

Fagrapport
EiT landsby 18 TDT4851, vår 2007:

Cooperation over Internet, using Rich Presence

Gruppe 4, 09.05.2007

Anders Gjerde
Eirik Hodne
Hallvard Røe Evensmoen
Ola Nordbryhn
Vegar Westerlund



NTNU

Norwegian University of Science and Technology
Faculty of Information Technology, Mathematics and Electrical Engineering
Department of Computer and Information Science

Abstract

This report is the result of four months work under the supervision of Telenor and it undertakes issues regarding Rich Presence services, their public acceptance and protection of privacy. Our motivation has been to aid Telenor R&I in their research by producing a report based on several documented references, our own opinions and two in-depth interviews. We have achieved results clearly indicating that people are initially skeptical as to sharing personal info, but are willing to share once the benefits are presented. The most important aspect is whether people trust the system and perceive it as secure and infallible. Our conclusion is that such a system needs to have a low-entry level, flexible options for advanced users, but with pre-defined and strict default settings. To boost the system's popularity, there is a need for a "killer-application".

Please visit our website, <http://prosjekt.idi.ntnu.no/websam/>

Table of Contents

1	Introduction.....	- 3 -
1.1	Approach to the problem	- 3 -
	Elaboration and assumptions	- 3 -
2	Agenda.....	- 4 -
2.1	Methods.....	- 4 -
2.2	Subjects	- 4 -
3	Background.....	- 5 -
3.1	Definitions.....	- 5 -
	Location	- 5 -
	Presence	- 5 -
	Rich Presence.....	- 6 -
3.2	Difference of opinion.....	- 7 -
3.3	Laws and jurisdiction regarding Rich Presence.....	- 7 -
	Code of Fair Information Practices (CFIP).....	- 10 -
4	Services.....	- 11 -
4.1	Pitfalls	- 11 -
4.2	Potential services	- 12 -
4.3	Existing services	- 13 -
4.4	Best-case Scenario services	- 13 -
5	Ethical and social issues.....	- 15 -
5.1	Privacy preferences and sharing patterns in context-aware telephony	- 15 -
	Context disclosure rates	- 15 -
	Context disclosure and social relations.....	- 16 -
	Grouping of social relations.....	- 16 -
	The interest for such a system.....	- 17 -
5.2	mySpace and privacy permissions	- 17 -
	Findings.....	- 18 -
5.3	When privacy is invaded.....	- 19 -
	Mismatch between assumptions made by designers and users.....	- 19 -
	Putting sensitive information to new use.....	- 20 -
	Unintentional privacy invasion	- 20 -
5.4	Security	- 20 -
	Misuse	- 21 -
	System integrity	- 22 -
	Trust.....	- 22 -
	Consequences.....	- 22 -
6	Interview	- 23 -
6.1	Background.....	- 23 -
6.2	Interview: Bjørn Kristian Indergaard.....	- 23 -
6.3	Interview: Tone P. Næss	- 26 -
6.4	Results.....	- 29 -
7	Discussion	- 30 -
7.1	Areas of application	- 30 -
	Killer application	- 30 -
	Range of use.....	- 30 -

A look at existing services	- 31 -
7.2 Quality of data.....	- 32 -
Multiple states	- 32 -
Level of detail	- 32 -
Information integrity	- 33 -
Timeliness of data	- 33 -
7.3 User Experience	- 33 -
Interface	- 33 -
Access control.....	- 33 -
System Trust	- 34 -
7.4 Public acceptance.....	- 34 -
How and when	- 35 -
Time	- 35 -
Level of automation	- 35 -
Coolness.....	- 35 -
Privacy management.....	- 36 -
Pricing.....	- 36 -
Benefits greater than the risk	- 36 -
7.5 Personal thoughts	- 36 -
Ethical concerns	- 37 -
What is to be expected from a serious and large actor	- 37 -
What services may or may not come from third parties	- 37 -
8 Future work.....	- 38 -
9 Conclusive thoughts.....	- 39 -
10 Bibliography	- 40 -
10.1 Books and articles	- 40 -
10.2 Web pages.....	- 40 -
11 Appendix A: Glossary.....	- 42 -
12 Appendix B: Point list used in Interview	- 43 -

1 Introduction

We were given a task from Telenor in which we were to explore the subject of Rich Presence and what is needed to gain public acceptance for such a service. We solved this with guidance from Sune Jakobsson in Telenor R&I in Trondheim and Reidar Conradi, professor of computer science at NTNU. This report is written in English by request from Telenor.

This report has been made at Norwegian University of Science and Technology (NTNU) in a course called Experts in Team (TDT4851). This is a course where people from different background are put together in a group and given a problem area. The group consists of five male students, ranging from 23 to 26 years old from different social and technical backgrounds. The goal is not only to write a final report, but also to learn how a team works. This report will give some of our opinions on the subject of Rich Presence from our point of view.

1.1 Approach to the problem

The question we're seeking an answer to through this report is the following:

“With regards to Rich Presence, what are the ethical and social issues, how can security and privacy be assured and how can public acceptance be achieved?”

Elaboration and assumptions

Our main purpose will be to explore which services users might be interested in and how they affect privacy. We will therefore be looking into some of the services that can be provided with regards to Rich Presence and how they can be accepted by the public. We will look at existing laws and jurisdiction regarding personal information protection, but will not go into detail on their appropriateness. Furthermore we will look into how this system can be used by third parties.

We do not include any technological problems or solutions; rather, we assume that any difficulties can be solved as long as they are technological and economically feasible.

2 Agenda

In this section we elaborate some of the methods that will be used in this report. We also look into which subjects will be investigated further and explain some of our personal views on the problem.

2.1 Methods

We will collect a lot of information by reading existing material related to our problem. But since this is a fairly new subject there exists only scarce amounts of information and research available. We will also use some help from recognized experts within the field as well as conducting a round of interviews, although with a small group of people. Our personal thoughts will also be given some weight in section 7, Discussion.

2.2 Subjects

Our main goal is to find out how public acceptance can be achieved and in this the social and ethical issues is essential. What users are likely to share, with whom and when, as well as finding the line where users feel their privacy is violated. Current laws will be explained and a short section regarding security will look at the difficulties Rich Presence services have to face. There will also be given a section on which services that may be provided based on Rich Presence and information on how they affect public acceptance.

3 Background

In this section we define our usage of some words and expressions used throughout the text that may not be familiar to some readers. The terms are also explained in section 11, Glossary. We will also look at some laws and their usage related to Rich Presence.

3.1 Definitions

Before discussing ethical issues with regard to Rich Presence some definitions need to be established. We will in this chapter give our definition of the terms *location*, *presence* and *Rich Presence* based on material found on the subject.

Location

Location based service (LBS) has been around for some time and different services has been developed by service providers. These services are always based on location coordinates and may provide personalized and location-specific information to users¹. It can also provide positioning of other objects such as trucks for a shipping company or containers to keep track of deliveries. Location-specific information will often answer questions like “where is the nearest restaurant”. These locations are often referred to as point-of-interest (POI).

Location includes these concepts:

- Geographical coordinates (often given by a mobile device)
- Proximity to POI

Presence

Presence is defined as the willingness and ability of a user to communicate with other users on a network. Historically, presence has been limited to "on-line" and "off-line" indicators; the notion of presence here is broader.² It is a term that tries to expand on the notion of location. Presence services “involves the exchange of user-level state information to facilitate communication”.³ Presence includes *location*, but expands to also include information about the state of the user. Presence is therefore more tightly connected to a person and not necessarily to a position.

Presence includes the following concepts:

- Location
- User-level State Information
 - Availability

¹ [1W] <http://www.mobileinfo.com/LocationBasedServices/index.htm>

² [12W] <http://www.ietf.org/rfc/rfc3856.txt>

³ [1B] Ben Teitelbaum, *Connectivity Middleware for Voice and Integrated Communications*

- Activity
- Mood

Rich Presence

Rich Presence expands the notion of *presence* even further.⁴ It is presence information from several sources combined to provide a richer set of automatically updated presence attributes combined. Users of such a system must also be able to “express and install policies that determine what information about them is published to different classes of watchers”^{3,5}.

Must include:

- Presence
- User defined information policies

And may include one or more of the following

- Personal information
- Device type
- Degree of privacy
- Context
 - Based on location
 - Derived from time
 - Based on surroundings
 - Based on history
 - Current role
 - User defined
 - Aggregated from other data
- Calendar events
- Status
- Personal MotD (Message of the Day)
- Present company
- Timeliness of data
- Time of day at user’s location
- History of the above
- Full control over which of the above attributes are shared with others

Should not include

- Strictly personal information such as
 - Economical situation

⁴ [11W] <http://www.ietf.org/rfc/rfc4480.txt>

⁵ [6B] J. Jachner, S. Petrack, E. Darmois, T. Ozugur, “*Rich Presence: A New User Communications Experience*”, Alcatel Telecommunications Review - 1st Quarter 2005

- Criminal record
- Medical history
- Personal history
- Social contacts
- Social Services information
- Any information that breaches *Personopplysningsloven*, see, 3.3.

The Rich Presence System

Thus, combining all the features mentioned for Rich Presence in the Definitions section, we get a quite powerful and flexible system for networking and keeping in touch. It will function on portable devices, making the device (thereby, yourself) traceable to all your friends/watchers. They will be able to retrieve your personal profile or parts of it, according to the access level you grant each watcher. As a part of the granting of access-level, users can segment their watchers into appropriate groups, giving them different privileges. When you are in social gatherings, watchers can see where you are and who you are with, provided of course that the individuals being located have approved this. Schedules and calendars can be shared, enabling users to be notified about and invited to events and happenings where their calendar allows for it. Since this system is able to share a great deal of information, we assume that the initial restrictions on sharing are stringent. Furthermore, the Rich Presence features available through this system, can serve as a fundament for other services. These can be provided by third-party actors using the platform CPA⁶. Such potential services will be mentioned in section 4.2.

These types of systems are perhaps symptomatic of a generation much more accustomed to sharing personal information and being more social. Even though people are using technology more and more as their means of communicating, some may feel this is removing the human touch out of the equation. Perhaps the natural compensation to this is the ability and willingness to share more information and share it to a larger group of people through the use of such a Rich Presence System.

3.2 Difference of opinion

The concept of Rich Presence is relatively new and there are different opinions as to a precise definition. RFC 4480 defines a set of identifiers as a proposal for a future system for distributing Rich Presence information.⁷ However, it also proposes means of introducing additional identifiers. The technical side of this will not be discussed in this paper. As this is fairly uncharted territory, there is a lack of a precise and general definition.

3.3 Laws and jurisdiction regarding Rich Presence

As previously mentioned, one of the main purposes of Rich Presence and LBS is to provide information about where the owner of the mobile device is and what his status is.

⁶ [9W] <http://cpa.telenor.no/cpa/>

⁷ [11W] <http://www.ietf.org/rfc/rfc4480.txt>

This kind of information is connected to individuals and is therefore considered as personal information⁸. The usage of this information is subject to the Norwegian law *personopplysningsloven*, and gives restrictions about how long it can be stored and if it can be sold to a third party. A third party might be other companies providing services within mobile communications.

The purpose of "Personopplysningsloven"⁹ is to prevent violation of personal information protection and to protect the individual from being exploited by the usage of personal information.

It gives clear definitions on what personal information comprises. This is defined in § 2 and includes information such as:

- Information which can be connected to an individual
- Treatment of personal info; collection, distribution or combination.
- Personal registers
- Sensitive information;
 - racial/ethnic background, political, philosophical or religious beliefs
 - criminal records
 - medical records
 - sexual relationships
 - union memberships

According to § 11, one cannot make use of this kind of information, unless one has prior consent from the individual. This is further specified concerning personal information in § 8 and concerning sensitive information in § 9. Both sections contain terms for when it is allowed for someone to use this info.

Personal information can thereby only be used when:

- the conditions in § 8 and 9 are fulfilled
- there exist justifiable purposes for the usage of this info by an enterprise
- the info is not to be used later in a context which is not affiliated with the original purpose
- the info is adequate and relevant as well as correct and updated and will not be stored for longer than necessary

In contrast to the above mentioned laws, which of course only apply to Norway, the US legislation is rather different. In the US, it is the company that owns the information which it gathers about you. This includes businesses, researchers and credit agencies.¹⁰ The companies can then sell this information to others, which is a huge market in the USA.

The Norwegian institution "Datatilsynet" has given strict regulations to the mobile companies and has secured that they gather consent from their subscribers before they are

⁸ [4W] http://www.datatilsynet.no/templates/article_1523.aspx

⁹ [5W] <http://www.lovdata.no/all/tl-20000414-031-001.html>

¹⁰ [6W] http://news.com.com/2030-1069_3-5068504.html

able to collect information about them.¹¹ The subscribers are then able to agree to that their mobile device is also used as a tracking device, and if personal information is to be divulged to other commercial institutions.

In this context, we must mention the e-privacy Directive 2002/58/EC as defined by the European Commission (EC).¹² Concerning the acquisition of consent from the user, the Directive 95/46/EC – Article 2, defines:

«For the purposes of this Directive 'The data subject's consent' shall mean any freely given, specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed».

The term 'freely given' is further specified as; consent is given when it is neither to the advantage of a counterpart nor the subject of negotiation on behalf of the data controller. This consent is given for a specific and identified location-based service, and it cannot be a general consent of being localized. This information to the user needs to be understandable and accepted by him/her before the collection of data can commence. We thereby see that the laws of the EC and Datatilsynet strongly correlate concerning the obtainment of consent from its users.

Article 9 of the 2002/58/EC directive states that processing of personal data may only occur when it is anonymous, with consent of the users, to the extent and for the duration necessary and with the purpose of added service.

It further states that information regarding the following must be sent to the user:

- Location data other than traffic data, which is going to be processed
- Purposes and duration of the processing
- Whether data will be given to a third party for the purpose of added service

The directive 95/46/EC states that a user must be informed of:

- The identity of the controller (the one processing information about you) and of his representative (firm or organization)
- The purposes of the processing
- The recipients or categories of recipients of the data
- The existence of the right to access to and the right to edit/rectify data concerning the user

The possibility to withdraw their consent is of course also present for the users, and is defined once again in Article 9 of 2002/58/EC:

«Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.»

We can thereby conclude that Datatilsynet and the EC have very much the same legislation concerning the processing of personal information.

¹¹ [7W] http://www.datatilsynet.no/templates/Page_874.aspx

¹² [7B] Mathias MOULIN. *Location-based services and the e-privacy Directive 2002/58/EC*.

Code of Fair Information Practices (CFIP)¹³

In the 1970s, the U.S. Department of Health, Education and Welfare, issued out the following code to protect personal information from abuse. Although this code has not been passed as a law in the US, it has inspired national privacy policies around the world. During the rise of internet-based organizations, this code influenced the establishment of privacy policies and has given important guidelines to information-gathering organizations. Today, the following four practices or a combination of them, are widely used concerning privacy on the Internet.

1. Notice – Organizations collecting personal data must disclose their collection practices beforehand.
2. Choice – People must have an opportunity to either deny or give prior consent to divulging personal information.
3. Access – People must be able to view the information stored about them, learn how it is used, and have access to editing it.
4. Security – organizations collecting, maintaining, using and releasing personal information must prevent the misuse of such data and ensure that the data is only used for reliable purposes.

“Personopplysningsloven” thereby contains many of the same aspects concerning privacy, like prior consent, preventing misuse and notification of selling to other organizations. The directives of EC also concur with this code when it comes to all the practices.

¹³ [14W] http://firstmonday.org/issues/issue5_9/sholtz/index.html

4 Services

This section emphasizes on potential services, what could, should and must be included as well as our glance at a best-case scenario.

4.1 Pitfalls

At first glance, the potentially worst thing that could happen to this kind of system is if people feel their privacy has been invaded. This includes the reselling of a lot of the aggregated information, as this can both be annoying and dangerous. Annoying, as commercial actors can find out where you are and how inclined you are to have seen their product or shop previously. Dangerous as potentially hostile persons may see where you are and what you usually do each day. This ranges from finding your home and work address as well as your daily routines to knowing when you are in meetings, with whom you're with and what you do at that meeting.

As easily seen, if trust is not maintained between the user and the system, mentioned in section 3.1, few or none will use it. Another key aspect will be the ease of use, as this most likely will be used by people in all ages and with different background. The thing that we see as crucial is how little time is spent on actually setting your status, company etc. If this time is anywhere near as long as the time wasted had it not been set, people will find it a hassle. If you for each meeting you attend, all attendants start by setting their status to busy, specifying company, etc. in order to satisfy all the information required by the system, so much time is wasted that it is unlikely it'll ever be used.

Third-party commercial actors will always be on the lookout for new ways of getting information about potential customers. With a system that could provide them with location, mood, company and more they could get a powerful marketing tool in the way that they can direct adverts to certain groups. If users got an SMS with a marketing offer from a store in their vicinity if they had status set to "Shopping", this could be a cheap and effective tool to increase sales. In the same way, a grocery shop may give you a suggestion for dinner shopping with special offers, sent to you right before you usually leave work. The possibilities are endless, and the marketing can be homed much better than mass-sending of advertising leaflets or the recent pain for all users of e-mail, so-called spam. The problem with this is that users may feel dismay knowing that information about you is given away or sold by their provider, as this may breach the delicate trust between user and provider. Therefore, it is vital, if information is to be sold, given away or published, that users are informed and that they easily could disable this. As an addition, even though users are obliged to read agreements, most will probably not read all the fine print on an end-user agreement. This call for making a very clear point of the provider's policy on many important points, including what information can be published or sold.

Once trust and ease of use is established, a broad implementation is indeed possible. What needs to be in focus then is how the system is best used.

4.2 Potential services

- Location-aware services such as¹⁴
 - Destination guides that adjusts after the user's current location
 - Friend finder, to locate nearby friends
 - Taxi finder, call a taxi service and the call will be forwarded to the closest available taxi
 - Real-time routing assistance that adapts to your current heading and speed
 - Yellow-pages search that can sort results based on user's location
 - Power saving by turning off for instance central heating, lighting and/or other appliances in a house if no one is present.
 - Traffic guiding based on which roads are congested
 - Emergency services that precisely locates devices for quick response
 - POI finder for tourists that can be connected to an interactive tour guide
- IM or SIP-like presence services
 - Status such as busy, on the phone or eating
 - Means of communication, voice, voice + video, plaintext
 - Message of the day or personal message, blog updates
- Presence and Rich Presence aware services such as
 - Presence changer, if a user's scheduler specifies a time and date for a meeting, within that timeslot all calls will be sent to voicemail and callers will be given information on next time the user is probable to be available.
 - Company identifier, to identify another user's current company and relations
 - Advertising services that can identify potential customers based on status, mood and location
 - Alumni services that can keep track of personal networks
 - Privacy reservation, based on either person filtering or schedule filtering
 - Credit or payment services based on personal identification from mobile device.
 - Buddy Driving, where friends sharing their route to work may find each other and drive together.
 - Sphere definitions, stating that a user is *home* or *at work*, but not giving geological positions, and varying other user's access levels accordingly
- User pattern analysis
 - Fastest route based on empirical patterns
 - Hot-spots in urban environments
 - Automatic status updater based on user patterns
- Group and collaborative services
 - Services that can set up a phone meeting when both or all parts are available
 - Check team mates' schedules
 - Event planning and sharing
 - Meeting and collaboration organizer

¹⁴ [9B] Dr. Robert P. Minch. *Privacy Issues in Location-Aware Mobile Devices*. IEEE 2004

4.3 Existing services

Some service offerings already provide some of these points. For instance, buddy-services have existed for some time, although with limited success. These have largely been based on GSM location. Also, a lot of programs enable their users to set different statuses for when they are busy, eating and so forth. Scheduling programs, both online and offline have widespread use and many rely on them to keep order of their meetings. Further, service providers such as Telenor already keep history over users and their calls and movements; this has currently not been used to any extent to provide services to the general public.

4.4 Best-case Scenario services

In this scenario, we presume that a Rich Presence service has been widely implemented and used. We then look at how and which services help users in their daily lives in a best-case scenario. Services mentioned here may not yet or may never exist, however we see them as possible candidates to include in a Rich Presence service.

All mobile devices make use of a Rich Presence service. There are no complications regarding compatibility or cross-platform use of the system. The user may freely choose whom to trust with which pieces of information, and the system can detect and stop any attempt to gain access to information one is not entitled to. The base of the system is a person's personal calendar, where one can specify time and date for meetings, work, dinner meetings and the like, and your status and privacy is set by this. If specified by the user, selected individuals may see the current location of the user; however in the case of a "privacy" option being set, either manually or automatically because of i.e. a calendar event, some or all contacts may only see this person as in a general area, city or country, or may not receive any location at all.

If trust and access has been gained, the system may show Rich Presence information such as a person's precise location, present company, relation between the person and the company, the person's role, whether and how he/she can be reached and what the person is doing, according their calendar. It may also have the ability to show the timeliness of this data, i.e. how old this data is and how long the person is expected to be in the same setting.

History of this data is also kept in order to generate patterns of use so that the system may automatically find out information such as preferred means of transport to work. This may include both choice of route, time of day and whether or not you are traveling alone, in a car pool or with public transport. Users may also do a lookup in the system to see if any friends are heading the same way they are, in order to share car or meet on a train.

All this information, both real-time and historical data, may be collected from all the users, with their approval. This can be used to generate reports on location of traffic jams or popular sites, or it may be used for monitoring public buildings to turn down central heating if nobody is present.

Users should be able to easily change status, little or no effort should be needed for this system to properly work. This requires a high degree of integration with other applications such as an online personal scheduler, map services to tell what kind of place you're in and other services like traffic monitoring or providers of electricity to provide other services.

5 Ethical and social issues

The society we live in grows smaller, people get more and more connected and the information flows. And while people have an interest in preserving their privacy, they are also interested in for example disclosing sufficient information to colleagues to facilitate smoother communication and enable the job they need to do¹⁵, or to minimize cell phone interruptions¹⁶.

5.1 Privacy preferences and sharing patterns in context-aware telephony

Khalil and Connelly did an in-situ study of people's privacy preferences and patterns of sharing different types of context information with different social relations. During the study, they gave each of the participants a PDA. Throughout the day, every participant received inquiries prompting her to choose what context she would like to disclose to a potential caller. Participants were asked to assume the role of the receivers of a cell phone call. The caller assumed one randomly chosen role out of the 6 social relations; *significant other, family member, friend, colleague, boss and unknown*. In addition to

inquiring about participants' willingness to disclose different types of context information, every questionnaire included a list of questions about the current location, activity, number of surrounding people, and the social relationship to the surrounding people, as well as the participant's availability under those circumstances to receive a phone call from that particular caller¹⁶.

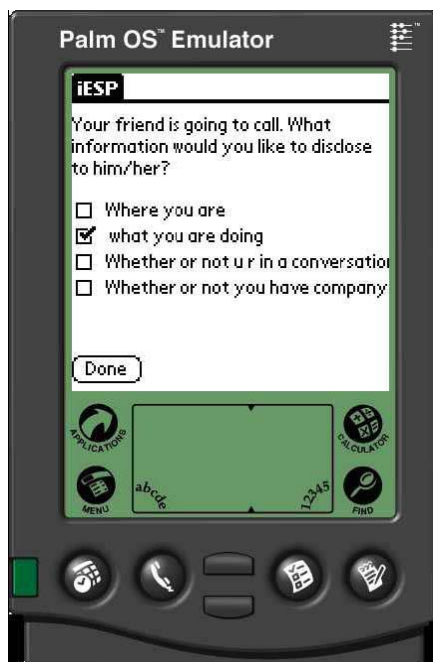


Fig. 1, PDA used in study, from [11B]

Context disclosure rates

The results from this study showed that all the information, location, company and conversation, were revealed 41 % of the time. More specific, company information was disclosed in 74.3% of the situations, conversation in 69.4%, location in 47.4% and activity in 46.4%. This suggests that Location and activity trigger lower privacy comfort levels, while company and conversation triggers higher levels of privacy comfort. This

seems sensible, taken into account that in learning the activity or location of a close friend automatically conveys substantial information about the friends' company and

¹⁵ [10B] Patil and Lai. *Who Gets to Know What When: Configuring Privacy Permissions in an Awareness Application*. 2005.

¹⁶ [11B] Khalil and Connelly. *Context-aware Telephony: Privacy Preferences and Sharing Patterns*. 2006.

conversation status. For example, finding out that a friend is at a movie theatre indirectly suggests with high probability that she has company and is not engaged in a conversation. However, this ability to infer information does not work reciprocally, i.e., knowing Company or Conversation status does not generally lend information about Location and Activity¹⁷.

Context disclosure and social relations

Khalil and Connelly also found that the availability rate not only depended on context of the receiver, but also on social relation. In fact, social relation was found to be one of the things that weighted most, when the participants were asked at the end of each questionnaire whether it was an appropriate time for the caller to call. The availability rate were highest for *significant others* (75%), followed by *friends* (68%), *family members* (63%), *boss* (50%), *colleagues* (47%) and *unknown* (39%). The average availability over all different social relations and for all participants is around 57%. This high rate of unwanted incoming calls stresses the importance and the need for solutions to minimize cell phone interruptions. It is worth mentioning that the rate for inappropriately received calls may be lower in real life than the one obtained from the study by Khalil and Connelly due to the familiarity of friends, family members, and significant others with the work pattern of the receiver. However, these results imply that designers of context-aware telephony applications also should take into consideration the social relation between parties in addition to the receivers' context¹⁶.

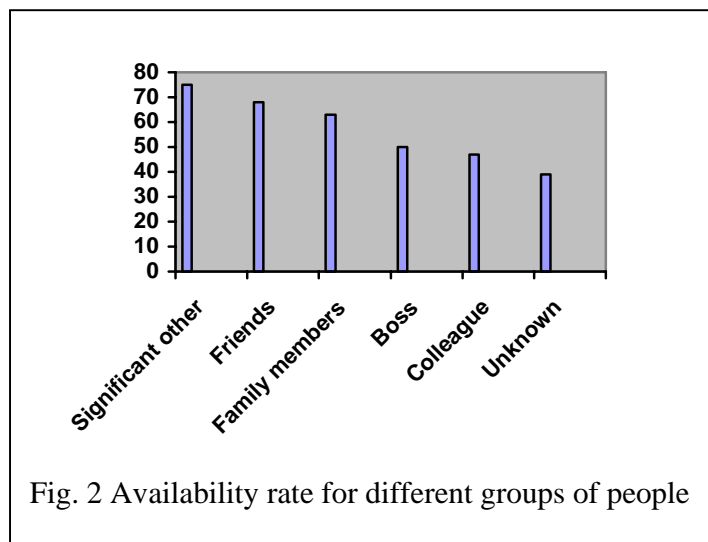


Fig. 2 Availability rate for different groups of people

Grouping of social relations

Social relationship between the caller and the receiver seems to be a major factor when people decide what context to disclose. Khalil and Connelly found 3 clusters with distinct sharing patterns, one cluster with Significant others, family and friends, another one with unknown callers and one with Boss and Colleagues. The first cluster was the one which the participants most willingly shared context information with, seeming reasonable since *friends*, *family* and *significant others* are the one that people usually thrust most. *Boss* and *colleagues* comprised the medium sharing group, seeming logically since sharing with this group often is based on an as-needed basis. The last cluster, consisting of unknown callers, was the group whom people shared least information¹⁷. These results are in agreement with Olson, who obtained similar results investigating patterns of 40 different types of personal information¹⁸.

¹⁷ [11B] Khalil and Connelly. *Context-aware Telephony: Privacy Preferences and Sharing Patterns*. 2006.

¹⁸ [12B] Olson et. al. *A study of preferences for sharing and privacy*. 2005.

The interest for such a system

Khalil and Connelly also found in the end-of-study interview that 70 % of the participants in their study were willing to use a service that publishes their context information comparable to the one used in their study, if their cell phones were equipped with it and if they were provided with a tool to manage their privacy preferences. And when asked how useful they found the system, 55% rated it 4, 30% rated it 3, 10% rated it 2, and 5 % rated it 1. The scale went from 1 to 5, 5 being most useful¹⁹.

5.2 mySpace and privacy permissions

mySpace²⁰ (see Figure 3) is a browser-based interactive visualization of a user's physical workplace that provides dynamically updated information about people, places and equipment. Users maintain a list of contacts (or "buddies" in IM terminology). For each contact, there is an associated set of permissions granted to the user by that contact. For

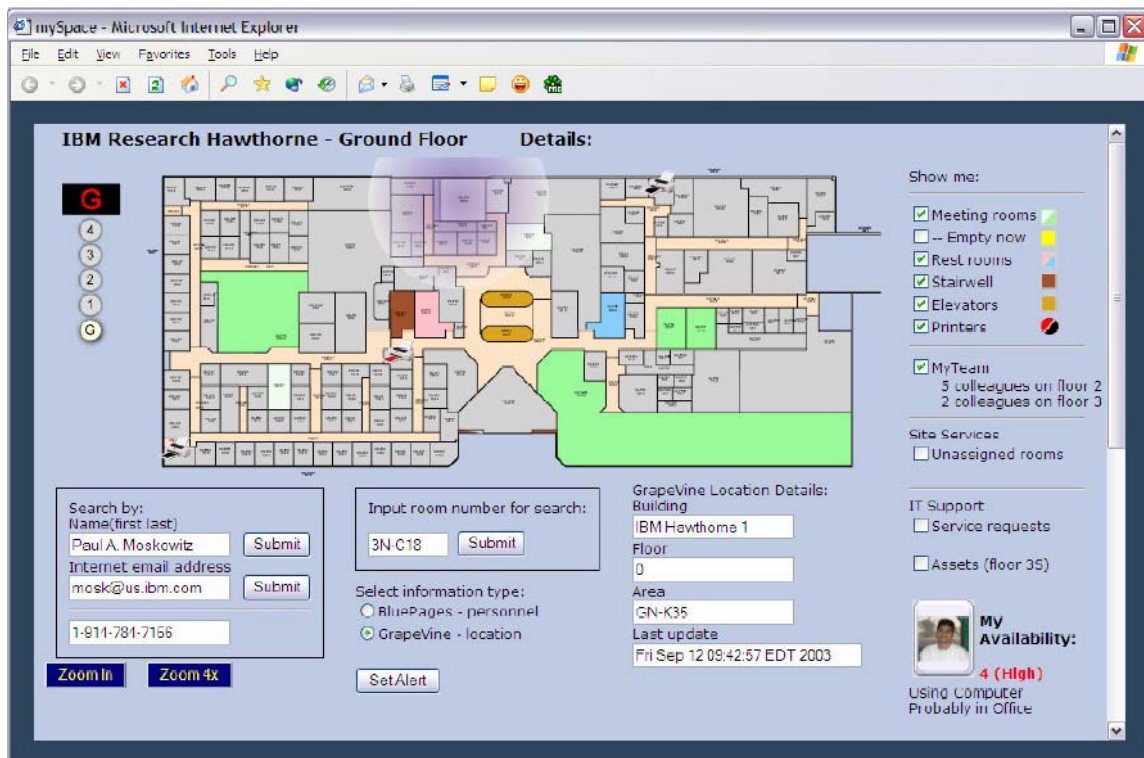


Fig. 3, Map from mySpace application, from [10B]

example, if Sally has Paul in her team list, Sally will be able to view whatever information Paul has granted her permission for. Possible permissions include whether Paul's phone is off the hook, the location of the wireless access point that his laptop is

¹⁹ [11B] A. Khalil and K. Connelly. *Context-aware Telephony: Privacy Preferences and Sharing Patterns*. 2006.

²⁰ Note: This is not the social networking site www.myspace.com, this is a test application developed by IBM. See ¹⁹

connected to at work, whether he is connected remotely (if not in the building), which application he is currently using, and his IM activity. Additionally, a badge-based location tracking system is in the pipeline. Paul can choose whether to allow Sally to view all system-known information about him, or just a subset²¹.

mySpace allows users to view the location of fixed resources (e.g. conference rooms, printers), mobile equipment (e.g. laptops) and to interact with them. For example, once a user has located the closest printer to his or her current location, clicking on the printer will take him or her to the web page for setting up that particular printer. Clicking on an unoccupied conference room connects the user to the reservation page for that room, and clicking on a colleague will bring up that person's e-card (see Figure 4). An e-card is a means of initiating one-click communication¹⁶.

Findings

In their study, Patil and Lai investigated how people configured privacy settings in order to inform appropriate default settings for mySpace. A majority of participants (~ 70%) chose to configure permissions in the "Groups" mode. Permissions granted to various groups were significantly different from each other. Location was the most sensitive aspect of awareness. However, participants were comfortable disclosing it to colleagues on their team while at work during business hours. More privacy was desired after business hours – even in a company with a culture of flexible work hours and occasional telecommuting. Contrary to expectations, explicit upfront disclosure of all pieces of personal context to which the system has access, did not seem to induce more privacy preserving settings.

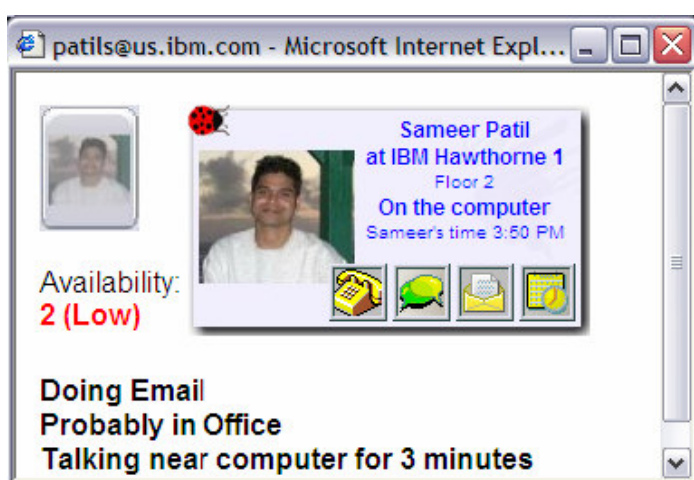


Fig. 4, User view from mySpace application, from [10B]

Contrary to expectations, explicit upfront disclosure of all pieces of personal context to which the system has access, did not seem to induce more privacy preserving settings.

Preference for groups

Participant feedback indicates that the preference for groups was driven primarily by providing enough flexibility for controlling access to personal information, without requiring too much burden to set up and configure. Participants indicated

that *Global* and *Team* modes weren't flexible enough, while *Individuals* mode required configuring more details than necessary. They also mentioned that, if necessary, a group with only one individual could be created. Many of those who chose groups indicated that they organized their IM contact list into groups as well. However, even participants who did not group their IM contacts selected groups mode of configuration because of

²¹ [10B] S. Patil and J. Lai. *Who Gets to Know What When: Configuring Privacy Permissions in an Awareness Application*. 2005.

the greater sensitivity of the information involved in mySpace. Majority (15) of the 25 participants who chose groups created 4 groups. The rest specified between 2 to 5 groups. In actual use, without the burden of having to specify all groups at once, the number of groups created would probably be slightly higher than in the study. Patil and Lai found a lot of commonality among group definitions. Typically, specified groups exhibited a concentric circle pattern with less and less awareness being shared as one moved away from the center. In some cases the center was *family* and in others it was *team*^{Error!}
Bookmark not defined.

Paired-samples t-tests for comparison of mean permissions for family and team were not statistically significant. The only exception was location information when working from home. Participants were willing to share with team members that they were at home (i.e. building-level information) but not information at the floor or room level²².

Permission for business and non-business hours

As expected, Patil and Lai found that more privacy is desired during non-business hours – both at work and at home (with the exception of family). Compared to the corresponding permissions for business hours, all groups (except family) received lower sharing during non-business hours – regardless of the user's location. They also found that sharing for team members, collaborators, and managers decreased significantly during non-business hours. Identical patterns were seen for the other aspects of awareness²².

5.3 When privacy is invaded

What one feels as invasion of privacy varies from one individual to another. This section tries to look at different situations that lead to privacy issues related to Rich Presence.

Mismatch between assumptions made by designers and users

When designing a new service which includes personal information one needs to establish a privacy model for how this information should be handled. According to Adams and Sasse²³, "most invasion of privacy occurs when users realize that a mismatch has occurred between their perceptions and reality." This mismatch can be due to a weak model that fails to take every possibility into account or faulty model which do not satisfy users need for privacy.

The policy enforced by the privacy model has to be communicated to the users. Several factors are involved:

- Informed policy
- Implicit assumptions made by users

²² [10B] Patil and Lai. *Who Gets to Know What When: Configuring Privacy Permissions in an Awareness Application*. 2005.

²³ [2B] Anne Adams & Martina Angela Sasse. *Privacy in Multimedia Communications: Protecting Users, Not Just Data*

- Implicit assumptions made by designers

Informed policy communicates to the user how the sensitive information will be used. This builds a mental model of how the privacy model enforces policy. Most users do not go to great length to understand informed policy in every situation²³. This is especially so when they are dealing with organizations in which they have a great degree of trust. Instead they make implicit assumptions about how the system works.

If there is a mismatch between the real model and users mental model this often leads to situations where users feel their privacy has been invaded. The privacy model may have to be re-evaluated if the mismatch is between informed policy or implicit assumptions made by designers and the mental model of the user. Since invasion is felt by the user, his assumptions must be given the most weight.

Putting sensitive information to new use

How sensitive information is depends strongly on the context in which it is used. Situations where personal information is put to new use often leads to privacy issues. To use existing information in a new service, a re-evaluation of the privacy model is necessary to confirm that sensitive information is handled correctly. Also a new confirmation from the user may be required. If these measures are not taken, users might react very strongly against it.

Unintentional privacy invasion

Leakage of sensitive personal information occurs when individuals gain access to more information than was intended. This is often due to insecure databases or human errors when handling personal and possibly sensitive information. 2006 has been a especially bad year for such information leakage in the US as stated on security focus²⁴. This has led to new laws where businesses have to report to central authorities when and if personal information is leaked. A list of these can be found at Privacy Rights Clearinghouse²⁵. A total amount of 104 million records have been recorded as leaked since 2004. These information leakages are clearly a privacy issue, and leaked information has been used in identity thefts and fraud.

5.4 Security

This report does not focus specifically on security, but some of the issues do deserve some attention. This section will look at some of the issues regarding abuse of Rich Presence services.

²⁴ [2W] <http://www.securityfocus.com/news/11429/2>

²⁵ [3W] <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

Misuse

Misuse is when the service is used in a way not intended by its designers. This can be both legal activities not considered in the design phase or exploitation of security risks in the system.

Legal use

Examples of misuse within the system's legal boundaries may be the observation of historical data gathered over time. This can be automated by a job fetching information and storing for later use. Statistical analysis can be used to look for patterns in the data and fairly accurate assumptions about the future can be made. Roger Clarke looks at issues where location tracking is used to match behavior against predetermined patterns to enable a range of unwanted possibilities²⁶. These "attacks" are very hard to protect against as each request are not considered harmful until aggregated over time.

Illegal use

One could argue that no information is safe from hackers as there is always a way to get to the data if it is stored electronically. Kevin Mitnick claims that all internal databases can be accessed given enough time and resources and shows how this can be done²⁷. Therefore one concludes that system security on a Presence Service is not as important. But the fact that information is more available through a provided service also means it is more available for hackers. According to The Honeynet Project²⁸ there are at least four types of hackers. The first two hack for fun or money. These are normally not interested in going to jail for what they are doing and do not have a lot of resources. Then there's government and industrial spies hacking and terrorist doing hacking. These groups have less moral issues, more resources and are willing to go further. All four groups are important to protect against and different tactics has to be used.

If an attacker gains unauthorized access to the raw data he can usually do what ever he wants with it. Usage range from:

- Identity theft
- Extortion
- Information trading
- Fraud

We will look more into the consequences of such attack later, but protection from illegal use should be taken into consideration when creating Presence Services. The information stored is highly sensitive and can be dangerous in the wrong hands.

²⁶ [3B] Roger Clarke. *Person location and person tracking. Technologies, risks and policy implications.*

²⁷ [4B] Kevin Mitnick. *The Art of Deception: Controlling the Human Element of Security*, 2002.

²⁸ [5B] B. Carrier et al. *Know your enemy: Revealing the security tools, tactics and motivation of the black hat community*, 2004

System integrity

For Rich Presence services to work the data have to be maintained so that the integrity is intact. Broken integrity comes from wrong input to the system or malicious changes made by an attacker. This will result in the service giving out information that is not up to date with reality.

System integrity can be compromised in a number of ways:

- Fooling the system
- Breaking the system
- Outdated status

Fooling the system can be done by simple giving the system wrong data. By turning off a tracking device at the right time or simple leaving it at home, a user of the system can fool it to assume the wrong conclusions. For instance the system can assume that you are sick and take a day off since the mobile device has never left the bed stand.

If the system is broken then the data integrity is compromised on a whole other level. Now one cannot trust the historical information stored in the system as it may have been tampered with. To restore system integrity one would now have to restore the raw data from backup or use some other means of consistency checking.

Trust

For the service to be useful people must be able to trust the information they receive. This comes from system integrity. If the information is just outdated then users will be annoyed. More seriously if system integrity is lost due to a security breach then not only will the users doubt the information it provides, but they will also wonder if their personal information is safe, and perhaps stop using the system altogether.

Building trust is very difficult as people always are a little suspicious about new technology. Even worse is regaining trust after it has been lost. The users needs to know that the information about them is secure for a presence service to be successful.

Consequences

As stated before there are many personal attacks based on Rich Presence information. Most would perhaps not consider this information to be dangerous or even sensitive, but the fact remains that a lot of your habits can be derived from this data. Also, the information gathering can be done automatically on a large number of users.

This means that a breach in security might have quit large consequences for the users and should be taken seriously. This has to be done by the system owners and designers as users often are not careful enough with their own personal information and what they share with whom.

6 Interview

We performed two interviews with two representatives from other generations than our own. We feel that the views of the older generations have a greater deal to say for public acceptance, than those of the younger one. We therefore made a conscious decision to leave out the typical teenager and concentrate on the views of older, and perhaps more critical people.

6.1 Background

In this interview we hope to find statements that can support our theories, however, we choose subjects that differ from the participants in our group on many levels. Our subjects have different age, education, technical experience and social background than ourselves. The motivation for this is to see if these subjects have a substantially different view of things or if they agree with our views. We therefore take precautions not to reveal our own opinions in advance in order not to bias them.

As we choose only two subjects this will be a qualitative interview, not a quantitative. We hope to get in-depth answers to our questions which we can draw conclusions from. If the answers to some degree agree with our own opinions, we feel that these opinions are representative for a greater part of the population than just the five of us. Because of this we focused on *how* and *why*, instead of *when*, *what* and *where*-questions. If the opinions differ from our own, we know that the conclusions and thoughts in this report may only be partially valid or only valid for a part of the population.

We chose our subjects on behalf of their age, sex and area of work. Our first subject is a lot older than we are and therefore may see things from a different angle than we do, both because of usage pattern of phone and modern computer software, and because he did not grow up with mobile technology the same way as we did. Our second subject was chosen in some part because of her age, but also her sex. Men and women have different usage patterns²⁹, and it is therefore important in a qualitative setting to investigate the difference.

We will after the interviews attempt to draw conclusions based on what our subjects' opinions. Because of the small sample size it is vital to get as much and as general as possible from both our subjects.

6.2 Interview: Bjørn Kristian Indergaard

Our first subject was Bjørn Kristian Indergaard who is a 60 year old lecturer at NTNU, Dragvoll. He was selected to represent the views of an entirely different generation than ours. Nevertheless, we hoped that he would provide us with statements we could use to strengthen our theories. We started out by probing into how much he used his phone and what knowledge he had about different services. Then we moved over to the core of our interview, asking about what kind of information he would share, and what kind of

²⁹[13W] http://socio.ch/mobile/t_geser3.htm.

incentive would be necessary for sharing to happen. After this, we moved into the area of usefulness regarding specific information and services. After this followed questions about options within such services, and questions regarding the storage of personal information by Telenor.

How often do you use your mobile phone?

We started out by asking how often he used his phone, and he answered that he rarely uses it to call other people, but other people call him. He does not have a close connection to his phone. He humorously added that he mostly uses it to answer other people and communicate his own grievances and annoyances concerning things he is preoccupied with.

Are you familiar with Instant Messaging software (MSN, Skype)?

We proceeded by asking if he had ever heard about Instant Messaging-software, like MSN or Skype. He had heard about MSN and seen it in magazines, but he didn't quite know what it was. He assumed it was something which included not only messaging but also images. The internet-telephony software Skype had he only just heard of a couple of days ago. He has a son who lives in England and he heard from him that they were able to communicate through Skype for no charge. He wouldn't mind having Skype, just to save the money, but he feels that he is bound by tradition and therefore doesn't bother downloading and learning to use this application.

Have you heard about Buddy (Netcom) or Kompis (Telenor)

He had not heard about the «Buddy» and «Kompis»-services of Netcom and Telenor respectively. We then explained that these services provided location-based information, and he felt that sharing this kind of information was a bit scary.

What kind of information would you share with your friends?

This led us into the big questions of our interview, namely those concerning sharing of location, status, company and the other aspects of Rich Presence. Questions like «Where are you?», «What are you doing?», «What is your status?» and «Who are you with?» are the archetypal questions which Rich Presence aims to answer. We asked him what he thought about such services and sharing of information at this level. He said he was not at all comfortable with sharing information about himself regarding location, not even with his close friends. We then presented him with the option of turning off the sharing, and we perceived him as less skeptic, although he still was under the impression that people could get this information if they wanted. His main issue of concern was that of security. He explained at this point that he felt that the sharing of this kind of information was to cross an important boundary, and he repeated his discomfort with this kind of sharing.

Instead of functionality like automatical answer depending on context(if he for instance is in a meeting, the caller will see this), his first thought was that he would prefer that people just don't get an answer and have to try again later. He saw it as too much hassle to have set the status at every occasion. After dwelling on this a few moments, he came around and admitted that it could be useful in certain cases. This would be for example if he was waiting for an important call, he could filter out the «non-important» ones and tell

them to wait for one hour and try again, and just let the important one through. He only saw the potential for this service at work though, not in his spare time. This must be able to switch off.

Regarding Rich Presence, which also includes the possibility to give out information about whom you are with at the moment, he considers it to be uninteresting to him. He does not wish to provide this info to anyone, and claims this is probably a difference of generation.

When we ask him about sharing his calendar, he says he would not wish this either. He would rather that people call him and make an appointment personally. Your calendar should be your own business. However, he saw the advantages of sharing his work-calendar with his colleagues, so he was willing to accept some of the presence-features to a certain degree. If it were his closest family, they could also be given some further privileges regarding calendar. He displayed some skepticism around this subject, but less if he was able to control privileges to certain people. He distinctly preferred the old-fashioned way of doing this, by calling people instead of having an insight into his contacts' calendar. He basically didn't feel that this technology solves any problems, but he understood that it would be used if available, because technology creates needs.

What kind of incentive would make you use these services?

As we can understand from the above, this man is skeptical to innovations of this kind, where sharing a great deal about yourself is possible just by hitting a few keys on your phone. We wanted to find out what it would take for him to use the technology, what kind of incentive would make him become interested? First of all, he stated that the system had to be 100% secure, and an option of different access for different users. The entry level of use would also need to be low, because many people in his age perceive new systems as hard to learn and difficult to get acquainted with. Even though he claims to have some insight, he still doesn't have enough knowledge or the energy to actively search for these services. The service should therefore be easy to operate, with a manual written by an idiot, as he wittily put it himself. As a final point he mentioned that over who you let into your personal sphere should be up to you from the very beginning. In more technical terms, it should have strict default settings where you permit access for specific users whilst others aren't allowed, and not the opposite situation where you have to block everybody you don't want to allow.

Which information would you see as useful to know about others?

We asked him who he might be interested in receiving Rich Presence information about his boss, colleagues or children. He would certainly not want to receive info about his colleagues, neither his boss. A few moments later, he admitted that maybe he would like to know where his boss was, just so he could relax a bit more. Concerning his children, he might want to know where they were, at least if they were still small. It would be okay if they still were at an age where they felt they didn't want to be too far away from their parents. He would feel uncomfortable if he was in the situation of being located, so he understood the potential difficulties of this.

Which services would you see as useful?

He did not display any immediate enthusiasm about traffic pattern services or heat-regulation on the condition that his location would be traceable continuously. However when we informed him that this would be totally anonymous, he was able to see the advantages. He wouldn't mind giving up some anonymous info as long as he would be notified about fastest routes or the roads with the least traffic. Heat-regulation would also be interesting, provided of course that it is possible to disconnect both of these services.

BuddyDriving was something he yet again displayed skepticism towards, claiming that this was a question of difference in age. He could see the advantages of the service, mentioning such arguments as it would be nice to have a companion if there was heavy traffic and the possibility of splitting cas costs with someone else. But he didn't have any problems with heavy traffic, so therefore no.

Is it important to be able to control who has access to which piece of information?

He would only segment his watchers into family, friends and colleagues. Within family, he would also like to differentiate between wife, children and siblings.

What do you think about Telenor storing your Rich Presence information for 3 months?

He doesn't like it, although he doesn't see the huge problem since he has nothing he wants to hide. But it is a matter of his personal life and he maintains the idea that information stored somewhere has the potential to be misused. Again the security issue arised, and he imagines flaws in the system, permitting access for hackers.

Which services do you think a third party could provide?

He would not give any info to a third party unless it was anonymous. This spread of his info, would just lead to greater risk of misuse in his opinion. He repeated services like the ones mentioned for traffic and electricity, but only when anonymous.

On another note, he mentioned that he wouldn't mind that dangerous criminals be monitored through such services.

Conclusive thoughts

He seemed very negative to begin with, but when we explained the possibilities as well as limitations that exist in the system, he was able to see a real potential in it. Still, he was very concerned about the security of his personal information, and was more preoccupied with what he was forced to give up compared to what he was able to gain from the services. He was aware that these views probably reflect those of older gentlemen.

6.3 Interview: Tone P. Næss

Our second subject was the 37-year-old Tone P. Næss, married, one child, working at one of NTNU's canteens. This subject was chosen because she differs in age, gender, education and marital status from ourselves. Women often have a different pattern of usage regarding phones than men (citation needed), and we are quite interested in seeing if this will result in different opinions than those previously presented.

How often do you use your phone?

She said her own use of mobile phones were limited, she didn't use her phone very much and didn't regard herself to be an advanced user. She used her phone mostly for calls and did not use many of the advanced features offered on today's phones.

Are you familiar with Instant Messaging software (MSN, Skype)?

Through her child she had gotten some understanding on what IM programs were, but she didn't use them herself. She had not herself seen the need to use it, but had seen how it could be used to maintain contact with people and inform others of your current status. She did not use Skype or other similar VoIP programs either, but she had heard of them.

Have you heard about Buddy (Netcom) or Kompis (Telenor)?

We asked her whether or not she had heard of Buddy or Kompis services, she said she recognized the names, but not what they offered. When we explained the details, she seemed a bit skeptical.

What kind of information would you share with your friends?

We continued and asked her what she thought of a service that monitors your position and can provide your friends with your exact position. At first glance she was a bit worried, but said it would be easier to accept if it was possible to turn the service off. This option, she said, would for her just be a safety valve, as she thought most of the time she wouldn't be bothered with turning it off, but if she at one point really didn't want anyone to see where she was it would be a necessity. She said that it was out of the question to pay to get this service.

On our question on if she would share with her friends her current activity, she clearly opposed at first. She became more positive to set her status to IM-like busy or not available. This she saw as quite practical and potentially time-saving. She also saw it fit to share with her friends her present company. If you are in a meeting that isn't confidential, people can see your state as busy, and also, since it isn't confidential, see your current company.

She said that from her work she is used to sharing many of her calendar events with her colleagues. She therefore had no problem accepting the sharing of this to her contacts. She said it would ease the work of calling people to see if they were available, and also made meeting planning easier. It would be practical in a non-professional manner as well, as she could see if her friends were on holiday, or if her sick mother had an excuse for not answering the phone.

What kind of incentive would make you use these services?

We saw that she became more susceptible to a Rich Presence service as we explained the positive sides, but she seemed a bit uncertain regarding who could access personal information. She felt the system had to be easy to use and secure, and said she did not want to pay much, and it had to be optional. She also said she wanted to feel she had

control over all the information she was giving away, so that only those she felt comfortable with knowing her personal information got access to this.

Which services would you see as useful?

We described a system with traffic monitoring that could identify for instance your route to work and give you an alternative route with less queues. She said that she herself had no need for this as she lived in walking distance to work, but said that she saw how it would be practical for those driving to work in rush hours. We then described a power-saving system that turned down central heating if no one has at home or a system that started heating up the cabin half-an-hour before their predicted arrival. She embraced these services, saying they were genius and gave her a reason to get a cabin. The buddy-driving system we described for her fell a bit short of her enthusiasm, mostly because she had no need for this herself as she walked to work.

Is it important to be able to control who has access to which piece of information?

She seemed very aware of what information she wanted to share with what people, so we asked her to describe what kind of grouping of people she would like to use. Her thoughts were to divide into closest family, her handball team, colleagues and boss, and finally everyone else.

What do you think about Telenor storing your Rich Presence information for 3 months?

We told her how much information about her mobile phone that is stored, and her first thought was that it was quite frightening. She went on saying that it could be nice to use it to stop crime, and in a way that it was comforting. When told what a Rich Presence service could store about the users and with this build a complete profile on who you are, she said that it was scary and an invitation to misuse. She was clear stating that the data records should not be used unless it is absolutely imperative.

Which services do you think a third party could provide?

With regards to what services Telenor should have and what services third party could offer, she had no clear opinions. As long as the services complied with *personopplysningsloven* she felt okay with it. She thought that this party service provider could provide with more exciting services than Telenor, and that she might be interested in such services. Finally, she remarked that the more number of people or companies that had information about you, the bigger the risk of misuse was. Because of this, she didn't entirely trust Telenor either.

Conclusive thoughts

Generally, she said that Rich Presence services had to be services that users must be able to disable or decline, i.e. it could not be something forced on you from you phone company. It should be something you had to order to get it, not something you had to cancel to get rid of it. As a final remark, she thought more people might be interested in anonymous services, and that there had to be ways of controlling the flow of information to limit what other users are able to see about you.

6.4 Results

From the interviews we did, we see some correlation with the answers given and our own opinions. We see that both subjects will in some degree see how a Rich Presence service can be of use. However, they point out some obstacles that needs to be overcome in order to get acceptance from them, as representatives of their respective demographic groups. The first and foremost thing needed is security. The importance of this cannot be underrated, as most people will not give away private information if they suspect it may be misused. As this system relies on accurate personal information at all times, security must be a key issue.

Another observation was that both subjects chose to differentiate what pieces of information are given to various groups. They both saw fit to separate family and colleagues. Also, the potential of groups like friends, close/distant relatives and other important contacts were mentioned. These groups could be given different privileges depending on what the user is comfortable with sharing. This feature coincides what we also see as an important part of the system.

The third thing mentioned that closely resembles our thoughts is the need for an easy-to-use interface and that the entry level should be low. Many users may not bother spending hours customizing and setting up the software, neither will they start using an application that requires training or technical insight in order to function properly. This is especially important when trying to reach the older generations and those who have no previous experiences with similar or related (IM-programs, scheduling software, GIS services) software.

On another notice, both interviewees brought up the subject of keeping track of known criminals. We see some difficulties with this, both in a legal and practical sense. Firstly, surveillance without court approval of probable cause is illegal³⁰, and if criminals suspect their movements and Rich Presence information is monitored, they can easily dispose of their phone or work actively to fool the system. This monitoring also approaches the Big Brother-society of George Orwell's *1984*.

As a summary, we see that despite differences in age and sex, much of our subjects' general views and thoughts are similar to our own, although with different approaches. This is interesting, as we suspected there might be a difference of opinion. In fact, we saw how our first subject initially was quite skeptic, but when presented with possibilities of a secure system set up for his needs, he actually got quite enthusiastic and started suggesting some services on his own. All this suggests for us that our own thoughts and opinions may be of general character, also applicable to those of an entirely different generation than our own.

³⁰ Personal communications with Pål Jeger Pedersen, Rogaland Politidistrikt, 25/4, Phone (+47) 518 99 000

7 Discussion

This section contains the discussion part of this report.

7.1 Areas of application

This section describes appliances of Rich Presence services. We will here be looking at a wide range of uses for these services, what services exists already and what we call a killer application which may be needed to bring these services into widespread use.

Killer application

A killer application is a service that is so useful or cool that it will attract a large number of users and thereby reaching widespread use. Since Rich Presence fills a need that to some degree does not already exist, it might require this type of application to be a success. To identify a killer application in advance is often very hard as it is hard to predict how the market will respond, and experience has shown that experts have been wrong before. Earlier examples of killers are the camera now found on most cellular phones, text messaging (SMS) and over-priced services that sell ring tones and wallpapers. On the other hand, WAP, MMS and video telephony was expected much broader appeal than it actually has got.

A killer application for Rich Presence services needs to be very easy to use and appeal to a majority of the users. It should give people a better feeling of privacy and availability and might also fill a need that people did not know they already had.

Range of use

Rich Presence services have a vast range of uses where only the imagination sets the limit. Here we will look at some of the more useful ones that we have identified

Availability settings based on context

When one is in a meeting or otherwise busy it is very annoying if the phone starts ringing. As a consequence one usually turns of a cellular phone on such occasions. However you would still like to be available for a family emergency or other crisis. This can be achieved with a Rich Presence service giving out different availability options for individual groups or users.

Team and collaborative services

A very useful prospect with Rich Presence is to integrated services with existing collaborative services to provide more functionality and better solutions to teams like project groups and between colleagues at work. The possibility to combine agenda with actual updated information about what individuals are doing and where has the opportunity to greatly increase efficiency in an organization.

These services will mainly be used in an organization where the members either work for the organization or have some other connection to it. It can also be used in private life to

figure out what friends and family are doing at the moment, but this has some privacy issues that we will come back to and might not be as useful anyway.

Traffic pattern services

Traffic pattern services are based on the fact that powerful computers can look at collected raw data and find useful patterns by analysis. These patterns can be used by city planners who need to know which public square is most frequently used or by individuals who want to know the fastest means of transportation through an urban area based on weekday and time.

These services are mostly anonymous as the data is deduced from a lot of samples done over a longer period of time. This means that it should be impossible to gather information about individual persons from these services. Liability issues may arise if this is not the case.

Location aware services

Location aware means that a service uses a known position of the user of the service to provide useful information. This has for instance been used for tourists to provide proximity to point of interest (POI). These services are not necessarily categorized as Rich Presence services, but come as a by-product of having positioning systems active at all times.

A look at existing services

A lot of the functionality categorized under Rich Presence is already offered by existing services. Many users already have familiarized themselves with some presence information through the use of IM and VoIP services such as Windows Live Messenger or Skype. Some of these applications are finding their way onto mobile devices, both as means of communications and to exchange presence information. These services offer the ability for user to set status information from a number of presets, such as busy or away. These services have attained a large group of users and many studies have been conducted on the use of these services.

Social network services are also gaining popularity; these include MySpace and Facebook, online services that allow people to come together online around shared interests, friends or causes. Many of these services also offer online schedules and event planners, ways to explore full or limited views of your friend's friends, as well as ways of organizing your contacts into groups depending on your relationship.

Current web giant Google offers a wide array of services where users may share content with others including collaboration software like online document and spreadsheet applications, photo sharing with selected friends or the entire world. As needed with a Rich Presence service, a lot of care is needed in the development of these services to take care of the users' need for privacy. How much they are likely to reveal about themselves in this manner may also differ from what is experienced elsewhere. For instance, many users will disclose a lot of personal information in their personal web logs or may reveal political views, educational level or professional experience by contributing to a wiki,

both usually publicly available

Positioning- and map services have existed for many years. Services include GIS readers like above mentioned Google's Google Earth, NASA World Wind or GeoPDF for Adobe Reader. Positioning services has long been synonymous with GPS, however, the EU with a wide array of partners are planning an independent service called Galileo. Also, GSM, WLAN, RFID or almost any other wireless technology may offer positioning with varying degrees of accuracy and range.

7.2 Quality of data

Rich Presence services gather data about its users make assumptions about the data gathered and presents this in form easily understood and perceived by humans. The quality of the underlying data is an indication of how accurate the service will be.

How the data is presented and what information is included also say something about how useful the service might be.

Multiple states

Users may find themselves in a situation where they want to be in several states, for instance if a user is *hungry*, *in a meeting* and *at work*. The system should prioritize the states that require the most privacy, but should be able to keep track and display all states. Conflicting states, such as *at home* and *at work* at the same time, should be allowed, but discouraged as this may confuse and cause mistrust from other users.

If multiple states are used, the system should still differentiate on which pieces of information, in this case which states, users see. This means that your colleagues may see you as *in a meeting*, whereas your friends and family may see you as *busy* and *hungry*.

Level of detail

The underlying data should be as detailed as possible, but it should be aggregated before presented to the user. The data needs to be interpreted, since data like geolocation are not very readable for humans. Also one would not want to give up ones position at all times. For instance if a user is located inside his house simply saying *at home* will be enough for friends and family to know exactly where the user is located and without this being exposed to complete strangers. Also *in a meeting* can be combined to show data from the calendar where the title *Project X budget meeting* might be stated. Further knowing participants in the near proximity will increase the level of detail. This level of detail should defined by the user and set individually for different groups and users. High level aggregates are useful for defining human readable statuses.

Some services do need the exact data, for instance when third party services need exact geoposition for a location based service. This is ok, but what information these third party services receives, should be clearly defined and under the control of the user.

Information integrity

As stated in the security section, the integrity of the information is very important. If system integrity is broken in some way, one cannot trust historical data to do statistics and other pattern matching procedures. Users do not care too much about historical data. For them information integrity means that they can trust the status they see on friends and family. If they cannot they will start to distrust the service making it less useful

No matter the state of the user it should be accurate, informative and unambiguous.

Timeliness of data

When checking the status of others, it is often interesting to know how updated this information is. It would also be interesting to know for how long the user is expected to stay in this state. A presence service should provide both so that users are able to determine to what degree the data can be trusted. It also increases the usability of the service as one has more information to base assumptions on. As we have seen, Rich Presence attributes should be updated automatically with minimum effort from the user. If automatic updates are done at short intervals the derived status are more predictable and trustworthy.

7.3 User Experience

This section is concerned with how these services should be designed to give users the best experience.

Interface

Rich Presence services will be used by a lot of non-technical users and therefore needs to be intuitive and easy to use. This means that an average Internet user should be able to set up his or her profile in a matter of half an hour without further introduction. Also users should feel comfortable that their personal information is taken care of in a secure manner.

For this to be achieved the system needs to have a reasonable default configuration so that users do not suddenly realize that their information is available in a way not intended. Common pitfalls are described in section *When privacy is invaded*. We will not present detailed recommendations on how this user interface should be designed, still we must encourage that effort is put into making the interface as easy and simple as possible, with the possibility of advanced options for advanced users. If made to run on mobile phones it is important to make an application that runs on as many mobile platforms as possible. An example of an application that runs on almost every platform is the part-Norwegian developed browser Opera Mini³¹, where prestige is put into porting the application for as many platforms as possible.

Access control

One way of getting an easy-to-use system is to give users the ability to arrange their contacts into appropriate groups. There should by default be a number of groups, each

³¹ [7W] <http://www.operamini.com/>

with a set of access rights that most users would agree upon. For more advanced users, the system must allow the customization of both groups and access rights. This also includes the ability to give individual users special rights regardless of groups. Also Khalil and Connelly³² suggested that when creating a new group, permissions could be copied from an existing one. This improves usability and means that users can spend less time adjusting their settings.

The set of rights for both groups and users may vary with the current role a person is in. If a user is *at work*, he or she will probably be more comfortable with their boss knowing their exact coordinates and company than the same information if the user is *attending a party*. This calls for different roles, these may be set by status, calendar events, location or manually. These roles should also have presets which most users can agree with, in order to minimize the manual labor of setting up the system properly and to save time when a new group is created.

For advanced users there should be an option of previewing other users view of them self. This means that a user should be able to see what information the system displays about them from the point of view of any of their contacts. This is useful for both advanced and paranoid users because it gives a *What-you-see-is-what-you-get* interface that intuitively tells you if you are giving away too much or too little information to any user.

From what we have seen it is important to have a powerful set of options, but still have the opportunity to do configurations fast.

System Trust

It is imperative for the users that they feel secure in using this system. Users need to trust that the personal information they enter into the system is only distributed to approved watchers. They also need to trust information they get from the system regarding other users. As long as users feel they save time or get more spare time using this system, they will have no problem spending time on setting it up and actively using it.

7.4 Public acceptance

One of the main purposes of this report was to look at how to achieve public acceptance for Rich Presence services. This will be discussed in this paragraph. We have already looked at many of the prerequisites for acceptance, like security and what people are willing to share.

The kinds of services which are designed to let you know where your friends, family and colleagues are needs a large user group to be successful. Without a certain amount of users the service will be of no real value. Therefore we will also look at what is needed to draw a lot of users.

³² [11B] A. Khalil & K. Connelly. *Context-aware Telephony: Privacy Preferences and Sharing Patterns*. 2006

How and when

For people to start using Rich Presence services they need to accept the fact that personal information will be accessible for other online users. Sharing should therefore be optional and users should have to explicitly accept an agreement before any information is shared. Also it should be possible for users to turn the system on and off. Skeptical users will probably do this every night or in other special circumstances where they feel the need for privacy. We believe users will quickly start to trust the system all the time, but at first this option can be useful. This would be similar to when people started using cellular phones. Most would turn it off when at home or at night when they are sleeping. The growing trend now is to keep the phone on at all times.

Time

One of the main benefits of Rich Presence is for people to be more accessible and save time by making daily routines easier. People get annoyed by tedious work, so it is important that a Rich Presence service has a sensible level of automation. The level of automation will be discussed more later on. Further one should get more done in the same amount of time. Increasing efficiency can be a major factor for people to start using new technology. On the other hand, if the service is highly successful people would start spending a lot of time exploring the possibilities and expanding categorizing the social network. A service where you can find people you have not seen for a long time and learn what they are doing and where in the world they are can be extremely popular. Examples of such successful personal network services are LinkedIn and Facebook as discussed in before. These types of services has no problem getting public acceptance even though the information shared is highly personal and people tend to spend a lot of time just browsing to see what friends are doing. These services would steal a lot of time, but since people are using the voluntarily it is accepted.

Level of automation

People do not want to manually change their status all the time. Ideally, one would not have to worry about updating the information at all depending on a service to do this on its own. However this could prove problematic. One solution would be to train the system so that it would recognize reoccurring situations based on time of day and position and use historical data to set status. This still has to be manually verified for errors as users will quickly loose interest if they can not rely on the information they get to be accurate. Still a high level of automation is required to achieve public acceptance.

The level of automation would have to be set according to tests so that the rate of errors is small. Whether or not the status information is set manually or derived from other data, knowing when it was last updated and for how long the information is believed to accurate would be very useful to increase users trust in the system. This would further increase the chances of acceptance.

Coolness

We have already talked about a killer application and how it could be what a Rich Presence service needs to become a success. One important key to a killer application is

the coolness factor. Louise Barkhuus³³ found that our privacy concerns using a new technology can be greatly influenced by the coolness factor of the product. This can be seen in a lot of services where coolness has contributed to the success of a product. Examples are Facebook which we have mentioned earlier.

Privacy management

People have a strong preference for managing privacy by configuring permissions at group level when defining permissions for sharing various aspects of awareness about themselves according to Patil and Lai. This suggests that grouping provides a convenient balance between privacy control and the burden of configuration. Empowering users to control how and when aspects of their context are shared with whom, can enable them to find more suitable points of balance between awareness and privacy. This is evident from the willingness of participants to provide high levels of awareness to team members at work during business hours. Increased system transparency through upfront disclosure of pieces of personal context to which a system has access seems to act as a trust builder. And for the future, appropriate feedback mechanisms and interfaces need to be explored to further help users visualize their permission settings.

Pricing

Since most Rich Presence services would need a lot of users to be successful the general use by private individuals should be free of charge. This means that many will sign up even though they may not plan to use the services much. Money can be made by charging corporate customers or corporations who are willing to pay for collaborative services.

Another way to make money is to charge extended services that people are willing to pay for. One of benefits of Rich Presence services is that the users usually have a customer relationship with the services provider. This means that payment for specific services can be charged together with the normal monthly fee. No extra payment method is needed. Extended services can also contribute to the coolness factor discussed in the last section.

Benefits greater than the risk

A last element to contribute to public acceptance is for the value of the services to be greater than the negative possibilities. Many of the proposed services we have looked at here give great value to the users. Some of them will help save time, others to save money on electrical bills. One would also be able to work more effectively, which a lot of people finds important. If the benefits are large enough people will easily overlook the downsides.

7.5 Personal thoughts

In this section we will look at some of our personal concerns regarding Rich Presence. It seems that personal privacy is losing towards the Internet enabled services which makes more and more of our personal life available online. This is not necessarily a bad thing, but developers and designers of these services should keep these issues in mind.

³³ [8B] Louise Barkhuus. *Privacy in Location-Based Services, Concerns vs. Coolness*.

Ethical concerns

The ethical concerns related to Rich Presence are all connected to the distribution of personal information. People's information is much more easily available and may be aggregated in many ways. Some people may gain access to information that they may misuse. This could lead to the loss of public acceptance for the service, and raises some ethical concerns.

What is to be expected from a serious and large actor

Since these services seem inevitable and people will start using them whether it seems safe or not (given a security and ethical point of view) one should strive to achieve services that are both useful and safe. This was pointed out by Louise Barkhuus. Also this should be done by serious actors which people believe in. We feel Telenor may be such a serious actor, and is one of the few companies that may be trusted with personal information. Already they keep an amount of data that may be harmful to some if released, but they have the integrity to keep it securely stored.

What services may or may not come from third parties

Most people will have different opinions regarding what information they allow third parties to gain access to. Our point of view is that there should be no limits on what a third party may provide or gain access to, but that the users themselves grant access to information in each case for each service provider. This means that if they subscribe to a third-party service requiring for instance position and current status to work, users need to approve that the provider gets access to these pieces of information. This is information that the provider should only get access to as long as the service is active, and should be pruned for deletion when the service is unsubscribed.

We found that our interview subjects had different opinions on what they would release; one would only release anonymous information, whereas the other saw no difference in letting Telenor or a third party get access to her information. This shows that people have different frontiers on what they feel is invasion of privacy and what may pose as a security risk. Having the opportunity to share all information with any third-party provider, but always limiting it to what the users feel secure with at all times may prove to be a good solution.

This puts no constraints on what kind of services that may be offered, as the users themselves always need to approve the distribution of personal information. As long as there is a willingness to share information, the gain will be innovative ideas and new services.

8 Future work

This report is a collection of ideas, thought and opinions based on what our group knows and has learned by reading source material. Our thoughts and opinions have been confirmed by our two interviews that in many ways approved on our views. Future work from this report should be a larger-scale survey or make a test application for proof-of-concept and public try-out. This report should only be viewed as a tentative result, in spite of what we feel is a thorough and well-considered study of what source material we found.

In addition, we see a need for the “killer app” that really can launch a Rich Presence service. We have not spent much time in brainstorming to find new, innovative ideas; this subject needs to be further explored. Indeed, there may be a market for a Rich Presence service, as this creates needs users did not know they had. However, before actual data concerning test results and user patterns is acquired, it is hard to say if it will work. We hope that our conclusion will reflect a larger-scale survey and may be valid for a substantial part of the population, and hope that Telenor will benefit from our preliminary studies.

9 Conclusive thoughts

We have during our work been trying to answer some questions regarding how acceptance for Rich Presence can be achieved and what should be considered when implementing such a system. Through our work we have identified several key points for acceptance and success. Users need to trust the system; in both that they need to know that their personal data is kept personal and that the information they get from others are correct. Norwegian laws will in many cases protect against organized misuse of information.

Keeping a low entry-level and giving users the ability to put contacts into groups with pre-defined access levels that may also be user-defined has also proven to be important, this because users' sense of privacy may change with setting and context. One also sees the need for a killer application that will boost the system's popularity and generate a need that currently does not exist. We have named some potential services and expect that both Telenor and third-party service providers eventually will find new areas of application.

10 Bibliography

This is a list of all sources used in this report.

10.1 Books and articles

- [1B] Ben Teitelbaum. *Connectivity Middleware for Voice and Integrated Communications*. Page 6. 2004.
- [2B] Anne Adams & Martina Angela Sasse. *Privacy in Multimedia Communications: Protecting Users, Not Just Data*. Page 4. 2001.
- [3B] Roger Clarke. *Person location and person tracking. Technologies, risks and policy implications*. Section 6.3. 2000.
- [4B] Kevin Mitnick. *The Art of Deception: Controlling the Human Element of Security*. Part 2. 2002.
- [5B] B. Carrier et al. *Know your enemy: Revealing the security tools, tactics and motivation of the black hat community*. Page 562. 2004.
- [6B] J. Jachner, S. Petrack, E. Darmois, T. Ozugur, *Rich Presence: A New User Communications Experience*. Page 4. 2005.
- [7B] Mathias MOULIN. *Location-based services and the e-privacy Directive 2002/58/EC*. Slide 5. Source: http://ec.europa.eu/information_society/policy/ecomms/doc/info_centre/public_consult/location_based_serv/comments/location_based_services.ppt. 2007.
- [8B] Louise Barkhuus. *Privacy in Location-Based Services, Concerns vs. Coolness*. Page 4. 2004.
- [9B] Dr. Robert P. Minch. *Privacy Issues in Location-Aware Mobile Devices*. Page 4. 2004.
- [10B] Sameer Patil & Jennifer Lai. *Who Gets to Know What When: Configuring Privacy Permissions in an Awareness Application*. Pages 2-9. 2005.
- [11B] Ashraf Khalil & Kay Connelly. *Context-aware Telephony: Privacy Preferences and Sharing Patterns*. Page 5. 2006.
- [12B] J. Olson et al. *A study of preferences for sharing and privacy* Page 2. 2005.

10.2 Web pages

- [1W] Location-Based Services, <http://www.mobileinfo.com/LocationBasedServices/index.htm>, Last visited 07.02.2007, Mike Flom, 2002
- [2W] Securityfocus. *UCLA alerts 800,000 to data breach*. <http://www.securityfocus.com/news/11429/2>. Last visited 28.02.2007
- [3W] Privacy Rights Clearinghouse. *A Chronology of Data Breaches since the ChoicePoint Incident*. <http://www.privacyrights.org/ar/ChronDataBreaches.htm>. Last visited 28.02.2007
- [4W] Datatilsynet. *Lokalisering av mobiltelefoner*. http://www.datatilsynet.no/templates/article_1523.aspx. Last visited 21.03.2007.
- [5W] Staten. *Lov om behandling av personopplysninger (personopplysningsloven)*. <http://www.lovdata.no/all/tl-20000414-031-001.html>. Last visited 21.03.2007.

- [6W] Cnet news. *Selling your personal data*. http://news.com.com/2030-1069_3-5068504.html. Last visited 21.03.2007.
- [7W] Opera. *Opera Mini™ - Free Web Browser for your Mobile Phone*. <http://www.operamini.com/>. Last visited 18.04.2007
- [8W] Datatilsynet. *Krav om samtykke ved bruker av lokaliseringsdata*. http://www.datatilsynet.no/templates/Page_874.aspx. Last visited 21.03.2007.
- [9W] Telenor. CPA – Telenor Mobil. <http://cpa.telenor.no/cpa/>. Last visited 25.04.2007
- [10W] RFC 2778, A model for Presence and Instant Messaging. <http://www.ietf.org/rfc/rfc2778.txt>. Last visited 25.04.2007
- [11W] RFC 4480 RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF). <http://www.ietf.org/rfc/rfc4480.txt>. Last visited 25.04.2007
- [12W]] RFC 3856, “A Presence Event Package for the Session Initiation Protocol”, 2004
- [13W] Are girls (even) more addicted? Some gender patterns of cell phone usage, Hans Geser. http://socio.ch/mobile/t_geser3.htm. Last visited 25.04.2007
- [14W] Economics of Personal Information Exchange, Sholtz, Paul. http://firstmonday.org/issues/issue5_9/sholtz/index.html. Last visited 06.05.2007

11 Appendix A: Glossary

GIS – Geographic Information System. A system designed to capture, store, analyze and manage geographically-referenced information. By the use of this tool, you can analyze, edit, present and execute queries on geographical and spatial information.

IM -Instant messaging refers to a service where users can send short messages to each other. This is typically one or few sentences, but can also be used for entire conversations.

Location – LBS (Location Based Services) Services that can provide the present location of a mobile device. Most often this information will appear as a marker on a map. No further aggregation of information, like coupling of location and status is done.

POI – Point of Interest, a geographical location of interest which could be referred to through a location based service. For example, when you request a location based service for a place to eat, the closest restaurant would be a Point of Interest.

Presence – Information about the owner of a mobile device concerning his/her current status. This info is shared with other users(watchers) Instant messaging is the foremost field for use of presence information.

Presentity – Abbreviation of “Presence Entity”. An entity which provides presence information to a presence service³⁴

RP - Rich Presence – Combines Location and Presence into a service where you are also able to divulge information about activity, type of location, relation to other presentity, mood, time zone, status, when the service last was used, and overall role.³⁵

SIP - Session Initiation Protocol is an application-layer protocol for creating, modifying and terminating sessions between users.

VoIP - Voice over IP, using IP (Internet proctocol) as a carrier for speech instead of the traditional copper wire.

Watcher – Users who subscribe to a presence service in order to receive presence information about other users.

34 [10W] <http://www.ietf.org/rfc/rfc2778.txt>

35 [11W] <http://www.ietf.org/rfc/rfc4480.txt>

12 Appendix B: Point list used in Interview

Note: Because the interviews were conducted in Norwegian, this part is only written in Norwegian. It contains pointers to guide us through the interviews.

Intervju spørsmål til "Den vanlige mann"

Om person:

- Alder
- Yrke
- Kjønn
- Sivilstatus

Bruk av teknologi:

- Hvor mye bruker du mobiltelefonen din?
- Bruker du Instant Messaging-programmer? (MSN, Skype)
- Vil du klassifisere deg som en avansert bruker? Hvor avansert?
- Har du hørt om *Buddy* (Netcom) og *Kompis* (Telenor)?
 - Hvis ikke, forklar

(Bør være et kort sett med spørsmål som får ut den vesentlige informasjon.)

Hvilken type informasjon ville du ha delt med flere av dine bekjente?

- Hvor er du?
- Hva gjør du?
- Hva er din status? (Opptatt/ledig/borte)
- Hvem er du sammen med?
- Kalenderen din?

Insentiv

- Hva skal til for at du er villig til å dele informasjonen gitt ovenfor?
-

Hvilken informasjon ville du synes var nyttig?

- om dine venner
- om sjefen din
- og kollegaene dine
- om barna dine (if applicable)

Hvilke tjenester ville du synes var nyttig?

- Trafikktjenester (raskeste veier, minst kø)
- Strømsparing (hjem og hytte)
- Er du villig til å oppgi din lokasjon kontinuerlig, mot at du får tjenester som for eksempel at varmen i huset reguleres opp når du begynner å nærme deg hjem?
- Slippe å få jobbtelefoner hjem, telefon når du er i møte...m.m fordi Rich Presence er oppgitt.
- Buddy Driving, dvs at om du deler reiserute og –tidspunkt kan systemet finne ut hvem av dine venner du kan dele bil med.
- Høre om de har noen tanker?

Er det viktig for deg å kunne styre hvem som til en hver tid har tilgang til hvilken informasjon?

- Ville du bruke tid på å sette opp en slik rangering?
- Hvilket detaljnivå ville du ønske?
 - For eksempel skille familie, venner, kolleger, sjefen din.

Hvor lenge skal for eksempel Telenor kunne lagre informasjon om deg? De er forpliktet til å lagre alt om samtaler, lokasjon av samtaler i 3mnd og kan lagre opptil 6mnd.

- Hva synes om Rich Presence informasjon blir lagret om deg så lenge?
- Hva synes du om at dine venner kan danne seg et komplett bilde om hvem du er, utifra hva slags informasjon Telenor har samlet opp om deg?
- Enn om hvis dine venner kan finne ut hvor du bor, hvor du jobber/studerer, dine rutiner ut ifra oppsamlet informasjon om deg?

Hva bør telenor ta seg av og hvilke tjenester synes du tredjepart kan ta seg av?

- Seriøsitet
- Sikkerhet
- Spennende løsninger
- Utbredning