 6.24. In reality this could pose a big threat to ones personal life, but most of the users only saw the positive opportunities in this proposal. The users that added a textual comment to their answer said that this would give the system a new dimension and this would lead to that the system actually could be used (as opposed to The FriendRadar). One user also mentioned that it would be easier to use, because she was rarely inside the coverage area of Wireless Trondheim. This question also received negative comments however, as one user that said it would be scary and another that said she would allow fewer friends. The one user that said she would use it less said that one needs a private life. The users' privacy feeling and privacy mechanisms will be discussed more under the discussion if RQ-3 and RQ-4.

Another important factor that can explain the low login rate of The FriendRadar is that it is in the nature of social network services that they need a large user mass to survive. Nobody would have used Facebook if there were no other registered users there. It becomes a vicious circle; the difficulties with Wireless Trondheim lead to that few or no users are connected at the same time, which again leads to that the users that actually manage to log in, loose the interest in the system because there are no other users connected at the same time as them. In a synchronous system like The FriendRadar, the users have to be connected to Wireless Trondheim at the same time to be able locate each other. Table 6.3 shows that there actually was only three times it happened that two or more users was connected to Wireless Trondheim at the same time, and in only two of these cases was the users involved actually friends with each other. It is in fact only a total of five users that during the test period had a chance to see some of their friends on the map. These problems combined with the initial low user mass of only 23 possible users, seemed to be enough for the users to loose interest in the system. The interviewee confirms this assumption as he says that he thought the system would be more exciting to use than it actually was, but said that he probably would have another impression if Wireless Trondheim worked better. This is explicitly pointed out by especially one of the respondents of the questionnaire. This respondent said as an explanation to why she never had logged in to The FriendRadar with an intention to check her friends' location that she probably would have been more interested to log in to The FriendRadar if she had more friends and if there was always someone logged in like on MSN. She lost the interest since there was nobody logged in each time she checked. The same thing was explained by another user that wrote that she could not say how it was to use the system in practice, since too few users had the possibility to log in to the system. Figure 6.15 shows that the users that actually has logged in to check their friends location, are among the users with the most friends, which is another indication that the system could be used more if there was a bigger user mass in the system. The interviewee also said that even though many of the friends he had in The FriendRadar was his friends in real life, he would never have had all the friends he had in The FriendRadar as friends if the system was put on the market. He said further that he would have had few friends in a real system, and that all his friends would be friends that it would be normal to hang out with on his spare time. This was also mentioned by one of the respondents on the questionnaire. This could indicate that the users of The FriendRadar not necessarily had too few friends, but the friends they had was not the right ones. This could also hamper the user experience of the system.

Even though The FriendRadar was not used that much, some differences between the genders was found; the females logged in to The FriendRadar a lot more times than the male users, almost twice as many times in average. At the same time, the male users connected to Wireless Trondheim more times than the females. This could be an indication on that female users was more interested in the social aspect of The FriendRadar, while the boys was more interested in the technical aspect of the system. This indication is strengthened by the fact that all four respondents that hold Facebook as an important part of their lives is females and that boys said that they managed to perform various tasks on the iPod better that the girls (Figure 6.10).

If one judge from the results presented in Figure 6.17 it would be easy to answer 'Yes' to this research question, as opposed to what the usage of The FriendRadar might indicate. Only three of

the 16 participants said that they would not use a similar system as The FriendRadar if it was put on the market with all the shortcomings of the system and the positioning fixed. Interestingly, two of the three negative respondents were among the total four respondents that stated that Facebook was an important part of their life. An answer to why this is the case would only be speculation, but it could be that they would be afraid that such a system will ruin their already well-established relationship with Facebook. One question of the questionnaire asked what the participants thought about the concept of locating their friends, and most users showed great enthusiasm about the concept. One user thought it was exciting, original and fun and another thought the concept was very good. One user liked the concept, but wondered why one had to be connected to Wireless Trondheim to use it as he thought the network was not good enough. All these answers indicate a genuine interest from the users in using the system.

The participants of the questionnaire were asked to imagine a future system where they could be located anywhere, and asked to choose between a system that is very similar to Facebook and a system that is very similar to MSN. The name MSN is used to describe the application of MSN Messenger. These two systems were chosen as examples because they are well known to the users but at the same time quite different. While MSN Messenger is quite simply a chatting application, at least form the users' perspective, Facebook are more a message and photo sharing service. The two services also have a very important difference in that MSN Messenger uses synchronous communication and Facebook uses asynchronous communication. Figure 6.19 show that the participants were split in their choice on which service to choose. Nine users wanted a system like MSN and seven would prefer a system that was more similar to Facebook. The interesting part however is that only one of the participants that answered Facebook chose to substantiate this answer with a textual comment, while eight of the participants that answered MSN did the same. The single users that commented and chose Facebook said he only did it because he used Facebook the most. The participants that preferred MSN however, were clearer in their choices. Three users thought it was better with direct contact, one thought it was more social, one thought it would be more private, another user felt it demanded less effort to log in on MSN and finally one user said she felt safer with MSN because she had used it longer. The most interesting answer however was from a user that wanted a mixture of the two systems, where you both could send synchronous and asynchronous messages. These answers indicate that a system that would have more aspects similar to a instant messaging service than The FriendRadar would be chosen for a future system. The positioning is synchronous, and this would probably be a better fit with synchronous communication. Since almost all the participants that answered MSN did substantiate their answers, it is also natural to assume that these participants actually has thought their answer more through and have a stronger preference towards the system than the Facebook respondents. Another factor that strengthens a system that has more similarities with a messenger system is their form of direct communication without any central server. If this becomes the case with the location information as well, the user would be able to trust that no unwanted parties get hold of their location information. This will help the system to get users centricity, as mentioned by (Bellavista, Küpper et al. 2008) as the main factor for success for the 'new' LBSs. The interviewee however said that he thought it would fit better in Facebook, because it has a lot of functionality already, and he would prefer MSN to be as simple as it is now. As the results from the questionnaire shows there are no difference between the genders on this question, but the users that use Facebook several times a day would prefer the Facebook system. This is naturally, as they are more used to using Facebook. As the results show it is a split view among the participants and it will probably be split between the rest of the population as well. Anyway, the results from the questionnaire show that it is more preference towards a simple instant messaging system with location functionality among the users that answered the questionnaire.

The two final questions of the questionnaire asked if the users wanted to use a system where you would be located everywhere, and in one case could not turn off the positioning functionality and in the other case could turn off the positioning functionality (Figure 6.31). It shows a significant

difference between the two cases. Only two participants said they definitely would use a system where the positioning functionality could not be turned off, while eleven users said they would use it if it could be turned off. Five said 'No' to a system without possibility to turn off and no participants said 'No' to the system that could turn off the positioning functionality. This shows the importance of privacy mechanisms for systems to be accepted by users, and especially the possibility to turn the system off. The prestudy (FindMyFriends) concluded with that many users saw is at an absolute requirement that it was possible to turn the system off if they would use it in a city wide environment, and it seems like this (naturally) holds even stronger for a worldwide system. The fact that 11 of 16 users says an unconditional 'Yes' to use a future system if it possible to turn off, shows that as long as a few, but important privacy mechanisms are fulfilled, users are absolutely interested in the concept of being able to locate their friends. The interviewee even said that he could possible have paid for using such system, which was not the impression the users from FindMyFriends gave. It is however a strong indication that location tracking systems could have a great future.

So far the discussion has in particular been based on if users want to find their friends and family with the help of a computer service. It is not difficult to understand that they do. As mentioned earlier, this naturally leads to that someone need to share their location. Since users of The FriendRadar could only locate their friends when they themselves were connected to Wireless Trondheim it is probable that the users understand this connection. The answers of the questions also indicates that the users naturally assumes that they have to share their own location to be able to see others location. The survey from Manhattan described in Section 3.2.2 shows further that people are willing to share their position to get access to the positive things P3 systems offers. The usage of The FriendRadar in Wireless Trondheim shows that these kinds of systems are dependent on that there are some users that share their position in the system, or else the users loose the interest pretty quickly. With users sharing position, the need of privacy mechanisms naturally emerges. To be able to turn off the system has already been mentioned as an important mechanism. The earlier research presented in Section 3.4 also confirm that without privacy mechanisms that offers users feedback and control over which users that can see what, the users will not use applications that share the user's location with others. This subject will be further discussed under RQ-4. It seems that whether a user wants to use an application that shares the user's location or not, is determined with a tradeoff between the usefulness of the service and the user's privacy concerns. This is shown by the success of Connecto (Barkhuus, Brown et al. 2008). The developers of Connecto think that the usefulness and the practical use and the awareness of the system outweighed the users concerns for privacy in the system. Connecto's success also shows that there is not only privacy mechanisms that determines the usage of a location-tracking system, but that the user friendliness is of utterly importance. This is obvious in the usage of The FriendRadar as well, as it was shown that Wireless Trondheim was not user friendly and that this scared the users away from the system.

7.3 RQ-2

RQ-2: *Will users of a system with functionality for locating other users behave in a different way than they normally would?*

- RQ-2.1: *Will a user who knows the location of other users behave in a different way than she normally would?*
- RQ-2.2: *Will a user who knows that other users can know her location behave in a different way than she normally would?*

RQ-2 is split into two smaller research questions, to make it easier to distinguish between the behaviour that is caused by the user's knowledge of their friend's location and the behaviour

caused by the user's knowledge of the possibility that others can know their location. This section will first treat RQ-2.1 followed by the discussion of RQ-2.2.

7.3.1 RQ-2.1

This research question asks if the users of a system that makes the users aware of the location of others, will behave in a different way than they would have behaved if they had not used the system. Basically, they will behave in a different way only by logging in to the system, because they would not have done this if they were not using the system. This however counts for all activities, and will not be discussed here. It is the behaviour that is affected by the fact that the users have located some of their friends by using the system that are interesting. Colbert's study about rendezvous presented in Section 3.3 shows that rendezvous not frequently occurs exactly like planned, and that 70 percent of the rendezvous needed at least one extra communication between the rendezvousers, normally made by mobile phone (Colbert 2001). The introduction of mobile phones in our daily life made us act in a different way, especially when we were going to meet each other. Colbert states that the negative outcomes of a rendezvous (stress and lost opportunities), has become smaller after the introduction of the mobile phone, as it for example is easier to give notice if one know one is going to be a little late. Colberts theory is that these rendezvous will occur with even less negative outcomes if a location-tracking system could be used. The example he gives where a mother could see that the father had already picked the kids up at school, and therefore not have to drive to the school and check, shows indeed an action that is affected by the mother's knowledge of her kids' location. This knowledge however, she could equally well have received by calling the father's mobile phone. The outcome would have been the same; the mother would not have to drive to the school and check if the kids were picked up. The difference in the two situations is that in the first case the mother got this knowledge automatically without disturbing the father when he was driving, while in the second case she had to call him. The location-tracking system made it easier for the mother to get hold of this information, but she did not in fact act in a different way, except of course of the way she retrieved the information. The Connecto study however (Barkhuus, Brown et al. 2008), shows behaviour that is affected by the Connecto system's positioning functionality. A good example is the user that was at the shooting club and hoped that some of his friends would join him, when two friends actually showed up at the shooting club because they have seen that he was there with the help of Connecto. The two friends that showed up at the shooting club would never have known their friend's location if not Connecto have showed it. The fact that users reported occasions where they did not call their friends because they saw that they were in some particular situations, are also behaviour (actually non-behaviour) affected by the system. In the example mentioned with the commuters, the users actually have made Connecto a part of their daily routine. The arrangement between the commuters made the waiting commuter's morning more flexible as he would be aware of when his friend would arrive, and he could maybe get time to thing he normally not would have done. These examples show that studies have shown that a user's knowledge of another user's location can affect her behaviour.

The results presented from the FindMyFriends study, are also clear on this question; the users behaved in a different way as a consequence of their knowledge of other user's position. Over 50 percent of the users tried to find their friends at least once after locating them on a terminal at Samfundet. Some of their friends could of course be found with the help of a mobile phone, but the difference when using FindMyFriends is that you get an overview of all your friends at a single instance. This means that the user can choose which friends to visit after they are localised, and not in advance as she would have to do if she had to call them. The results show also that over 10 percent of the users went to Samfundet as a consequence of seeing some of their friends on the map of FindMyFriends from a computer located outside Samfundet. Seven participants stated that they postponed a trip to Samfundet and seven people stated that they cancelled a trip to Samfundet at least once after seeing that none or few of their friends was at Samfundet. These actions, especially

cancelling a trip, differ quite radically from the planned actions of the users. There is no way they would have gotten the same knowledge about the people currently on Samfundet, without calling a large amount of people, so there is no doubt that these actions are consequences of FindMyFriends positioning functionality.

Because of its low usage, it is more difficult to spot behaviour that is affected by the system in the usage of The FriendRadar. As shown in the analysis of the registered data, it only happened two times that two or more users that were friends with each other were connected to Wireless Trondheim at the same time, and therefore able to locate each other on the map. On the other hand, both of these occasions seemed to have a connection as the users was either located at the same spot, or very close to each other. Figure 6.5 shows the users movements in the second of these two occasions. The movements seem to have a connection, but it is impossible to say something for sure. All the users went in the same class, and it is possible they would have been at exactly the same places without using the system. Very little information to add depth to this research question appeared in the questionnaire. It showed that five users found their friends on the map and that one of these users tried, and managed, to find one of the friends that were located. This is of course behaviour that was a consequence of the positioning functionality. The users that did not try to find their friends said it was because they either not had the opportunity, the need or the energy to go and find the friend at the time. The interviewee did not report any behaviour affected by The FriendRadar, but said that if it became a daily routine he could imagine he would behave different because of it.

Earlier studies and FindMyFriends show that users indeed act in different ways because of their knowledge of other position. The actions they made that was different, both the users of Connecto and the users of FindMyFriends, was mostly spontaneous actions. Both deciding to go to the shooting club or Samfundet because the system showed that a friend or some friends was there and postponing or cancelling trips to Samfundet are spontaneous actions that probably not would have been done if it had not been for the positioning functionality these systems offer.

7.3.2 RQ-2.2

This research question search to discover if users behave in a different way, when they know it is possible that other users of the system can know their current location. There are two aspects to look on in this question. The first one is the things a user will avoid to do, because she wants to hide her actions to the users that possibly could see her location. The second part is the action a user will do, because she assumes that the users she wants to see her location, will see it and know where she is. The first part is a disadvantage for the user, and in the second part the user uses the system for her own advantage. An example of the latter one is when Colbert suggests how a user might act during a rendezvous if she and her boyfriend both have a location-tracking system (Colbert 2001). He suggests that if she is early for a rendezvous with her boyfriend, she will probably be more willing to pop into a shop while waiting, assuming that her boyfriend will know her location when he arrives. He points out that in this case the rendezvousers are taking higher risks, which can lead to new problems. An actual example of this kind of action is the user that actively uses Connecto to show his friends that he is at the shooting club. Examples of actions that is avoided to do are not reported in any literature. However, (Consolvo, Smith et al. 2005) reports on situations where the users did not want to disclose their location to their friends. It was for example while doing innocent actions and they simply did not want to be disturbed, like by their boss after work hours and by anyone when being out on dates with their significant others. It was also more cynical hiding of their actions, for example being out on errands and did not want to pick thing up for others or hiding for their significant other that they were not doing what they was supposed to be doing. Finally, it was more 'guilty' actions like hiding actions that they where not supposed to do for their significant others (like another love affair). One can also imagine hiding more innocents actions for their significant others, for example a husband hiding for his wife where he buys her

Christmas present. However, this is only situations where the users want to *hide* their locations, but it is not reported that they avoided doing it because they thought someone was watching their location.

The results found in the study of FindMyFriends show a similar pattern. There were only a few inconsiderable actions that came as a result of that people knew they could be located. On the other hand, many users reported that they had been hiding the signals from the tag, and as a result had become impossible to track for their friends. It was therefore assumed that the system did not hinder people in doing things they did not want other people to know, they just hindered the system to show they were doing it. Another interesting point from the study of FindMyFriends was that the users seemed to want to be located. The system did not require anyone to wear the tag that located them, but nevertheless, most of the users wore their tag 'always' or 'most of the time' when visiting Samfundet. This is an example that shows the users used the system to show their friend where they were located.

From the users registered behaviour in The FriendRadar it is impossible to say that anyone did behave in a different way than they normally would because they knew they could be located. No respondents of they questionnaire said they have done something they normally would not do. None of them had tried to hide their action either. This is of course a natural consequence of that the users very rarely could be located by other users, simply because they rarely were connected to Wireless Trondheim. It was a much bigger effort to actually connect to Wireless Trondheim than not doing it, and therefore the users only connected to it when they needed to. In the questions that deal with security mechanisms however, the respondents mention that there are situations where they possibly would want to hide their locations, both for security and convenient purposes. Examples are embarrassment for showing their location to others, that they do not want to meet a specific person at a specific time and that they can not be sure that there are not fake profiles in the system.

The little indications that exists to answer this research question, indicates that users do act in different ways to take advantage of the fact that they know other users can see their location by showing their friends what they are doing, but they do not avoid to do actions they do not want others to do because of the system. If they would start to have to avoid doing things it is probable that the users would not be using the system. A system's privacy mechanisms are there to help the users doing all the things they normally would do, without being afraid that others can see things that they should not be seeing. Privacy mechanisms will be discussed more under RQ-4.

7.4 RQ-3

RQ-3: *Do the users of social interaction systems that share context sensitive information like location feel they are loosing their own personal privacy?*

Since this research question treats the feeling of the users of a system, The FriendRadar's logged data will not give any information about this research question, except one: All the users allowed all their friends to see them on the map. This could be an indication on that none of the users worried too much about their privacy. On the other hand, there were many friend requests that were not accepted. A reason for this may be that the system was not used so much, but it can also be a deliberate action by some users to rather not accept a friend request altogether, than accepting a friend and just allowing the friend to see her proximate location. This assumption is supported by (Consolvo, Smith et al. 2005), as their survey shows that the users either disclosed the location information in the detail that was most useful for the requestor, or did not disclose the location at all. In the case of The FriendRadar the 'nearby' setting could never be the most useful for the requestor, since a friend that has a 'map' setting can see both if the friend is nearby and her exact location on the map. It is no way to know if these unaccepted friend requests are just unseen friend requests, or if the friend requests are deliberately not accepted by the users. The two users that

commented this answer in the questionnaire both said that they did not have a problem with that other users could see their location, which is an indication towards the conclusion that the friend request was not accepted because they was not seen. The interviewee however said since this system was made for locate each other it would be strange not to show his friends on the map, and he would rather not accept them as friend if he did not want them to locate him. Unfortunately, there was no question in the questionnaire that specifically asked if the users deliberately chose to not accept friend request because they did not want that user to see their location in the city. There was however a question that asked if the users would allow the same friends to see them on the map if the system could locate them anywhere, and not only downtown Trondheim. In this case half of the 14 users would allow the same friends to see them on the map and the other half would allow fewer friends to see them on the map. It is however unclear if they only would choose the 'nearby' setting on the friendship or if they would not accept them as friends at all. Figure 6.28 show that only one male respondent would accept fewer friends to see them on the map, while as much as six female respondents would do the same. This is a strong indication that male users, or at least the males among the test users, are less worried about privacy threats than the female users. The same figure shows that most of the respondents that would prefer a Facebook similar system with positioning would have allowed the same friends, while most of respondents that would prefer a system more similar to MSN Messenger would allow fewer friends to see their location on the map. This could be explained by the fact that the interviewee said that he had fewer, but closer friends on MSN than in Facebook, which very well can be a general trend. The differences between the two systems are however so clear that it should not go unnoticed.

The questionnaire and the interview had several questions that were meant to give indications to the answer of this research question. None of the respondents of the questionnaire said that they ever felt that The FriendRadar's positioning system disturbed their personal life during the test period. As mentioned before, the system was used too little to be able to get a good answer to this question, since it natural that nobody felt that their privacy was threatened when they knew nobody used the system. Another factor is that users generally were rarely connected to Wireless Trondheim, which was the only way they could share their location with others. One user did however say that he was worried that some of the system administrators would use the location information or other information about him to something he did not know about. This privacy threat does not come from the other users, but has more in resemblance with the threat that is associated with Big Brother from Orwell's novel. In the introduction lecture at the start of the project it was stressed that the user information was split from the device, and that the persons that studied the data would not couple location information and message content to personal information. On the other hand, it is easy to understand that this concern arises. The authors of the 'science fiction' article presented in Section 3.4, actually mentions user centricity as the main reason of the 'new' systems popularity (Bellavista, Küpper et al. 2008). They further explain (imagine) that it was not until the users started managing their location data themselves, and sharing it directly between the users without a central server that the users started to trust the systems. Since this was the only report of a user that was unsure about the sharing of personal information, it can indicate that it is a problem that the users do think about. However, only one of 14 users saw this as a problem, even though the users knew that their location data was going to be analysed and used in this master thesis.

Further, The FriendRadar had reciprocity in location-sharing implemented, which means that a user had to be connected to Wireless Trondheim to see others location. Five users claimed that they would use The FriendRadar more if this security mechanism was not implemented, and nobody said that they would use the system less. This can again be explained by the problems Wireless Trondheim caused the users, but it indicates that the users do not care as much about privacy as they do about user friendliness. Figure 6.22 shows that it is in general the male users that would use The FriendRadar more and the female users would that would use it equally much, and that it is the users that have used the iPod the most that would use the system more if they did not have to be

connected to Wireless Trondheim. The males used their iPod slightly more than the females, but the difference was small. Therefore it seems like it is two different trends; the male users and the heavy iPod users are the users that either are less careful with privacy, or is more demanding when it comes to user friendliness. This shows again that the male users are less concerned about privacy, as the case was with their imagined privacy settings in their friendship if the system would locate them anywhere. When the users was asked if they would use The FriendRadar more or less if they would be located anywhere, as much as six users said they would use it more, and only one said he would use it less. Again the dominant gender among the users that would use it more was male. The one user that would use it less however, was also male. It is still the females that would not be affected by this change in the system. It is showed earlier that the females was the ones that used The FriendRadar the most during the test period, and this could be a possible solution in why they would not use it more, but the trend is still clear; the male users shows less concern about privacy. An interesting point shown in Figure 6.25 is that many users have changed from more to the same and opposite between the two questions. This is probably a good sign, because it can indicate that the users has read and understood the difference in the two questions. One user in fact changed from more to less. The substantiated answers to this question show that the user that would use it less, explained this with that one needs a private life. The users that said that they would use it more showed no signs of concerns toward the fact they could be located everywhere, but only saw the new possibilities with this 'improvement'. The two comments from the users that would use it equally much shows slight signs of concerns as they said it would be scary that it could not be controlled and that probably fewer friends would be accepted if the system could locate them everywhere. The interviewee also pointed out that he would have accepted quite few friends; only the one he could have been with on his spare time, if the system could locate him anywhere.

Another indication towards that the users of The FriendRadar are not too concerned about privacy, is their comments about the Facebook privacy. Six participants said that they felt the privacy was not good enough, but as one commented: *"I think than one is vulnerable, but I don't care, it's not important"*. This can be an indication of even though the users know they are vulnerable, they keep using Facebook because the usefulness is greater than the concerns. This is the same as the case was with Connecto, also mentioned under the discussion of RQ-1. The positive aspects of the system outweighed the user's privacy concerns, and the users did not worry about privacy at all. This is further confirmed by (Barkhuus 2004), which suggests that the 'coolness' and usefulness of a system can undermine the users' focus on privacy concerns. The Flickr and ZoneTag study, shows that users are more worried about damaging others privacy than their own (Ahern, Eckles et al. 2007). Users was also careful when it came to hurting their own identity, like being seen on a gay parade, but in general the users was not concerned with the pictures revealing their location data as they said they would not publish them if they were at places they did not want others to see. One issue that appeared during their study was the problem with users wanting to show some users where they was, but at the same time not show some other people where they are if they for instance not are invited. This problem shows that often is the identity of the enquirer more important that the situation you are in when deciding if you want to share your location information. This is further confirmed by other studies presented in Section 3.4 (Lederer, Mankoff et al. 2003) (Consolvo, Smith et al. 2005).

Results from the preliminary study of FindMyFriends indicated that privacy was not a big issue in FindMyFriends, but that a city wide system would cause bigger privacy concerns among the users. It seemed like the users was aware of the possibility to block their tag's signal and therefore disturbed the system in such a way that they could not be located instead of letting the system disturb their own personal privacy. This can be compared with the problems of Wireless Trondheim. Privacy was not an issue because the users could easily avoid connecting to Wireless Trondheim.

NRK's article that describes that The Women Shelter have been contacted by women that feels their men are using location-tracking systems for surveillance purposes, shows that there surely are

people using such systems that gets a feeling of loosing their privacy. A mentioned by The Data Inspectorate, this is the case for a very low portion of the systems users (NRK 2007) . However, this is a serious problem, as it can be a matter of life and death instead of getting embarrassed if doing something you do not want others to see.

7.5 RQ-4

RQ-4: *How can privacy mechanisms be used to help the users of context sensitive systems for social interaction not to loose their personal privacy?*

As mentioned several times, what determines if a user wants to use a system that shares the user's location with other is a tradeoff between the usefulness of the system and the system's threat to the users' personal privacy. But is it not only as simple as that. Most authors of this subject agree that feedback and control is the two most important things to consider to keep the personal privacy of the users and to make a system with sufficient usability. The user needs feedback about what information other users possibly can see about her, and the user need to be able to control what is being conveyed to which users. Both are achieved by the use of privacy mechanisms. If a location-based system is implemented with the right amount of privacy mechanisms it can be both useful and privacy preserving. This section will discuss which privacy mechanisms that are needed and which that are not, to achieve this.

The FriendRadar had some privacy mechanisms implemented. These were implemented because the preliminary study with FindMyFriends' users concluded that these where of great importance for a system like The FriendRadar to be successful. As showed by the usage of the system, The FriendRadar was not a great success among the users. Both the interviewee and the respondents of the questionnaire showed great enthusiasm about the concept of the system, but did not follow this up by using it. As discussed in Section 7.2 where it was discussed if people are interesting in using such a system, the main reason for the low usage of the system is probably the difficulties with Wireless Trondheim. In fact, these difficulties offered the system a privacy mechanism automatically. It was very easy for the users of the system to give problems with Wireless Trondheim as a reason that they was not available for being positioned by their friends, in other words, it offered the users plausible deniability. They could plausible deny being localised by their friends without any questions. The fact that they had to connect to Wireless Trondheim to be localised, would offer plausible deniability even if users had not had any problems connecting (and keep being connected) with Wireless Trondheim. First, Wireless Trondheim only covers a limited area, and a user could just say she was outside of the coverage area. Second, if a user entered the coverage area, she would still have to manually connect to the network and could say that she just forgot to connect to the network, and easily get away with that explanation.

One of the privacy mechanisms that were implemented in The FriendRadar was reciprocity in location information, which in practice is that a user only is able to locate her friends when the friends can locate her. This was suggested as one of the main factors behind a successful city scale location-tracking system in the preliminary study about FindMyFriends, even though it was not implemented in FindMyFriends. Most of the relevant literature also underlines this as an important privacy tool for location-tracking systems, among other by *the principle of minimum asymmetry* (Jiang, Hong et al. 2002). This, among with plausible deniability, is mentioned as the most important factor when it comes to protection from legitimate users in the 'new' systems of 2012 in the back to the future article (Bellavista, Küpper et al. 2008). This protection from legitimate users is imagined by the authors as an important feature that helped the LBSs to gain popularity. In the questionnaire about The FriendRadar it was asked if users would use the system more or less if reciprocity in location sharing was not implemented. As the results presented in Figure 6.21 shows, five users said they would use it more and the rest said they would use it about the same. In other words, no users would use it less. This indicates that the users instead of seeing this feature of the system as a

privacy protecting mechanism, they see it as a functionality that makes the system less useful. Again, this could be explained with the problems of Wireless Trondheim. FindMyFriends was implemented in such a way that the users could locate their friends without being at Samfundet while doing it, and therefore not possible to locate by other users. It seems that this implementation could be beneficial for a system in a closed environment as both FindMyFriends (Samfundet) and The FriendRadar (Wireless Trondheim) is. As many users said, they were rarely inside the coverage area of Wireless Trondheim and therefore did not have the possibility to use the system. If one could check which friends that is currently downtown while being at home, it could probably be more useful for the users. This was also reported happening several times in FindMyFriends; users checked if some of their friends currently were at Samfundet, and as a consequence both decided to go to Samfundet and change their plans and not go. One can imagine that this usage pattern could happen in The FriendRadar as well if it had been possible. It would be interesting to see however, if the users actually would have the patience to put in the effort it is to connect to Wireless Trondheim if they did not have to for be able to locate others. It is actually a possibility they would, because as seen both in FindMyFriends and other surveys presented earlier it seems that users often want to be localised because they are using the system to tell others of their location. It could be assumed however that there is only systems that only can locate users in a closed environment that would benefit from not have reciprocity in location sharing. There was one of the respondents of the questionnaire however, that said that she thought it was great that one could not see the location of others when your own location is deactivated. She was not among the participants that received the iPod, and did therefore not test the system. The other security mechanism that was specifically implemented to The FriendRadar was the possibility to choose between three granularities of location sharing in a friendship, which is closely related to reciprocity in location sharing. This is because the lowest granularity chosen by a part in the friendship becomes the granularity of the friendship. In this way, ifuser A of the friendship chooses that she can be viewed on the map by user B , but user B only wants that user A can see if she is nearby or not, both users can only see if the other user is nearby or not. In this way they achieve location reciprocity. As mentioned earlier, all users allowed all their friends to be seen on the map. Figure 6.27 however, shows that if The FriendRadar could locate the users anywhere, half of the users said they would allow fewer friends to see them on the map. This could backup the assumption that reciprocity in location information is more important in a system where the users could be located anywhere in the world This also corresponds to the intuitive principle people normally live by; if I can not see you, then you can not see me.

The privacy mechanism that was considered the most important from the preliminary study for a system like The FriendRadar was the possibility to turn the system off, and preferably in a way that offers the users plausible deniability. As mentioned above, this mechanism was automatically achieved both by the limited area Wireless Trondheim covers, the troubles with Wireless Trondheim and the fact that a user has to manually connect to Wireless Trondheim before someone can localise her. A very large portion of the users of FindMyFriends said that this would be a necessity if they were going to use a system that covers an entire city or more. The users of The FriendRadar were not immediately worried about this ability to turn the system off, as Figure 6.24 shown. Six users would have used the system more if one could be localised independent on network, and only one would use it less. None of the textual answers that backups these answers say anything about the possibility to turn the system off, but some user shows privacy concerns. From the answers of this question alone, it seems that the users actually are willing to use a system that locates them everywhere, without thinking of privacy mechanisms. But when asked specifically if they would use a turn-off functionality in a system where they could be located anywhere, thirteen respondents said they would and only one respondent said she would not. To substantiate this, the users wrote that they would use it to hide and that there are situations where one wants to be left alone. A couple of users did also mention in other questions that they though it was great that one could turn off the system as it was implemented today, and they would probably think this

is even more important in a larger scale system. The answers of the two final questions of the questionnaire were also pretty clear. These results are shown in Figure 6.31, which shows that only two users said that they definitely would use a future system that located the users anywhere if it was *not* possible to disable the positioning functionality. Nine users were unsure and five would not use it. When the same question was asked about a system where you *could* disable the positioning functionality, as many as eleven users said that they would use the system, with five users that were unsure. Figure 6.32 shows that two users did change from 'No' to yes and seven changed form 'Maybe' to 'Yes' when it became possible to disable the positioning functionality. These results are pretty clear, and they clearly indicates that a possibility to turn off the positioning if you do not want to be located is a feature the users expects form a location-tracking system, and that a system without it would have more difficulties to become a user success than a system that have this feature.

A privacy mechanism that was not implemented in neither The FriendRadar or in FindMyFriends was the possibility to say that you are at a different place than you in reality are, to lie about your location. If implemented the right way, this could another mechanism that helps the users to plausible deny disclosure of their location. The users of FindMyFriends did not see the purpose of this functionality except for a couple of user that said they would use it for fun. Many users in fact pointed out that this opportunity would ruin the whole concept of the system and that the system could no longer be trusted. About the same results did appear when this question was asked to the users of The FriendRadar, only two users said they would have used it in The FriendRadar and the one user that commented this answer said that it would be fun to fool someone. Six users did not know and six did not want to lie about their location. One of the 'No' respondents said that if one could lie, the purpose of The FriendRadar would disappear. Others said that they rather would log off the network than lie about their location. Also these results change dramatically when the users are asked if they would use a 'lie' functionality in a system where you could be located anywhere. In this case eleven users said that they thought they would use a 'lie' functionality, and only three said they would not. The textual answers shows for the first time someone that thought they would use it as a privacy mechanism, where one commented that it would be used for safety and one commented that it would use to hide embarrassment of their location. The results alone can indicate that such functionality would be necessary. A mistake was made however when designing this question for the questionnaire, as the 'Don't know' alternative disappeared. It is difficult to judge how many users that would answered 'Don't know' to this question, but the relative few comments indicates that it could be quite a few. As the testing of Connecto (Barkhuus, Brown et al. 2008) where the users had the possibility to suppress the automatically positioning and write in any location they wanted, this functionality was not used for privacy reasons, but used for giving the other users a better idea of what their actual location was. This again shows, as mentioned before, that the users either conveyed the location that they thought would give the other users most information, or they did not convey their location at all. This is confirmed by the comments from the respondents of the questionnaire and by the interviewee that said they would rather just log of the system, instead of lying about their location. Therefore, it is doubtful that a lie functionality would be of great importance for the users. It can in fact, as some users pointed out, damage the users trust in the accuracy of the system.

At last, there was some considered privacy mechanisms that was not implemented in The FriendRadar. The most important ones are the possibility to group friends and getting notice by the system when other localises you. The grouping of friends was not implemented because all of the users in this system were considered to be in the same group. The three groups that probably is mentioned the most in the literature about this subject is friends, family and work. Many studies has shown that the identity if the enquirer of location are of more importance than the user's current location (Lederer, Mankoff et al. 2003; Consolvo, Smith et al. 2005). Grouping of friend offer the users more control with less effort in configuring privacy settings, as all the members of each group has the same privacy settings. From this study it is difficult to say if it would benefit a

location-tracking system or not, but the interviewee said that he would not use it as a privacy mechanism, but as a mechanism to get better overview of his friends. Some respondents of the questionnaire about The FriendRadar, the interviewee and the interviewees from FindMyFriends said that they would have fewer friends in a system that could locate them in a larger area. This can indicate that it could be enough to have individual privacy settings, since the effort to configure the privacy settings individually decrease if they have few friends. To get a notification each time one get localised by others was not implemented mainly because the system was designed such as all the friends of a user was shown at the map each time the user shows the map. This could lead to many irrelevant location notifications for the users, as they might not be the target of the user that localises them. On the other hand, it gives the users better feedback over what other actually do see about them. A solution that might have worked was if the users only could localise one and one of her friends on the map, and each time the user opens a new friend's map, the friend get a notice about it. This would increase the feedback to the friends, but it would decrease the usability of the system. The interviewee felt that this could be a useful feature about a future system even if it used a single map which showed all the friends at once. It remains an open question however, if giving notice to users when they are localised is beneficial for a location-tracking system.

As mentioned in the start of this section, if a location-based system is implemented with the right amount of privacy mechanisms, the system can be both useful and privacy preserving. What the 'right' amount is, is difficult to tell. This study however has shown that to the possibility to turn off the system, or at least the position functionality, is of utterly importance if a location-tracking system would be used. It would beneficial if the system could be turned off in such a way that it offers the users plausible deniability. Further, such a system should have individual privacy settings for each friend, as this would be more precise and since users of location-tracking system probably would have few friends. Finally, a system that only can locate users within a limited physical area, would probably actually benefit from not implementing reciprocity of location sharing. This could lead to a system with a higher usefulness for the users, as they can check if any of their friends are within that limited area, even if they are not inside that area themselves. The increased possibility of plausible deniability that the fact that one can only be localised some places give, seems to weigh up for the lost privacy this decreased reciprocity in location sharing gives. If the system can locate users worldwide however, reciprocity of location sharing seems extremely important. Since it is already said that the positioning functionality should be able to turn off, this reciprocity will mean that a user will only be able to locate others when her own positioning functionality is turned on. It seems that both kinds of systems however, will benefit from having reciprocity in location sharing in each individual friendship, which means that the strictest privacy options chosen by the two parts in a friendship counts for both parts of the friendship. This study suggests that a system with these privacy mechanisms implemented with have the right amount of privacy mechanisms, and therefore be both privacy preserving and useful for the users. If more privacy mechanisms was implemented it would decrease the usefulness of the system, by either making the use of the system too cumbersome or by decreasing the users trust in the accuracy of the system.

7.6 Threats to validity

Some threats to the validity of the results from the logged data and the questionnaire exist. These will shortly be discussed in this section.

First, too few users participated both in the experiment and in the questionnaire to make it possible to generalise the results from this study. At least 30 test users would be a minimum size to do assumptions that counts for the whole population (Oates 2006). Thus, all the conclusions presented in this master's thesis are based on indications and not statistically proved results.

Further, the fact that some users received the iPod three days later than the rest of the users and therefore registered to the system a little late can threaten the realism of the results.

Next, some issues of the questionnaire can be considered threats to the validity of the results. First, question 15 that asked if the users had participated in the experiment *and* received an iPod was double barrelled as it asked two questions at once. It seems however like the users understand this question as a question about if they received an iPod. Second, question 29 and 30 that asked question about if the users had located themselves on the map, was clearly misunderstood. These results however are not considered in the discussion and have no effect on the conclusions. Third, the second lie question, question 55, did not have a 'Don't know' alternative like the first lie question. On the other hand, this question had a comment field that made this mistake less serious. Finally, a question was not asked in the questionnaire that should have been asked. The users should have been asked why they did not accept all their friend requests, because it would be interesting to know if they were not accepted on purpose or if they were just unseen requests.

Finally, the problems with Wireless Trondheim have probably affected the results, but this issue are dealt with through both the results and the discussion of this master's thesis.

8 Conclusions and further work

This chapter will first present the conclusions of the findings discussed in the previous chapter followed by the further work.

8.1 Conclusions

This master's thesis has investigated four research questions by the use of a prototype location-tracking system developed for this thesis called The FriendRadar. This system was tested on specifically selected test subjects which was equipped with mobile devices. The test subject's usage of the system was analysed using data logged by the system and followed up with a questionnaire sent to all the test persons and an interview of one of the test persons.

The users had to be connected to Wireless Trondheim to be able to be located with The FriendRadar. This study has shown that Wireless Trondheim is not suited for this kind of usage, mainly because the connection is lost when moving around with the device. There was also several other problems with Wireless Trondheim like bad coverage, low speed and the fact that users had difficulties to connect to the network in the first place. The choice of Apple's iPod Touch as the mobile device and gymnasium pupils as test persons seems to be right however. The iPod was used a lot by the test persons and it was user friendly for the users. The users also were satisfied with its coolness.

To answer the first research question of this master's thesis it was investigated if people are interested in using a system for locating and interacting with their friend and family using mobile devices connected to a wireless network. This was done by looking at the logged usage of The FriendRadar, together with the answers of the questionnaire and from the interview. The results from these studies showed that The FriendRadar was not used much by the test users. This is probably due to two factors that both amplify each other; the difficulties with Wireless Trondheim and the initial low user mass. The users expressed however great enthusiasm about the concept of being able to locate their friends and almost all users said they would use a similar system if all the shortcomings of the system and the positioning were fixed. It also seems that users are willing to use a location-tracking system if it would locate users worldwide. Further results indicate that the users naturally assume that they have to share their location to be able to see other's location in a worldwide system, and that they are willing to do so to achieve this. It seems like whether a user will use a location-tracking system or not is a tradeoff between the usefulness of the system and the user's privacy concerns. If the privacy mechanisms is balanced correctly, it seems that location-tracking systems have great potential to achieve a large user mass. It also seems that female users are more interested in using such systems than male users. Finally, it seems that a future system would benefit from being a simple instant messaging system, instead of a more complex social network system. This system should share both messages and location synchronously and directly between users.

Further, it was investigated if users of a system that reveals the users' location to others behave in a different way than they would have without using the system. This was done by using the answers from the questionnaire and the interview, together with results from the preliminary study about FindMyFriends and earlier research by other authors. The answers from the users of The FriendRadar indicate that the users of the system in general did not act in different ways because they could see others location. The study of FindMyFriends however had several examples of users that did actions that they would not have done without knowing their friends location. The same is shown by other surveys. Their actions which was different was mostly spontaneous actions, that appeared from their knowledge of their friends locations. The users of The FriendRadar did not act in a different way as a consequence of that they knew that others could see their location either, but they imagine they would do if the system was worldwide. The results from FindMyFriends also shows that in general, that the system did not hinder the users to do things they did not want other

people to know, but instead the users hindered the system to show they were doing it. Other studies show that users in fact do act in different ways to use the location-tracking system for their own advantage. They actively use the system to show others where they are or what they are doing, because the want others to find them.

Next, it was investigated if users that share location information feel that they are loosing their own personal privacy. Results from the interview and the questionnaire were used to investigate this. The results indicate that the users of The FriendRadar were not concerned about privacy at all while using the system, but as explained, it was not used much. The users did not seem to be overly concerned about future systems that could locate them anywhere either, but some users showed slight concerns about it. Most of the users seemed to be more excited about the new possibilities this would give instead. When specifically asked however, most of the users showed that they would want to use privacy mechanisms as turning off the system if they could be located anywhere, which indicate some concerns. The male users seemed to be less worried about their personal privacy in location tracking systems, than the females.

Finally, it was investigated how privacy mechanisms could help the users of location-tracking systems not to loose their personal privacy. This was done both by studying existing literature, and by asking the respondents of the questionnaire and the interviewee directly about these mechanisms. The study shows that privacy mechanisms are essential for users to want to use location-tracking systems, but they have to be balanced in such a way that they do not remove the possibilities such systems offers. If the right amount of privacy mechanisms are implemented to a location-tracking system, the system can both be privacy preserving and useful for the users. This study suggests that the right privacy mechanisms are the possibility to turn the positioning functionality off, and do this either towards all users or towards individual users. Further, if the location-system is worldwide, reciprocity in location sharing is essential, but if the system only locates users inside a limited area not larger than a city, this reciprocity only hampers the users' experience of the system. If further privacy mechanisms are added, it seems that the system no longer is useful enough for the users, and therefore will not be used.

8.2 Further work

This master's thesis has looked at several aspects of a location-tracking system meant for users to locate their friends. It is concluded that this concept is of great interest for the users, but that sufficient privacy mechanisms must be implemented. It has also shown that The FriendRadar was not used very much, among others as a consequence of the problems with Wireless Trondheim. Therefore, a study of a similar system that is based on another location technology and that had more users, would be necessary to be able to confirm the results found in this master's thesis. Even if it is outside the scope of this master's thesis, a combination of GSM and GPS positioning would seem a reasonable choice that makes it possible to locate each other almost anywhere in the world. The suggestions from this master's thesis could be used in the development of the system. If these are followed the system will be an instant messaging system where the users' location and messages are shared synchronously and directly between the users without any central server. It should be possible to turn off the positioning functionality, but if a user has turned it off, she will not be able to see the location of her friends either. Finally, the system's users should be able to turn the positioning off towards some users, and keep it on towards others.

Bibliography

Ahern, S., D. Eckles, N. S. Good, S. King, M. Naaman and R. Nair (2007). Over-exposed?: privacy patterns and considerations in online and mobile photo sharing. Proceedings of the SIGCHI conference on Human factors in computing systems. San Jose, California, USA, ACM.

Andresen, S., J. Krogstie and T. Jelle (2007). Lab and Research Activities in Wireless Trondheim Proceedings of IEEE International Symposium on Wireless Communication Systems. Trondheim, Norway**:** 385 - 389.

Barkhuus, L. (2004). Privacy in Location-Based Services, Concern vs. Coolness. Mobile HCI 2004 Workshop on Location Systems Privacy and Control. Glasgow.

Barkhuus, L., B. Brown, M. Bell, S. Sherwood, M. Hall and M. Chalmers (2008). From awareness to repartee: sharing location within social groups. Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems. Florence, Italy, ACM**:** 497-506.

Barkhuus, L. and A. K. Dey (2003). Location-Based Services for Mobile Telephony: a study of users' privacy concerns. Proceeding of the INTERACT 2003, 9th IFIP TC13 International Conference on Human-Computer Interaction**:** 709 -712.

Bellavista, P., A. Küpper and S. Helal (2008). "Location-Based Services: Back to the Future." Pervasive Computing, IEEE **7**(2): 85-89.

Bellotti, V. and A. Sellen (1993). "Design for privacy in ubiquitous computing environments." Proceedings of the third conference on European Conference on Computer-Supported Cooperative Work: 77-92.

Colbert, M. (2001). A diary study of rendezvousing: implications for position-aware computing and communications for the general public. Proceedings of the 2001 International ACM SIGGROUP Conference on Supporting Group Work. Boulder, Colorado, USA, ACM.

Consolvo, S., I. E. Smith, T. Matthews, A. LaMarca, J. Tabert and P. Powledge (2005). Location disclosure to social relations: why, when, & what people want to share. Proceedings of the SIGCHI conference on Human factors in computing systems. Portland, Oregon, USA, ACM.

Dey, A. K., G. D. Abowd and D. Salber (2001). "A conceptual framework and a toolkit for supporting the rapid prototyping of context-aware applications." Human-computer interaction **16**(2, 3 & 4): 97.

Grandhi, S. A., Q. Jones and S. Karam (2005). Sharing the big apple: a survey study of people, place and locatability. CHI '05 extended abstracts on Human factors in computing systems. Portland, OR, USA, ACM.

ITavisen. (2001). "Finn vennene dine med SMS." Retrieved 13. December, 2007, from http://www.itavisen.no/showArticle.php?articleId=1296979.

Jiang, X., J. I. Hong and J. A. Landay (2002). "Approximate information flows: Socially-based modeling of privacy in ubiquitous computing." UbiComp 2002: Ubiquitous Computing : 4th International Conference, Göteborg, Sweden, September 29 - October 1, 2002. Proceedings: 176.

Jones, Q. and S. Grandhi (2005). "P3 systems: putting the place back into social networks." IEEE internet computing **9**(5): 38.

Junglas, I. A. and R. T. Watson (2008). "Location-based services." Commun. ACM **51**(3): 65-69.

Langheinrich, M. (2001). "Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems " Proceedings of the 3rd international conference on Ubiquitous Computing 273-291

Lederer, S., J. I. Hong, A. K. Dey and J. A. Landay (2004). "Personal privacy through understanding and action: five pitfalls for designers." Personal and ubiquitous computing **8**(6): 440-454.

Lederer, S., J. Mankoff and A. K. Dey (2003). Who wants to know what when? privacy preference determinants in ubiquitous computing. CHI '03 extended abstracts on Human factors in computing systems. Ft. Lauderdale, Florida, USA, ACM.

mBuddy. (2007). "mBuddy homepage." Retrieved 14. December, 2007, from http://www.mbuddy.no.
Navizon. (2007). "Navizon - Virtual GPS for mobile devices and laptop computers " Retrieved 16. December, 2007, from http://www.navizon.com/.
NRK. (2007). "Vil stoppe mobiltjenester." Retrieved 14. December, 2007, from http://nrk.no/nyheter/kultur/1.4300325.
O'Reilly, T. (2005). "What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software." Retrieved 14. December, 2007, from http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html.
Oates, B. J. (2006). Researching information systems and computing. London, SAGE.
Orwell, G. (1949). Nineteen Eighty-Four. A novel, Secker & Warburg: London.
Palen, L. (1999). "Social, individual and technological issues for groupware calendar systems." Proceedings of the SIGCHI conference on Human factors in computing systems: the CHI is the limit 17-24
Palen, L. and P. Dourish (2003). "Unpacking "privacy" for a networked world." Proceedings of the SIGCHI conference on Human factors in computing systems: 129-136
Raento, M. and A. Oulasvirta (2005). "Privacy management for social awareness applications." The Workshop on Context Awareness for Proactive Systems (CAPS 2005): 105-114.
Robson, C. (2002). Real world research: a resource for social scientists and practitioner - researchers. Oxford, Blackwell.
Weber, W., J. M. Rabaey and E. Aarts (2005). Ambient Intelligence. Berlin, Heidelberg, Springer-Verlag Berlin Heidelberg.
Weiser, M. (1993). "Hot topics-ubiquitous computing." Computer **26**(10): 71-72.

Appendix A – The questionnaire

Questionnaire

Nr	Condition	Question	Alternatives
1. General questions			
1.		Gender:	-Male -Female
2.		Do you have a profile on Facebook?	-Yes -No
3.	Q2 – Yes	Why do you have a profile on Facebook?	Text
4.	Q2 – Yes	How many friends do you have on Facebook?	-0-19 -20-49 -50-99 -10-199 -200-300 -More than 300
5.	Q2 – Yes	How often do you log in on Facebook?	-Several times per day -About one time per day -Several time per week -About one time per week -About every other week -About one time per month -Less frequent
6.	Q2 – Yes	Do you feel that Facebook is an important part of your life?	-Yes -No
7.	Q6 - Yes	In which way are Facebook an important part of your life?	Text
8.	Q6 - No	Why are Facebook not an important part of your life?	Text
9.	Q2 – Yes	What do you use Facebook for?	Text
10.	Q2 – Yes	What do you think of your personal privacy in Facebook?	Text
11.	Q2 – No	Why do you not have a profile on Facebook?	Text
12.		How many other similar services are you registered to in addition to Facebook?	-0 -1 -2-3 -4-5 -More than 5
13.		Which mobile devices do you own?	(Choose one or many) -Mobile phone -Laptop -PDA -Mp3-player (iPod etc) -Other -None
14.		Have you participated in the testing of the	-Yes

		systems and received an iPod?	-No
15.	Q14 - Yes	How much have you used the iPod you received?	-I have not used it -I have used it once -I have used it a couple of times -I have used it fairly much -I have used it a lot
16.	Q14 – Yes	How much have you used the iPod at the following places? 1 means that you have used it very little, and 5 mean that you have used it a lot.	(Range, 1 to 5) -At home -At school -Other places
17.	Q14 – Yes	How much have you used the iPod to do the following activities? 1 means that you have used it very little, and 5 mean that you have used it a lot.	(Range, 1 to 5) -Listen to music -Watch saved video -Surf the web -Be at YouTube -Use The FriendRadar -Use @school -Other things
18.	Q14 – Yes	How difficult do you think it was to perform the following tasks? 1 means very easy and 5 means very difficult	(Range, 1 to 5) -Connect to wireless internet -Surf the Web -Upload music
19.	Q14 –Yes	How many times have you tried to connect to Wireless Trondheim with the iPod?	-0 -1 -2-3 -4-5 -6-10 -11-20 -More that 20 times
20.	Q14 –Yes	How many times have you <u>managed</u> to connect to Wireless Trondheim with the iPod?	-0 -1 -2-3 -4-5 -6-10 -11-20 -More that 20 times
21.		Do you feel that the coverage of Wireless Trondheim was good enough to use in practice?	-Yes -No -Don't know
2. Questions about The FriendRadar			
22.	Q14-Yes	How many times have you logged in to The FriendRadar from the iPod during the test period?	-0 -1 -2-3 -4-5 -6-10 -More than 10 times
23.	Q14-Yes	How many times have you logged to The FriendRadar from a regular computer during the test period?	-0 -1 -2-3

			-4-5 -6-10 -More than 10 times
24.	Q14-Yes	Would you have used the system more or less if you could have seen your friend's location even if you were not connected to Wireless Trondheim yourself?	-More -Less -About the same
25.	Q14-Yes	How many friends did you have at The FriendRadar?	-0 -1-3 -4-6 -7-10 -11-15 -More than 15 friends
26.	Q14-Yes	Have you logged in to The FriendRadar with the intention to check where your friends were located?	-Yes -No
27.	Q26 – Yes	How many times have you logged in to The FriendRadar with the intention to check where your friends were located?	-1 time -2 times -3 times -4 times -5 times -6 times or more
28.	Q26 – No	Why haven't you logged in to The FriendRadar with the intention to check where your friends were located?	Text
29.	Q14-Yes	How many times have you tried to find yourself on the map in The FriendRadar?	-No times -1 time -2 times -3 times -4 times -5 times -6 times or more
30.	Q14-Yes	How many times have you found yourself on the map in The FriendRadar?	-No times -1 time -2 times -3 times -4 times -5 times -6 times or more
31.	Q14-Yes	Have you ever found any of your friends on the map in The FriendRadar?	-Yes -No
32.	Q31-Yes	How many times have you found some of your friends on the map in The FriendRadar?	-1 time -2 times -3 times -4 times -5 times -6 times or more
33.	Q31-Yes	Have you ever tried to look up (physically) any of the friends that you have found on The FriendRadar?	-Yes -No

34.	Q33-Yes	How many times have you tried to look up (physically) any of the friends that you have found on The FriendRadar?	-1 time -2 times -3 times -4 times -5 times -6 times or more
35.	Q33-Yes	Have you ever found (physically) some of the friend you tried to look up?	-Yes -No
36.	Q35-Yes	How many times have you found (physically) some of the friends you have tried to look up?	-1 time -2 times -3 times -4 times -5 times -6 times or more
37.	Q35-No	Why haven't you found them?	Text
38.	Q33-No	Why haven't you tried to find them?	Text
39.	Q31-No	Why haven't you found them on the map?	Text
40.	Q14-Yes	Do you feel that the iPod combined with The FriendRadar's positioning-functionality has disturbed your own private life?	-Yes -No
41.	Q14-Yes	Have you ever behaved in different way when you have used the iPod in Wireless Trondheim than you would have done without the iPod, because you knew that all your friends could see where in the city you where located?	-Yes -No
42.	Q41-Yes	What have you done that is different?	Text
43.	Q14-Yes	How many times have you deliberately avoided connecting the iPod to Wireless Trondheim because you did not want other to be able to locate you downtown with The FriendRadar?	-More than 5 times -2-4 times -1 time -No times
44.	Q14-Yes	How many times have you left the iPod on a place where you were not, because you did not want it to show your real location?	-More than 5 times -2-4 times -1 time -No times
45.	Q14-Yes	If the system had the possibility to 'lie' on your location, would you have used this functionality?	-Yes -No -Don't know [Comment field]
46.	Q14-Yes	Was it some friends that you did not allow to see you on the map?	-Yes -No [Comment field]
47.	Q14-Yes	Were you ever afraid of that the system administrator or others would use your location or other information about you that was saved in The FriendRadar to something you did not know about?	-Yes -No
48.	Q47-Yes	What were you afraid they would use it for?	Text
49.	Q14-Yes	Have you ever sent a message through The FriendRadar?	-Yes -No
50.		Would you use a similar system as The	-Yes

		FriendRadar if it was put on the market, and all the shortcomings of the system and the positioning was fixed?	-No
51.		What do you think about the concept behind The FriendRadar, namely is the possibility to locate your friends?	Text
52.		If you have other comments concerning the usage or the functionality of The FriendRadar you can write it here.	Text
53.	Q14-Yes	Would you use The FriendRadar more or less if you could be located everywhere independent on which network you was connected to?	-More -Less -The same [Comment field]
54.	Q14-Yes	If you had been located anywhere, would you allow the same friends to see you at the map as you did in The FriendRadar?	-Yes -No, I would have allowed fewer to see me on the map -No, I would have allowed more to see me on the map
55.	Q14-Yes	If you had been located anywhere, do you think that you would have used a 'lie' functionality as mentioned earlier?	-Yes -No [Comment field]
56.	Q14-Yes	If you had been located anywhere and it had been possible to turn the system off, would you have used this turn-off functionality?	-Yes -No [Comment field]
57.		If you imagine that you could choose between a system that are very similar to MSN and where you could be located anywhere, and a system that is very similar to Facebook and where you could be located anywhere, which system would you choose?	-The MSN system -The Facebook system [Comment field]
58.		Would you have used one of the systems mentioned above if it was <u>not</u> possible to turn off the positioning-functionality?	-Yes -No -Maybe
59.		Would you have used one of the systems mentioned above if it <u>was</u> possible to turn off the positioning-functionality?	-Yes -No -Maybe

Results from questionnaire

1. Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	9	56,3	56,3	56,3
	Male	7	43,8	43,8	100,0
	Total	16	100,0	100,0	

2. Do you have a profile on Facebook?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Y	16	100,0	100,0	100,0

4. How many friends do you have on Facebook?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0-19	1	6,3	6,3	6,3
	50-99	2	12,5	12,5	18,8
	100-199	4	25,0	25,0	43,8
	200-300	6	37,5	37,5	81,3
	300+	3	18,8	18,8	100,0
	Total	16	100,0	100,0	

5. How often do you log in on Facebook?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	One time per day	8	50,0	50,0	50,0
	Several time per day	6	37,5	37,5	87,5
	Several times per week	2	12,5	12,5	100,0
	Total	16	100,0	100,0	

6. Do you feel that Facebook is an important part of your life?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	N	12	75,0	75,0	75,0
	Y	4	25,0	25,0	100,0
	Total	16	100,0	100,0	

12. How many other similar services are you registered to in addition to Facebook?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	2	12,5	12,5	12,5
	1	8	50,0	50,0	62,5
	2-3	5	31,3	31,3	93,8
	4-5	1	6,3	6,3	100,0
	Total	16	100,0	100,0	

13. Which mobile devices do you own? [Mobile phone]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Y	16	100,0	100,0	100,0

13. Which mobile devices do you own? [Laptop]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		6	37,5	37,5	37,5
	Y	10	62,5	62,5	100,0
	Total	16	100,0	100,0	

13. Which mobile devices do you own? [PDA]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		15	93,8	93,8	93,8
	Y	1	6,3	6,3	100,0
	Total	16	100,0	100,0	

13. Which mobile devices do you own? [mp3-player (iPod etc)]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Y	16	100,0	100,0	100,0

13. Which mobile devices do you own? [Others]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		12	75,0	75,0	75,0
	Y	4	25,0	25,0	100,0
	Total	16	100,0	100,0	

13. Which mobile devices do you own? [None]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		16	100,0	100,0	100,0

14. Have you participated in the testing of the systems and received an iPod?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	N	2	12,5	12,5	12,5
	Y	14	87,5	87,5	100,0
	Total	16	100,0	100,0	

15. How much have you used the iPod you received?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	.	2	12,5	12,5	12,5
	Fairly much	2	12,5	12,5	25,0
	A lot	6	37,5	37,5	62,5
	Couple of times	6	37,5	37,5	100,0
	Total	16	100,0	100,0	

16. How much have you used the iPod at the following places? [At home]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	3	18,8	21,4	21,4
	3	4	25,0	28,6	50,0
	4	6	37,5	42,9	92,9
	5	1	6,3	7,1	100,0
	Total	14	87,5	100,0	
Missing	System	2	12,5		
Total		16	100,0		

16. How much have you used the iPod at the following places? [At school]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	2	12,5	14,3	14,3
	2	5	31,3	35,7	50,0
	3	5	31,3	35,7	85,7
	4	2	12,5	14,3	100,0
	Total	14	87,5	100,0	
Missing	System	2	12,5		
Total		16	100,0		

16. How much have you used the iPod at the following places? [Other places]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	2	12,5	14,3	14,3
	2	5	31,3	35,7	50,0
	3	1	6,3	7,1	57,1
	4	2	12,5	14,3	71,4
	5	4	25,0	28,6	100,0
	Total	14	87,5	100,0	
Missing	System	2	12,5		
Total		16	100,0		

17. How much have you used the iPod to do the following activities? [Listen to music]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	1	6,3	7,1	7,1
	3	1	6,3	7,1	14,3
	4	4	25,0	28,6	42,9
	5	8	50,0	57,1	100,0
	Total	14	87,5	100,0	
Missing	System	2	12,5		
Total		16	100,0		

17. How much have you used the iPod to do the following activities? [Watch saved videos]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	8	50,0	57,1	57,1
	2	1	6,3	7,1	64,3
	4	5	31,3	35,7	100,0
	Total	14	87,5	100,0	
Missing	System	2	12,5		
Total		16	100,0		

17. How much have you used the iPod to do the following activities? [Surf the Web]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	1	6,3	7,1	7,1
	2	5	31,3	35,7	42,9
	3	4	25,0	28,6	71,4
	4	2	12,5	14,3	85,7
	5	2	12,5	14,3	100,0
	Total	14	87,5	100,0	
Missing	System	2	12,5		
Total		16	100,0		

17. How much have you used the iPod to do the following activities? [Be at YouTube]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	5	31,3	35,7	35,7
	2	6	37,5	42,9	78,6
	4	2	12,5	14,3	92,9
	5	1	6,3	7,1	100,0
	Total	14	87,5	100,0	
Missing	System	2	12,5		
Total		16	100,0		

17. How much have you used the iPod to do the following activities? [Use The FriendRadar]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	7	43,8	50,0	50,0
	2	5	31,3	35,7	85,7
	3	2	12,5	14,3	100,0
	Total	14	87,5	100,0	
Missing	System	2	12,5		
Total		16	100,0		

17. How much have you used the iPod to do the following activities? [Use @school]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	11	68,8	78,6	78,6
	2	1	6,3	7,1	85,7
	3	1	6,3	7,1	92,9
	5	1	6,3	7,1	100,0
	Total	14	87,5	100,0	
Missing	System	2	12,5		
Total		16	100,0		

17. How much have you used the iPod to do the following activities? [Other things]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	11	68,8	78,6	78,6
	2	1	6,3	7,1	85,7
	4	2	12,5	14,3	100,0
	Total	14	87,5	100,0	
Missing	System	2	12,5		
Total		16	100,0		

18. How difficult do you think it was to perform the following tasks? [Connect to Wireless Internet]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very easy	4	25,0	28,6	28,6
	Easy	3	18,8	21,4	50,0
	Medium	3	18,8	21,4	71,4
	Difficult	2	12,5	14,3	85,7
	Very difficult	2	12,5	14,3	100,0
	Total	14	87,5	100,0	
Missing	System	2	12,5		
Total		16	100,0		

18. How difficult do you think it was to perform the following tasks? [Surf the Web]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very easy	4	25,0	28,6	28,6
	Easy	3	18,8	21,4	50,0
	Medium	3	18,8	21,4	71,4
	Difficult	1	6,3	7,1	78,6
	Very difficult	3	18,8	21,4	100,0
	Total	14	87,5	100,0	
Missing	System	2	12,5		
Total		16	100,0		

18. How difficult do you think it was to perform the following tasks? [Upload music]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very easy	8	50,0	57,1	57,1
	Easy	2	12,5	14,3	71,4
	Difficult	2	12,5	14,3	85,7
	Very difficult	2	12,5	14,3	100,0
	Total	14	87,5	100,0	
Missing	System	2	12,5		
Total		16	100,0		

19. How many times have you tried to connect to Wireless Trondheim with the iPod?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2-3	1	6,3	7,1	7,1
	4-5	5	31,3	35,7	42,9
	6-10	6	37,5	42,9	85,7
	11-20	2	12,5	14,3	100,0
	Total	14	87,5	100,0	
Missing	System	2	12,5		
Total		16	100,0		

20. How many times have you managed to connect to Wireless Trondheim with the iPod?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	4	25,0	28,6	28,6
	1	2	12,5	14,3	42,9
	2-3	7	43,8	50,0	92,9
	6-10	1	6,3	7,1	100,0
	Total	14	87,5	100,0	
Missing	System	2	12,5		
Total		16	100,0		

21. Do you feel that the coverage of Wireless Trondheim was good enough to use in practice?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	13	81,3	81,3	81,3
	Don't know	3	18,8	18,8	100,0
	Total	16	100,0	100,0	

22. How many times have logged in to The FriendRadar from the iPod during the test period?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	5	31,3	35,7	35,7
	1	2	12,5	14,3	50,0
	2-3	4	25,0	28,6	78,6
	4-5	3	18,8	21,4	100,0
	Total	14	87,5	100,0	
Missing	System	2	12,5		
Total		16	100,0		

23. How many times have you logged to The FriendRadar from a regular computer during the the test period?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	2	12,5	14,3	14,3
	1	5	31,3	35,7	50,0
	2-3	5	31,3	35,7	85,7
	4-5	1	6,3	7,1	92,9
	6-10	1	6,3	7,1	100,0
	Total	14	87,5	100,0	
Missing	System	2	12,5		
Total		16	100,0		

24. Would you have used the system more or less if you could have seen your friend's location even if you was not connected to Wireless Trondheim yourself?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	.	2	12,5	12,5	12,5
	The same	9	56,3	56,3	68,8
	More	5	31,3	31,3	100,0
	Total	16	100,0	100,0	

25. How many friends did you have at The FriendRadar?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	2	12,5	14,3	14,3
	4-6	2	12,5	14,3	28,6
	7-10	5	31,3	35,7	64,3
	11-15	4	25,0	28,6	92,9
	15+	1	6,3	7,1	100,0
	Total	14	87,5	100,0	

Missing	System	2	12,5		
Total		16	100,0		

26. Have you logged in to The FriendRadar with the intention to check where your friends were located?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		2	12,5	12,5	12,5
	N	8	50,0	50,0	62,5
	Y	6	37,5	37,5	100,0
	Total	16	100,0	100,0	

27. How many times have you logged in to The FriendRadar with the intention to check where your friends were located?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	2	12,5	33,3	33,3
	2	3	18,8	50,0	83,3
	5	1	6,3	16,7	100,0
	Total	6	37,5	100,0	
Missing	System	10	62,5		
Total		16	100,0		

29. How many times have you tried to find yourself on the map in The FriendRadar?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	9	56,3	64,3	64,3
	1	5	31,3	35,7	100,0
	Total	14	87,5	100,0	
Missing	System	2	12,5		
Total		16	100,0		

30. How many times have you found yourself on the map in The FriendRadar?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	11	68,8	78,6	78,6
	1	2	12,5	14,3	92,9
	3	1	6,3	7,1	100,0
	Total	14	87,5	100,0	
Missing	System	2	12,5		
Total		16	100,0		

31. Have you ever found any of your friends on the map in The FriendRadar?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		2	12,5	12,5	12,5
	N	9	56,3	56,3	68,8
	Y	5	31,3	31,3	100,0
	Total	16	100,0	100,0	

32. How many times have you found some of your friends on the map in The FriendRadar?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	3	18,8	60,0	60,0
	2	1	6,3	20,0	80,0
	6	1	6,3	20,0	100,0
	Total	5	31,3	100,0	
Missing	System	11	68,8		
Total		16	100,0		

33. Have you ever tried to look up (physically) any of the friends that you have found on The FriendRadar?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		11	68,8	68,8	68,8
	N	3	18,8	18,8	87,5
	Y	2	12,5	12,5	100,0
	Total	16	100,0	100,0	

34. How many times have you tried to look up (physically) any of the friends that you have found on The FriendRadar?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	1	6,3	50,0	50,0
	5	1	6,3	50,0	100,0
	Total	2	12,5	100,0	
Missing	System	14	87,5		
Total		16	100,0		

35. Have you ever found (physically) some of the friend you tried to look up?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		14	87,5	87,5	87,5
	N	1	6,3	6,3	93,8
	Y	1	6,3	6,3	100,0
	Total	16	100,0	100,0	

36. How many times have you found (physically) some of the friends you have tried to look up?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	1	6,3	100,0	100,0
Missing	System	15	93,8		
Total		16	100,0		

40. Do you feel that the iPod combined with The FriendRadar's positioning-functionality has disturbed your own private life?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		2	12,5	12,5	12,5
	N	14	87,5	87,5	100,0
	Total	16	100,0	100,0	

41. Have you ever behaved in different way when you have used the iPod in Wireless Trondheim than you would have done without the iPod, because you knew that all your friends could see where in the city you where located?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		2	12,5	12,5	12,5
	N	14	87,5	87,5	100,0
	Total	16	100,0	100,0	

43. How many times have you deliberately avoided connecting the iPod to Wireless Trondheim because you did not want other to be able to locate you downtown with The FriendRadar?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	14	87,5	100,0	100,0
Missing	System	2	12,5		
Total		16	100,0		

44. How many times have you left the iPod on a place where you were not, because you did not want it to show your real location?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	14	87,5	100,0	100,0
Missing	System	2	12,5		
Total		16	100,0		

45. If the system had the possibility to 'lie' on your location, would you have used this functionality?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		2	12,5	12,5	12,5
	Yes	2	12,5	12,5	25,0
	No	6	37,5	37,5	62,5
	Don’t know	6	37,5	37,5	100,0
	Total	16	100,0	100,0	

46. Was it some friend that you did not allow to see you on the map?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		2	12,5	12,5	12,5
	No	14	87,5	87,5	100,0
	Total	16	100,0	100,0	

47. Were you ever afraid of that the system administrator or others would use your location or other information about you that was saved in The FriendRadar to something you did not know about?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		2	12,5	12,5	12,5
	N	13	81,3	81,3	93,8
	Y	1	6,3	6,3	100,0
	Total	16	100,0	100,0	

49. Have you ever sent a message through The FriendRadar?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		2	12,5	12,5	12,5
	N	8	50,0	50,0	62,5
	Y	6	37,5	37,5	100,0
	Total	16	100,0	100,0	

50. Would you use a similar system as The FriendRadar if it was put on the market, and all the shortcomings of the system and the positioning was fixed?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	N	3	18,8	18,8	18,8
	Y	13	81,3	81,3	100,0
	Total	16	100,0	100,0	

53. Would you use The FriendRadar more or less if you could be located everywhere independent on which network you was connected to?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	.	2	12,5	12,5	12,5
	The same	7	43,8	43,8	56,3
	More	6	37,5	37,5	93,8
	Less	1	6,3	6,3	100,0
	Total	16	100,0	100,0	

54. f you had been located anywhere, would you allow the same friends to see you at the map as you did in The FriendRadar?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		2	12,5	12,5	12,5
	Fewer	7	43,8	43,8	56,3
	Yes	7	43,8	43,8	100,0
	Total	16	100,0	100,0	

55. If you had been located anywhere, do you think that you would have used a 'lie' functionality as mentioned earlier?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		2	12,5	12,5	12,5
	Yes	11	68,8	68,8	81,3
	No	3	18,8	18,8	100,0
	Total	16	100,0	100,0	

56. If you had been located anywhere and it had been possible to turn the system off, would you have used this turn-off functionality?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		2	12,5	12,5	12,5
	Yes	13	81,3	81,3	93,8
	No	1	6,3	6,3	100,0
	Total	16	100,0	100,0	

57. If you imagine that you could choose between a system that are very similar to MSN and where you could be located anywhere, and a system that is very similar to Facebook and where you could be located anywhere, which system would you choose?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Facebook	7	43,8	43,8	43,8
	MSN	9	56,3	56,3	100,0
	Total	16	100,0	100,0	

58. Would you have used one of the systems mentioned above if it was not possible to turn off the positioning-functionality?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	2	12,5	12,5	12,5
	Maybe	9	56,3	56,3	68,8
	No	5	31,3	31,3	100,0
	Total	16	100,0	100,0	

59. Would you have used one of the systems mentioned above if it was possible to turn off the positioning-functionality?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	11	68,8	68,8	68,8
	Maybe	5	31,3	31,3	100,0
	Total	16	100,0	100,0	

Appendix B - The interview template

Introduce yourself.

Why interview?

Is it OK if the interview is recorded?

Thanks for participating in the interview. You are completely anonymous. Your name will not be mentioned anywhere. If there are any questions that you don't want to answer, just say so. Some questions may be difficult to answer. Just remember that there is no correct or wrong answer, I just want your opinion, and just try to answer as well as you can. You can interrupt me at any time, and ask for clarification in the questions.

Date:	
Gender:	
Did you answer the questionnaire?	

iPod
1: Did you receive an iPod??
2. Did you use it a lot?? How much? Where did you use it?
Yes: for what? No: Why not?
3: What do you think about the iPod??
4: Was it easy to connect to wireless network with the iPod? Substantiate.
5: Was it easy to connect to Wireless Trondheim with the iPod? Substantiate.

6: Was it easy to use the web browser at the iPod? Substantiate.

7: Do you think that the iPod was a suitable device to use The FriendRadar on? Why/why not? Compared to a mobile phone?
FACEBOOK -- MSN
8: Do you have a profile on Facebook??
9: For how long?
10. Why did you register a profile on Facebook??
11. How often do you use it??
12: How many friends?
13: What do you use Facebook for? What is good, what is bad??
14: Any thoughts of protection of your personal privacy on Facebook?
15: Do you use MSN? How much?
16. Do you have most contacts/friends on MSN or Facebook? Do you have the same friends in the both systems?
17. What is most important for you, Facebook or MSN? Why?
18. Are you registered in other social services on internet? MySpace, Nettby, Blink, Friendster, LinkedIn etc.

THE FRIEND RADAR

19. How often did you log into The FriendRadar?

From iPod:
From another computer:

20. Hoe many friends did you have? Why was they your friends? Did you know everyone?

21. What do you think about The FriendRadar?

22: have you any impression about what you classmates think about The FriendRadar?

23. Did you ever manage to log in to the system while you were connected to Wireless Trondheim, such as you found yourself on the map? How many times?

24: Was it any time that you thought that you wanted to check your friends' location with The FriendRadar? Did you do it? Why/why not?

25: Did you ever locate any of your friends on the map? In what situation? Where was they? Did you try to find them? Why/why not?

26: Did you do something you normally would not have done, or avoided doing something you normally would, because you was connected to Wireless Trondheim and knew that your friends could see your location?

27: Did you send messages in the system? Why/why not?

28. Do you generally feel that the system ever disturbed you private life?

29. Was it any functionality that you missed in The FriendRadar?

Mention the following things if no answer:
- Share pictures and video
- Link pictures with location on map

- The system logs the users' last observed position (with timestamp)
- Something else?

30. What do you think about the following functionality in The FriendRadar?

- Choose if you want your location to be shown on the map or not
-
- That it is only possible to see others location when you can be located yourself
-

31. Would it be useful with the following functionality?

- Group your friends with different privacy settings on map and etcetera.
-
- That you get notice if localised by others
-
- Lie about your location
-

32. If The FriendRadar had been put on the market, with connection to Wireless Trondheim, as it is today. Would you have used it? Why/why not?

33. If The FriendRadar was put on the market, and all the problems with Wireless Trondheim was fixed, would you use it? If you was localised anywhere at anytime? How many friends would you have in such a system?

FUTURE SYSTEM

34. If you imagine a system where you can locate your friends. Would you choose a system that is similar to Facebook or similar to MSN?

34.1 What do you think of the concept behind such a system?

35. When you further imagine this system, would you prefer your friends to be localised on a map, that you only would know if they were nearby or would you want that they could write their current location such as the locations was remembered by the system and automatically connected to the location next time?

36. Would you have fewer or more friends in such a system, than you have for instance on MSN or Facebook?

37. Imagine that the system could locate you (your phone or mp3 player) anywhere and anytime, independent on network connection? Do you think that this kind of system would disturb your private life? Why/why not?
38. Would you rather have, or not have, the following functionality if the system could locate you everywhere and anytime? If yes, how important had the following functionality been? Why? -Possible to turn off the positioning functionality -Choose personal settings and map granularity for each friend -That the users only has the opportunity to see other location when they themselves can be located -Group you friends with different privacy settings on each group -That you get notice when other users locates you -That you only can locate friends, that have approved that you can locate them -That you can lie about your own location (say that you are downtown, when you actually are at home for instance)
39. What do you think about such concept/system if all privacy mechansims you want are achieved?
40. Would you be willing to pay for such a system?
41. is there anything else you would like to say about the system or the experiment?

Thank you for the help! This is of great use for me.

Appendix C – The FriendRadar user manual

First time you use the system

The address to The FriendRadar is http://vr.idi.ntnu.no/vr. Write this in a web browser (either on the iPod or another computer). At the iPod the browser is Safari that you will find as an icon in the main menu. Then you will get up a login screen. Turn the iPod you have received, and you will se a sticker with a NTNU logo. On the sticker there is a code in the form 6310-0811-Axx, where xx represents two numbers. Login to the web page by using the three last characters of this code as nickname, in other words: Axx. If it say A15, use A15 as nickname. Write in 'passord' in the password field, which is the standard password. Now you're logged in. The first thing you should do is to edit your profile by choosing edit profile on the profile page. It is important to remember to change you password. Now your profile is ready, and you can start connecting with friends.

Friend settings

When you ask someone if they want to be your friend, or if you get a friend request you will be asked to choose a map setting towards your friend. If both you and your friend choose to be viewed on the map, can you see your friend in the map if he or she is inside the coverage area of Wireless Trondheim. The same thing is valid for your friend. If you choose that the friend can not see you on the map, the friend can't localise you on the map; just see your colour code on the friend list. The same thing is counts for you toward this friend. If you don't want to show on the map, then you can't see your friend on the map either.

Connect to Wireless Trondheim

For the system to be able to know your location, and for you to be able to localise others, you have to connect your iPod to Wireless Trondheim. You do this by choosing Settings in the main menu of the iPod. Then you push the topmost menu choice (Wi-Fi). Then a list over the available networks appears. Here you choose Wireless Trondheim. You are now connected to the network. Then you have to authenticate you on the webpage of Wireless Trondheim. Here you use the username and password you got as a gymnasium pupil in Trondheim.

Find your friends in the city

If you are connected to Wireless Trondheim, you can log in to The FriendRadar to find you friends. When you have logged in, you choose map in the top menu and all your friends that currently are connected to Wireless Trondheim is placed on the map together wit yourself. You can also choose one and one user in the left menu to localise only this person.

The colour codes in the friend list

The friends in the friend list in the left menu can have a background in three different colours: green, yellow or red. The background is red if the user is not connected to Wireless Trondheim, because he is either outside the coverage area or not connected to the network. Users can be localised without being logged in on the webpage, as long as they are connected to Wireless Trondheim. If you are not connected to Wireless Trondheim yourself, all the users get a red background regardless if they are connected to Wireless Trondheim or not. If a friend has a yellow background it means that the friend is connected to Wireless Trondheim, but is located more that 200 metres from you current location. If the friend has a green background, it means that the friend is closer than 200 metres from you current location.

Common mistakes

The map will not be updated: You have to update the map yourself by choosing map in the top menu or by choosing 'Update map'.

I can't see my friend on the map, even though they are located right next to me: If there are several users at the same spot, the markers can be on top of each other on the map, such as they get difficult to see. This can be solved by zooming the map, or choosing to view one friend at the time.

I can't upload a picture of myself: Pictures can only be uploaded from an ordinary computer and not from the iPod. The picture should be less than 100 kilobytes.

I can't get localised even if I am connected to Wireless Trondheim: Try to log in to The FriendRadar again. If this doesn't help, contact Per Anton Gransæther on e-mail (gransath@stud.ntnu.no).

Other errors

Report errors to Per Anton Gransæther on e-mail: gransath@stud.ntnu.no or phone: 93047053.

Have fun!