

# PRIMA—Privacy in the Making

---

*Final financial and scientific report*

## 1 Introduction

The PRIMA project was outlined in the fall of 2005, exactly five years ago. From a privacy perspective this half decade has been terribly exciting, mostly due to the accelerating pace of technological change and IT adoption patterns in society at large. Many people used IT five years ago, but social media (used by everyone, not only teenagers) and mobile Internet have created an unparalleled ubiquity and width in IT use. Social service like MySpace, Facebook, Twitter, and more recently, location-based services like Foursquare, as well as constantly Internet connected mobile phones like iPhone and Android, have skyrocketed the daily use of IT among large parts of the population in large parts of the world. During this period, the temperature of the privacy debate has risen from mild to hot, and privacy issues have expanded from being of concern to mostly IT professionals and policy makers to a matter for the whole society.

In the midst of this accelerating development, the primary goal for PRIMA has been to create an understanding of the concept that would allow for a prolific use of privacy as a motivating factor in IT design and development. The most important feature of our approach has been to develop and maintain a multi-disciplinary perspective of privacy (Bylund *et al.* 2010). Privacy is a social construction fundamentally rooted in relationships between individuals and other individuals, groups of individuals, as well as corporations and nation states. As such, we must have a clear understanding of how to interpret privacy from a social perspective. Some privacy-related conflicts are managed and regulated using social norms and codes, but in other cases conflict resolution relies on laws and formal regulations. Therefore, a solid understanding of how privacy is interpreted and dealt with within the legal discipline is required. Finally, the reason for the recent dramatic increase in interest in privacy issues is rooted in the rapid technological development and the accompanying development of the information society, not least since relationships nowadays are often mediated by IT. Grounding our work in various IT-related domains has therefore been natural.

One of the reasons for applying a multi-disciplinary research approach is that it assists in creating *divergence*—to extend the boundaries of what privacy is, or how it is interpreted—in order to explore both opportunities and threats to privacy in IT. In order to successfully open up a problem space like this, we have applied qualitative, quantitative, as well as explorative research methods. With this mix of perspectives and methodological approaches our aim has been to produce results that in combination provide a foundation for better design solutions.

In the following, we present the project results along the two main types of research activities pursued within the project: collaborative research activities (Section 2) and meta studies (Section 3). In Section 4 we outline our recommendation for how to proceed with future IT-related privacy research. We conclude with a listing of tangible project results (Section 5) and a financial report covering the period 2006 through 2010 (Section 6).

## 2 Collaborative research activities

On the most fundamental level, the bulk of the PRIMA project results builds on active collaborations with a range of other research projects. These have provided relevant domains for exploring privacy in relation to IT. PRIMA, on the other hand, have offered other projects increased attention to privacy issues, something that has not always been of top priority prior to the collaboration.

Below, we briefly describe 15 of these collaborative research activities.

### 2.1 Hot Potato

Hot Potato is a pervasive game design intended for Bluetooth-enabled cell phones. The game design of Hot Potato encourages players to search for people, known or unknown, with Bluetooth-enabled cell phones. Once such an individual is found, the player must follow her at close distance in order to attach and retrieve a potato. While it is difficult to find anything offensive with the technical implementation of Hot Potato, it is not very difficult to imagine that the behavior of the players that the game stimulate can be regarded as offensive, sometimes even experienced as stalking. In collaboration with the Solid and IPerG projects, we conducted two studies of the Hot Potato game: one quantitative based on questionnaires and one qualitative based on real use situations. The study was organized as a graduate level class at the Helsinki University of Technology as a collaborative effort between SOBERIT and SICS.

The results of this activity are described in detail in two technical reports (Nordström, Pyy & Salo 2007; Cottier, Salonen & Padilla 2008).

### 2.2 Habbo Hotel

Data from a case study (Johnson *et al.* 2010) on the virtual world and social networking site Habbo Hotel has been used to explore different privacy perspectives during the whole project. Compared to other social media, there have been few reported privacy violations in Habbo. We deem the following characteristics of the case as important privacy-shaping factors: 1) anonymous participation, 2) no possibility to post photos, 3) enforced policy of non-sharing of personal information (address, phone number, e-mail), 4) business model that relies more on micro-payments by users than on targeted ads. By looking at the case from an interactionist perspective, this case also strived to connect privacy more deeply with human-computer interaction. In particular, mapping privacy to particular user interface elements, via the theories of personal boundary regulation (Johnson *et al.* 2010). The study rests on a longitudinal mixed methods approach, including interviews with both developers and users, online texts written by users, and a user survey.

### 2.3 Citizens' views of privacy protection

As one of the first activities of the PRIMA project, we participated in the design of a questionnaire for a study of citizens' views of privacy protection conducted by a Swedish legislative committee ("Integritetsskyddskommittén"). The actual study was carried out by Statistics Sweden, but the results have been used in the PRIMA-project for understanding basic privacy concepts and needs for protection. Particular attention was devoted to what may be called the genuine information needs of the lawmaker, keeping in mind that many previous surveys and opinion polls have produced information of little or uncertain value. On the whole, the work provided opportunities to discuss theoretical and practical aspects of privacy protection that were perhaps just as valuable as the actual results of the survey.

The study is published in a public Swedish government report (Kirchberger & Seipel 2007).

## 2.4 Mirroring Digital Identities

Founded in observations of the vast amounts of personal information being stored and processed by everyday information and communication technologies, we define the term digital identity. The term refers to the different views of a single individual a spectator of this body of information may form, such as a family father, a journalist, or a football fan. In the current information technology discourse, similar observations generally stir fear and concern. While we acknowledge that there is reason for some of these concerns, we emphasize that in real life privacy is not only used as a protective shield, but also as a creative instrument for defining the self. In relation to social technologies, we also highlight the information imbalance that information and communication technologies introduce as compared to real life social interaction.

Motivated by the two facets of privacy and information imbalance, we designed a tool to support user awareness, to allow users to track the image they project on the net, to support them to uphold the identities they wish to maintain, and to enable them to identify and counter incorrect, inadvertent, or even unwanted facets of their personality made visible through their actions. The aim with the tool, The Digital Identity Mirror, was to crawl the Web for personal information regarding the user. The result would be analyzed and mined for different facets of the user's social identity.

The activity was conducted in collaboration with the Solid project. A prototype version of the design was implemented and described in a conference paper (Bylund *et al.* 2008) and an MSc thesis (Arvidsson 2008).

## 2.5 The role of anonymity in human-generated recommendations

Many social network sites, such as Amazon or TripAdvisor, give the members a chance to provide comments and suggestions to other members. This can be done either anonymously or by revealing the recommender's identity, either with a nickname or with a real name. Anonymous recommendations are convenient for the privacy of the recommender, but do they have an effect on the use and utility of the recommendation for the person reading it?

This was studied in the context of Amazon using a careful field study that focused on seven active users of Amazon. It was found that indeed, anonymity did have an effect: recommendations made with an identity whose recommendation history could be tracked within the site were read more often and judged more useful. In fact, some participants did not consider a site with only anonymous recommendations a social network site at all. This was not the only factor, though; for instance, some members concentrated on reading negative reviews, to become aware of potential pitfalls with the product they were considering.

This activity resulted in several publications (Räihä & Leino 2007; Leino & Räihä 2008; Ovaska, Leino & Räihä 2008) and an MSc thesis (Leino 2008).

## 2.6 Pieces of Identity

The Pieces of Identity installation was designed and implemented with the purpose of being used during the inaugural party of the Mobile Life centre. During the party, it gave the guests of the Mobile Life center the possibility of experiencing two aspects of automatic processing of personal information rarely reaching the surface of the privacy debate. The first aspect is that privacy is not so

much about secrecy as it is about timing. Personal information, no matter how trivial or non-controversial, can still be private if it is revealed in a way or a place out of the ordinary. With the installation, we experimented with revealing such information in different unordinary places serving different social purposes. The second aspect is that the processing of personal information of the information and communication technologies of today is increasingly important for the definition of the social identities of people. With the installation we illustrated this by allowing the guests to trigger the displaying of personal information by identifying themselves (both voluntarily and involuntarily).

The installation was deployed and studied live with 200+ users in late August 2007 during the inaugural party of the Mobile Life center in Kista. The activity was conducted in collaboration with the Mobile Life centre and resulted in a conference publication (Bylund, Höök & Pommeranz 2008). In addition to studies of the guests being the direct users of the installation, we could also observe legal concerns of indirect users, namely the top administration of the Stockholm University (the principal organization of the Mobile Life centre).

## **2.7 Privacy as a component of usability in ubiquitous computing**

Usability is a concept that is most often considered in the context of utility software and desktop environment. As ubiquitous computing becomes more common, the concept of usability needs to be re-evaluated and broadened. Of particular interest in ubiquitous environments is privacy and its role in usability, since ubiquitous environments make the inconspicuous monitoring of people's actions possible, sometimes even relying on such monitoring.

A survey study was carried out with 156 respondents, followed by discussions in small groups. The respondents were presented with 8 ubiquitous computing scenarios and asked questions about possible issues in the scenarios. The analysis of the results highlighted five important usability attributes: unobtrusiveness, ease of use, user satisfaction, error-free use, and visibility. Seven additional general properties affecting the take-up of such a system were identified: flexibility, user control and freedom, reliability, accessibility, efficiency, productivity, and privacy.

This activity resulted in an MSc thesis (Heikkilä 2007) and a part of a conference paper dealing more generally with the role of scenarios in studying privacy (Ovaska & Rähä 2009).

## **2.8 Legal perspectives of ubiquitous computing**

During 2008 we conducted a study of privacy issues related to the spreading of all kinds of automated computing to a rich variety of environments and activities, often referred to as *ubiquitous computing* or *pervasive computing*.

For the drafters of the Swedish Data Act of 1973, the right to be let alone was the key concept and the basis for shaping the law. The task consisted in striking a balance between the individual's right to be let alone and various legitimate claims to obtain access to and use personal data. Sweden was not unique in this respect, similar approaches can be found elsewhere.

Over the years, the overall view of privacy protection as well as its core principles have become increasingly complex and fine-grained, but the right to be let alone is still largely perceived as a corner stone. This view is not without problems.

The reason is that, as for invasion of privacy risks related to ICT, the classical right to be let alone has shortcomings as a guiding principle. It can be described as a basically negative strategy with its focus on fear and prohibition. In other words: in the perspective of the right to be let alone, ICT is considered a menace and uses of personal data have to be constrained. Taken to extremes – which is not unknown to happen – this negative view of ICT can stifle positive and desirable uses and developments of technology. Therefore, the right to be let alone should be balanced against a right to be included. Such a right is based on a positive view of ICT, where ICT is seen as a framework for togetherness (coming together, acting together, achieving together, and so forth).

To a large extent, this is a question of parallel thinking and of understanding and appreciating the significance of ICT as an instrument for human communication and cooperation. Thinking along such lines, the main concern should be not only to make the networked society a place where you dare live but to make it a place that improves life and living, a place where people can meet one another, join their strengths and develop together, where the everyday burdens of life become easier to deal with, where enlightenment and education are within everybody's reach, in short where ICT can help people grow as members of just and democratic societies.

A paper on the issues titled "Alone No More" was published in a Festschrift in 2008 (Seipel 2008).

## 2.9 E-Stockholm '08 Legal Conference

The 23rd Nordic conference in legal informatics took place in Stockholm on November 17-19, 2008. The conference theme was "IT Regulation and Policies – from theory into practice". The overall purpose was to capture a legal agenda for ICT regulations and policies. It was considered important to bring into focus the advantages and disadvantages associated with varying approaches to legal steering of ICT-related activities. Among other things, the conference aimed at shedding light on different theoretical, legislative models as well as practical experiences of self-regulation and contract law.

In addition to a number of general application areas discussed in plenary sessions, five special track sessions were organized to ensure that presentations and discussions also went into more depth. In several of these tracks issues concerning privacy protection were touched upon, but one of the tracks was exclusively devoted to privacy issues. The privacy track was organized by the PRIMA project.

The invited workshop presenters were advised to do their best to act as *dynamos* and to rely on their particular experience and expertise. They came from different quarters: lawmaking, administration, legal science, including legal informatics, journalism and media, computer and systems science, information security, human computer interaction, cultural anthropology, and social psychology. It is not without risk to open the door to let in all kinds of different perspectives. Usually, discussions of privacy protection are relatively one-sided. This provides for shared frameworks, aims, methods, priorities, and so forth. Misinterpretation of arguments *etc.* are fewer, the terminology used is familiar to all, and so forth. Conversely, different perspectives do not always complement one-another, instead they may be in conflict regarding specific matters as well as general world-views. For reasons such as these, many attempts to *go multidisciplinary* result – at best – in parallel discussions. The situation can then be described as similar to the *parallel play* of little children who can play side by side but have not yet developed a social capacity that enables them to play together (exchanging playthings, drawing pictures, playing games, building things *etc.*).

The discussions during the workshop, covering broad issues such as “what is privacy and what are the main concerns” as well as specific issues such as technical, legal, and social solutions, resulted in a book chapter in the Nordic Yearbook of Law and Informatics 2006-2008 (Bylund *et al.* 2010).

## **2.10 Effect of culture and context on privacy attitudes**

One aspect of privacy is what people are willing to reveal of themselves (*e.g.*, where they are) and to whom (to strangers vs. family vs. employee vs. merchants). Such a study was carried out in the US in 2003. Its main finding was that the inquirer was more important determinant than the context of the person: they would be willing to reveal the same amount of information to an inquirer independently of the situation.

Our study did not support this in all cases. In particular, our participants (246 altogether) were reluctant to show details of their whereabouts at leisure, but were happy to do so when at work. Conversely, contacts by merchants were frowned upon when at work, but received more favorably when on leisure. A cultural effect was also observed. A relatively large subset of our respondents was Chinese, and they were in general more willing to show details of their whereabouts to the inquirer than Finns.

This activity resulted in a conference paper (Räihä & Ovaska 2009) and contributed to part of a conference paper dealing more generally with the role of scenarios in studying privacy (Ovaska & Räihä 2009).

## **2.11 Pictures and privacy**

The increasing mediation of everyday life, as well as the opportunity for ever more people to produce and publish user-generated content, has raised questions regarding the ways in which the boundaries between public and private are (re)negotiated. This study provides empirical findings of users of Finnish online photo-sharing site Kuvaboksi, focusing on their privacy considerations in photo sharing, their strategies in order to maintain boundary regulations, and their reasons for sharing publicly, as well as a list of unresolved conflicts in photo sharing. In contributing to a growing literature on the subject of online privacy issues, the study’s presentation of a wide range of user comments embodies the further aim of providing material for future comparisons of different technologies with regard to privacy issues, a feature lacking in current online privacy studies.

All interviewees stress the importance of regulating their boundaries, and own to various concerns regarding the publication of their personal photographs. Even those sharing all their personal photographs publicly make the initial selection of what is to be shared, thus creating strategies for handling their privacy concerns in online sharing. Such user boundary regulation is unable, however, to take into account the lasting effect on computer-mediated communication wrought by the technologies used and the business models enabling their usage. This ensures that individuals can never fully control what they have been posting online, which will certainly have an impact on the forms of information that are and will be available. Nevertheless, a fundamental difference exists between the possibilities for interaction provided by one service enabling user-generated content and the next: studying usage of one specific service, such as Kuvaboksi or Flickr, and making universal generalizations from the findings will not take into account the difference in architectures, business models and users applicable to other web services.

This activity has resulted in two publications (Lehmuskallio 2009; Lehmuskallio, Tamminen & Johnson 2009)

## **2.12 Privacy Policy Study**

During the spring 2009 we surveyed the privacy attitudes of 100 students enrolled in the introduction lecture course of usability at the Helsinki University of Technology. The attitudes were surveyed toward three different digital systems (the HUT online learning and study tool *Noppa*, a prototype mobile music service LN2 developed by Nokia and HUT, and Facebook). Privacy attitudes were tested against the differently phrased privacy policies of the systems and used three variables affecting the attitudes towards the gathering and use of the personal data entered in the systems: 1) the *benefit recipient* (friends or commercial entity gain), 2) *purposes* specification (greater good, personal or commercial) and 3) *temporal dimension* variable (indefinitely stored data vs. deletion of personal data after a month of cancellation of the account). The study has resulted in an interim internal analysis report, which will be re-written and published as a scientific publication.

## **2.13 Considerate refinement of mobile communication network traffic data**

Curiosity over other people's whereabouts, doings, and opinions has always been strong, for many different reasons. Merchants and marketers are interested in understanding customers and their preferences. Politicians are interested in people's opinions in a whole range of issues. And most people are interested in what just about everyone else do, say, and think—just look at fashion and trends. The methods for collecting this type of information are many, ranging from simply throwing a glimpse at the square outside the shop to assess the customer base of the day to formal polls and statistical analysis.

With broad adoption of information technology throughout society, there is a whole range of new information that can be used to gain an understanding of people's behavior. This information can typically be classified as byproducts of some other activity, including the use of cash and credit cards, automatic toll gates, cellular telephony, wireless networking, and just about everything related to the Internet. We have collaborated with the Solid and Consider8 project to provide methods and algorithms for creating and making use of patterns of human mobility and behavior. End users in this case refer to subscribers of mobile communication services such as mobile phone or mobile Internet customers.

For PRIMA, the overall goal has been to provide results that not only improve current means to meet an existing informational market need, but also do this while ensuring the privacy of mobile communication subscribers. The approach for accomplishing this has been to ensure the complete removal of identifiable information from the information collection. This provides users with true anonymization in contrast to pseudonomization, which is the prevailing method for handling personally identifiable traffic data.

## **2.14 Awareness support based on spoken dialogue recognition**

We have developed a meeting awareness tool, PrimaVista. PrimaVista builds on automatic, real-time, speaker-independent continuous speech recognition (ASR) supporting informal meetings that are held within a working unit of about 50 people. Instead of full interaction capture and retrieval, the goal of PrimaVista is to build informal awareness within the working unit by providing an easy overview of the discussion that takes place in meetings. Contrary to much of the work in the field,

these meetings were not meant for planning or decision-making but information dissemination and project presentations. PrimaVista meeting logs are mainly targeted at those colleagues not present in meetings. Gaining these overviews helps the co-workers to retain some aspects of the working relationship even when not being able to physically attend the meetings.

We have developed the software needed for the tool and used it in several meetings. Innovative solutions were needed for finding a way to segment the spoken utterances in a way that makes their real-time processing possible, and to develop visualizations that give a useful overview of the discussion both during the meeting (when the ASR processes are run in real time) and after it.

We have evaluated the system at various stages in varying levels of detail. It became clear that the system needs further work, which is on-going, and the final systematic evaluations will not be done before fixing some remaining issues. The most important further steps are either improving the quality of the speech recognition to reduce the amount of noise, or the improvement of the processing and visualizations so that only the key concepts are displayed to users. The current rich displays distract the user who focuses too much on incorrect recognitions and the combinations of words which, when not correct, may create false and distracting illusions.

In the context of PRIMA, the primary target of this study was to find a proper balance between informative meeting capture and support of awareness while not raising privacy concerns among the meeting participants or disturb the flow of the meeting. Our initial study before introducing the system showed that there were some concerns, but more a curiosity towards the system. In general, after having used the system a couple of times, participants did not have privacy concerns. This is certainly partly due to the current development state of the system, but can partly be attributed to a design that (by necessity) does not give away the identity of the participants unless they volunteer to do it themselves in, *e.g.*, written comments entered into the system.

This activity resulted in a conference paper (Heimonen *et al.* 2010), two manuscripts (Ovaska *et al.* 2010; Turunen *et al.* 2010), and the actual software. Evaluation results will be reported later after further development of the system.

## **2.15 Location, activities, and privacy**

For some groups of people, like bird watchers or teens, knowing what others are doing and where they are is important. This kind of information can be provided automatically in modern mobile telephones, or the user can “tweet” about it into a microblog web interface. What is the role of the activity and location information in small groups, and do the shared goals of the group affect what information is considered private? This topic is under investigation in collaboration with researchers at HIIT, from whom the bird watcher & teen data sets have been received for closer data analysis.

This activity resulted in an MSc thesis (Roine 2010).

### 3 Meta studies

The relatively long duration of the project has allowed us to conduct studies running across the collaborative research activities described above. While the aim with the collaborative studies has been to expand and open up the problem space of privacy research, the aim with the meta studies has been to find commonalities between the results from individual activities.

The meta studies have primarily been carried out through a series of project-internal workshops, three per year, during which results from collaborative research activities have been presented and analyzed. While the results from the different individual research activities indeed cover a broad spectrum of privacy issues, they hardly represent enough width and detail to allow for proper generalization, if that would ever be possible to achieve in the case of privacy. Rather, we have sought to identify clusters of similar perspectives among the different activities as well as intersections of different perspectives. Based on these results, our goal has been to come up with relevant privacy-related questions to ask in various IT and regulatory design situations, in contrast to answers to questions that soon become irrelevant due to the large variations in contexts of IT use.

#### 3.1 The Krusenberg privacy analysis framework

Acknowledging the great difficulty of succinctly defining privacy in a way that allows its direct use in IT requirements specification and design activities, we have experimented with an analytical framework for reinventing and redefining the concept in each use situation. Thus, the framework provides the means for situating privacy given a particular use case, thereby creating more tangible incarnations of the concept for use in design, development, and evaluations of specific technologies. The framework was outlined and first tested during a project-internal workshop at Krusenberg, Sweden, hence its name.

The Krusenberg framework stems from the work of Adele Clarke's method for *situational analysis*, which in turn builds on a collection of models of social analysis developed by Strauss in the 1970s referred to as *grounded theory*. Clarke's method extends grounded theory with postmodern insights from recent social theory not available to Strauss at the time. The model now includes previously non-accounted forms of action and actors topicalizing *non-human* actors (such as discursive formations and technologies). Privacy-related research involving users, especially in the field of HCI, usually do not take other privacy concerns than those emerged in user interviews into account. The suggested analytical framework inspect more fully the different stakeholders, the technology, and its context, and how they actually influence end-user privacy.

The analytical framework provides a number of categories for creating situational maps of privacy in relation to a particular technology.

- **Stakeholders of interest**, including individual, collective, and implicated/silent stakeholders.
- **Social relations and power structures**. Who is able to interact with whom and in which ways?
- **Discourse formations**. How do different stakeholders frame the use of specific applications?
- **Norms, regulations, and rules**. Which behavioral scripts do different stakeholders suggest?
- **History, traditions, persistence**. How has the application in question evolved, what traditions have emerged and which information is kept and why?
- **Interactional enablers**. How is interaction made possible and what kind of information is thereby suggested?

- **Communicational forms.** How do stakeholders interact with each other?
- **Business models.** How is continuous work compensated?
- **Non-human actants.** Which technologies are used to form and maintain the interaction, and which technologies are necessary for participation in a specific interaction?

By studying and analyzing a particular technology, prospective or existing, with regard to these categories, various interpretations of privacy may be sketched. These situated interpretations of privacy can then be used as more concrete concepts in requirements specifications, hypothesis formulations for studies, or evaluative criteria.

### 3.2 The what and how of privacy research

One of the meta-level discussions within PRIMA has concerned privacy research in HCI and its two genealogical roots: data protection and personal privacy research. In our study, we have set out to examine how privacy is understood within the two approaches and what they consist of. The aim has been to point out inherent problems hindering further advances of the field and suggesting how to overcome these challenges.

In this work, we recast the data protection research tradition to *the what approach to privacy research*, in which privacy is framed and understood mainly as a problem or obstacle for IT development. Within this approach, research questions are grounded on *a priori* value preferences (regarding what is private) from which basic constitutive elements of privacy can be analytically deduced. Within *the how approach*, expanded from personal privacy research, the emphasis is placed on the everyday practices, or, how people *do* privacy in different contexts.

The *what* approach has its historical roots in attempts to regulate personal information processing, dating back to the earliest debates on computers and privacy. At that time, computerization introduced an unprecedented informational power asymmetry, as information started to be collected, processed, stored, and distributed in novel ways. This posed challenges for regulating authorities in many countries (notable in the USA and Sweden, for example) leading to attempts to define private boundaries by identifying types, and legitimate uses, of personal information. This led to the creation of numerous regulative means, both binding and informative in their nature. New legal concepts (such as data controllers and data subjects), instruments (laws and principles of self-regulation), and overseeing institutions (authorities and governing bodies) were born. These results have slowly found their way into HCI, although their roots are many times forgotten in analyses of end-user privacy.

The *what* approach to privacy research encompass large variations. However, on a general level the different concepts and models encompassed by the approach rest on three pillars. First, they are normative in that they work as explicit guiding norms for personal information handling. Second, they are informational in that they define the types of personal information that privacy is all about. Finally, they are negative since they are based on restrictions on the handling or use of personal information.

To the contrary, the *how* approach takes a step back and asks how users come to manage and know about privacy in the first place. Having its roots in social sciences, this approach concerns how privacy as a phenomenon is constructed and achieved in people's everyday life as part of their empirical interactions, nowadays more and more mediated by IT. Within this approach, privacy is

understood as an important aspect of the constantly ongoing management of social relations in which boundaries delimiting private spaces are monitored and set, at least in terms of disclosure, identity, and temporal aspects of action. Herein, privacy is not found in the protection of particular types of personal information but in ongoing actions by which dynamic spheres of privacy are created, regulated, protected, and opened.

The *how* approach to privacy research is a tricky beast because it defines privacy as a relation rather than a state—it allows multiple interpretations of, and various ways to manage, privacy. Different relational configurations that create private spheres are possible. This is why it values the actors' point of view—privacy is what people make out of it. Simply, this standpoint gives researchers empirically grounded view to research many *privacies* instead of reducing it to one definition.

While the domain for both of these approaches is privacy research in HCI, the two are different according to almost every imaginable standard. The pressing question is how well these approaches contribute to the design of privacy in IT? Judging by the repeated privacy violations of service providers like Google and Facebook, for example, the answer ought to be: *not very well*.

Framing privacy research in HCI in terms of *what* and *how* approaches clearly illustrate a gap between privacy requirements and the appropriation of information technologies. On the one hand, we have a long tradition of normative studies of privacy, or how IT should behave and how it should be used when it is ready. On the other, we have a more empirically-based research tradition of how people appropriate IT while struggling to maintain, more or less successfully, their privacy. But none of the two approaches have proven effective in enhancing the current design practices and processes, at least not in any significant way, despite the suggestion of numerous design principles for privacy respectful design aiming at providing feedback to the design process itself. Also, when two extreme standpoints constitute the norm, other opportunities to bring privacy considerations into design are silenced, such as design-implementation life-cycle models.

To our knowledge, there are currently no systematic studies on how privacy could be part of design process all the way from the normative descriptions to the empirical evaluation with users. The PRIMA project is founded in a conviction that a multi-disciplinary perspective must be maintained in order to create useful understandings of the domain (Bylund *et al.* 2010). In combination, the *what* and the *how* approaches cover this disciplinary width, but the two are rarely combined to create the so much needed critical mass of different perspectives. Thus, with particular attention to research efforts in HCI, we argue that in order to create a broad understanding of individual privacy design challenges, every serious effort to design for privacy should include elements of both the *what* and the *how* approaches. In the PRIMA project, we have strived to bridge the two extremes by treating privacy as an *object of design* in its own right—a conceptual driver for defining the expectation of prospective users and a specific object of attention in our empirical studies of how the technology is brought to use, both combined in a single design process.

In a forthcoming paper (Tamminen, Bylund & Johnson 2010) , we provide a full analysis of the *what* and the *how* approaches, as well as a recommendations for how they should be combined to maximize their respective utility in privacy-aware IT design and development.

### 3.3 Privacy protection from a legal perspective

Grossly put, in research projects such as PRIMA, there are two ways of approaching legal privacy protection matters. One is *legalistic*, the other is *open-ended*. The legalistic approach aims at charting law in force and the more or less detailed regulatory issues that it encompasses (ways of expressing consent, for example). The task is broad, not least since it concerns national as well as international aspects and since privacy protection law blends into all kinds of surrounding areas such as human rights, labor law, consumer protection, national security *etc.* The open-ended approach strives to understand the basic concepts at issue, the interaction of law and information technology, different scholarly ways of approaching the notion of privacy, the rationale of privacy protection legislation, regulatory strategies, and so forth.

In PRIMA, emphasis has been on the open-ended approach, a kind of meta study of the legal issues. This is a natural consequence of the multi-disciplinary nature of the project. In other words, the legal sub-project has aimed at supporting PRIMA's social science- and ICT-oriented research activities both by clarifying how they relate to the legal discourse and by assisting particular collaborative efforts such as the study of privacy as a component of usability in ubiquitous computing. Both tasks have been dealt with in connection with PRIMA regular internal workshops and by separate work in between. Briefly put, there has been a constant watch-out for legal issues and complications in connection with the research activities and studies outlined above.

As for the meta study approach, it should also be mentioned that privacy protection is not the only area of law where ICT generates an interest in the re-shaping of traditional legal concepts and solutions and raises questions of how law interacts with ICT. Other examples can be found in intellectual property law, public administration law, criminal law, and media law. It is a matter of different opinions how far and how deep this development goes. It may very well be that traditional notions of the rule of law and of the way law is made and applied will change radically as the *information society* develops from snippets to wholes. The PRIMA project has paid attention to these matters (briefly, privacy in the framework of general ICT law), as documented in "ICT Law. A Kaleidoscope view" (Seipel 2010). The study sheds light on, among other things, two aspects of ICT in relation to law, viz. (a) the descriptive tasks and (b) the operative tasks. As for (a), a legal understanding of the regulated subject-matter must include a new understanding the new techno-social framework. And as for (b), legal regulation is not only an issue of regulation *of* ICT, but also an issue of regulation *through* ICT, i.e. using ICT as an instrument to reach legal goals.

### 3.4 E3: expectations, experience, and expiration

One fruitful meta level approach to privacy in IT is based on three temporally distinct phases: the *expectations* of privacy before the system use, the *experience* during the use of the system, and the afterwards *expiration* of trails generated during the use of the system.

The factors affecting the privacy expectations before the use include, for example, the different stakeholders related to the system (*e.g.*, different kinds of uses and institutions), the implicit or explicit *rules of the game* (a virtual world, a social network, a bluetooth game), the legal context (EULA, Privacy Policy, Informed Consent, technology, and country specific regulations) and the business models (freemium, premium, ad-supported, user data commodification logics) for the making the system economically feasible.

The factors affecting the experience during the use of a system relate to the different possibilities to regulate one's data (in relation to the service provider) and interaction between other users (other data subjects). The current systems vary widely in how the possibilities of these two central relations involved in the negotiation of personal privacy are implemented through explicit privacy preference options and interactional enables (chatting, picture sharing, saving conversations, etc.).

Finally the factors relating to the expiration of digital trails after the use of any given system relate to the ways in which these trails can be propagated and aggregated, how third parties have access to these or not (technically relating to cryptography and other means of data security against unwanted breaches by malevolent audiences such as hackers). The idea of *expiration* of digital trails is becoming more relevant especially considering the extent of (unsuspected or straightforwardly unrightfully performed) data mining relating to personal information available around the digital universe of today.

Within the PRIMA project, we have experimented with the E3 model as a heuristic to be used in quick evaluation of digital systems.

### **3.5 End user privacy management strategies**

The end user privacy management strategies in negotiating the boundaries of public and private data, identity disclosure techniques, and temporal dimensions related to personal data retention, all depend on the nature of the system used. However, it seems that from the individuals' viewpoint the different strategies and the problems encountered in these (resulting in a feeling of privacy violation) could be explained by the psychological Self Determination Theory (SDT). The theory predicts that in order to be fully mentally coherent and to maintain a sense of well-being over time, individuals need to experience and accomplish a sense of a) autonomy as a discreet and effective actor different from others in a given context, b) a competency of acting and predicting the outcome of their own actions and c) relating to other individuals in an autonomous and competent way.

Novel ICTs potentially disrupt all of these dimensions of an individual's self determination by disintegrating its three constitutive components: (a) the autonomy of a person using novel systems is in many cases shattered because of the complex technical skills needed in order to foresee the uses of the collected digital trails generated by collected data and IT use, (b) thus disrupting both the sense of control over one's own action and (c) the management of data release to one's social contacts (of individual or institutional origin). This framework is currently explored and a manuscript for a paper (Tamminen & Oulasvirta forthcoming) on the relation between the theoretical model of SDT and problems of privacy is in preparation.

### **3.6 Talk vs. practice (say-do) mismatch**

A relevant distinction in privacy studies concerns the operationalization of the concept. Most well known privacy studies, such as Westin's differentiation of people into three different categories (privacy "fundamentalist", "unconcerned", and "pragmatists") according to their attitudes towards novel technologies, have operated on normal polling techniques aimed at surveying the population opinion at large. These surveying techniques rely on verbalized questions and, as many have noted, always include a suspicion about their ecological validity. The problem of surveys is commonly stated as the "say-do" problem: people tend to respond to general survey questions in one way but behave differently when faced with the real situation.

We observed this mismatch in two separate studies of privacy, thus further questioning the validity of large scale surveys (at least in the form they are used today). First, in studies of Hot Potato we observed people who explicitly voiced no privacy concerns regarding the Bluetooth-enabled game while now wanting to participate personally due to reasons of feeling “uneasiness” about it. The talk about privacy on general level seems to be different from becoming an active user of potentially privacy sensitive technology in person. Second, in the replicated privacy study of the original Watcher and the Watched in a Swedish context (Friedman *et al.* 2008), we found a similar effect – people did not consider the video technology in itself problematic on general level. However, they were concerned about the potential privacy effects when they were to evaluate themselves as potential users of the technology.

The *say-do* problem in privacy studies is a side effect of techniques of opinion and attitude measurement and should be considered in any large-scale population sampling performed in the future.

## 4 Post PRIMA

Despite substantial progress during the past four years, the so much needed expansions of the privacy problem and solution spaces are not concluded with the end of the PRIMA project. On the contrary, it is quite likely that these spaces will never be fully explored. In part, this is due to the high complexity of the concept, but it is also due to the constant transformation of the interpretation of the concept resulting from the cultural, political, and technological development at large. As information technology is further developed, adopted, and appropriated, a continued expansion and exploration of the concept is therefore needed.

The multi-disciplinary stance of the PRIMA project has proven important for providing different perspectives of, and thus new insights into, privacy in relation to IT use. In retrospect, however, the project would have benefited from the representation of yet other disciplines, not least a business perspective. Several of the socio-legal-technical tradeoffs that we have encountered in our work have been difficult to assess due to a limited understanding of the resulting opportunities and challenges from a business perspective.

Another challenge related to the multi-disciplinary approach of PRIMA is related to finding a suitable method for combining the diverse methodologies, ontologies, and epistemologies of the different disciplines. In PRIMA, we have managed to cope with these differences mostly because of the small scale and generous timescale of the project. In larger constellations and situations where time is more pressing, more stringent methods for bridging these differences are most likely needed.

Finally, while we have pursued two parallel research tracks—the collaborative research activities for opening up the problem space, and the meta studies for relating the individual results to each other thus finding the right questions to ask—we have yet to touch upon the issue of how to explore, define, and redefine privacy in ever new contexts continually over time. How to manage this continuous process of rediscovery, how to find a balance between old truths and new insights of the ever changing phenomenon of privacy, is a question that we leave to be dealt with post PRIMA.

## 5 Results

In this section, we summarize tangible project results in terms of scientific publications (5.1), academic talks and appearances (5.2), efforts for public outreach (5.3), and software and systems (5.4). In Section 5.5, we list the range of research projects that we have collaborated with during the whole project period.

### 5.1 Scientific publications

#### 5.1.1 Academic conference and journal articles

- Bylund, M., Höök, K., and Pommeranz, A. 2008. Pieces of identity. In *Proceedings of the 5th Nordic Conference on Human-Computer interaction: Building Bridges* (Lund, Sweden, October 20 - 22, 2008). NordiCHI '08, vol. 358. ACM, New York, NY, 427-430.
- Bylund, M., Karlgren, J., Olsson, F., Sanches, P., and Arvidsson, C. 2008. Mirroring your web presence. In *Proceeding of the 2008 ACM Workshop on Search in Social Media* (Napa Valley, California, USA, October 30 - 30, 2008). SSM '08. ACM, New York, NY, 87-90.
- Friedman, B., Hook, K., Gill, B., Eidmar, L., Prien, C. S., and Severson, R. 2008. Personlig integritet: a comparative study of perceptions of privacy in public places in Sweden and the United States. In *Proceedings of the 5th Nordic Conference on Human-Computer interaction: Building Bridges* (Lund, Sweden, October 20 - 22, 2008). NordiCHI '08, vol. 358. ACM, New York, NY, 142-151.
- Heimonen, T., Ovaska, S., Turunen, M., Hakulinen, J., Rajaniemi, J. and Räihä, K. 2010. Visualization of Multi-sensory Meeting Information to Support Awareness. In *Proceedings of the 14th International Conference on Information Visualization (IV10)*, London, UK, July 2010, IEEE Press, 194-199.
- Johnson, M., Hyysalo, S. and Tamminen, S. In press. Virtuality of Virtual Worlds, or, what can we learn from play-acting horse-girls and marginalized developers. *Symbolic Interaction*.
- Lampinen, A., Tamminen, S. and Oulasvirta, A. 2009. All My People Right Here Right Now: Management of Group Co-Presence on a Social Networking Site. In *proceedings of the ACM 2009 international conference on Supporting group work*, ACM Press, New York. 281-290.
- Lehmuskallio, A., 2009. "A photo is not an extension of me, it's plain surface." – Views of users of a Web 2.0 photo-sharing site on photos and privacy. *SPIEL: Siegener Periodicum zur Internationalen Empirischen Literaturwissenschaft* 26 (2007) (2, Phenomena of Web 2.0 as agents of cultural change):271–289.
- Lehmuskallio, A., Tamminen, S., and Johnson, M., 2009. Managing Privacy on Social Network Sites. In *Medienamateure: Wie verändern Laien unsere visuelle Kultur?* Universität Siegen.
- Leino, J. and Räihä, K. 2007. Case amazon: ratings and reviews as part of recommendations. In *Proceedings of the 2007 ACM Conference on Recommender Systems* (Minneapolis, MN, USA, October 19 - 20, 2007). RecSys '07. ACM, New York, NY, 137-140.
- Leino, J. and Räihä, K. 2008. User Experiences and Impressions of Recommenders in Complex Information Environments. *IEEE Data Engineering Bulletin* 31, 2, 32–39.
- Ovaska, S. and Räihä, K. 2009. Teaching privacy with ubicomp scenarios in HCI classes. In *Proceedings of the 21st Annual Conference of the Australian Computer-Human interaction Special interest Group: Design: Open 24/7* (Melbourne, Australia, November 23 - 27, 2009). OZCHI '09, vol. 411. ACM, New York, NY, 105-112.

Ovaska, S., Leino, J. and Rähkä, K. 2008. Studying user interest in social media site. In *Proceedings of Workshop on "How Can HCI Improve Social Media Development"*, NordiCHI 2008, Lund, October 2008, 64–71.

Rähkä, K. and Ovaska, S. 2009. Faces of Privacy: Effect of Culture and Context. In *Proceedings of INTERACT 2009*, Part I, Uppsala, August 2009, 700–703. LNCS 5726, Springer.

### 5.1.2 Books and book chapters

Bylund, M., Johnson, M., Lehmuskallio, A., Seipel, P., and Tamminen, S. In press. Privacy Research through the Perspective of a Multidisciplinary Mash up. In *Nordisk årsbok i rättsinformatik 2006-2008*, S. Greenstein, Ed.

Seipel, P. 2006. Integritetsskydd och folkets röst (The Protection of Privacy and the People's Voice). In *Syntymästä kuolemaan, oikeudesta informaatioon. Ahti Saarenpää 60 vuotta*. Red. Aulis Aarnio *et al.* Helsinki: Suomalainen Lakimiesyhdistys.

Seipel, P., 2008. Alone no More. In *Festskrift till Marianne Levin*. Red. Ulf Bernitz *et al.* Stockholm: Norstedts Juridik.

Seipel, P. 2010. ICT Law. A Kaleidoscope view. In *Scandinavian Studies in Law*, Vol. 56. Editor Peter Wahlgren. Stockholm: Jure

Tamminen, S., Johnson, M. and Lehmuskallio, A. In press. Sosiaalinen media ja yksityisyys: uudet haasteet oikeustieteen, yhteiskuntatieteen ja tietotekniikan rajapinnoilla. In *Silmät auki sosiaaliseen mediaan*. Tietotekniikan liitto, Helsinki.

### 5.1.3 Academic dissertations

Arvidsson, C. 2008. Finding representations of people from web appearances, MSc thesis, Uppsala University.

Heikkilä, H. 2007. Usability of Ubiquitous Computing (in Finnish). MSc thesis, University of Tampere.

Kaartinen, H. Forthcoming. Presentations of the private self in Facebook. MSc thesis, Department of Sociology, University of Helsinki.

Leino, J. 2008. Searches and Recommendations: Item-finding in Complex Information Environments. MSc thesis in Interactive Technology, University of Tampere.

Neuvonen, T. 2009. Practices of Privacy: A User Perspective to Online Photograph Sharing. MSc thesis, Department of Sociology, University of Helsinki.

Roine, J. 2010. What do I do and where am I? Social presence through a microblog (in Finnish). MSc thesis in Interactive Technology, University of Tampere.

Tamminen, S. 2009. Toward Privacy Inspired Design. PhLic thesis, Department of Computer Science, Helsinki University of Technology.

Westerlund, A. 2009. Privacy and e-payment systems. LLM thesis, Stockholm University.

### 5.1.4 Unpublished manuscripts

Cottier, P., Salonen, T. and Padilla, I. 2008. *Pervasive Gaming and Privacy Seminar: A quantitative study of Hot Potato*. TKK / SICS / University of Helsinki.

Johnson, M., Tamminen, S. and Lehmuskallio, A. 2010. Interaction design for personal privacy in a virtual world.

- Nordström, M., Pyy, J. and Salo, L. 2007. *Qualitative analysis of Hot Potato*. TKK / SICS / University of Helsinki, T-121.5900.
- Ovaska, S., Hakulinen, J., Heimonen, T., Rähkä, K. and Turunen, M. 2010. User-Centered Design and Evaluation Challenges in Developing UbiComp Meeting Software.
- Seipel, P. 2006. PRIMA Activity Notes. Övervakningssamhället (The Surveillance Society). Seminar arranged by Institutet för framtidsstudier. (Övervakningssamhället 2006-12-06.doc). In Swedish).
- Seipel, P. 2007. PRIMA Activity Notes. PRIMA seminar on protection of privacy, 4 June 2007. Peter Seipel's contribution, Protection of privacy today and tomorrow (PRIMA sem 2007-06-04.doc).
- Seipel, P. 2008. PRIMA Activity Notes. Privacy in the Making Workshop 2008 (PRIMA workshop 2008.doc).
- Seipel, P. 2010. PRIMA Activity Notes. Contemporary Challenges to the Scope of the Right of Access to Information: Drawing the Line between the Public, the Private & the Personal – Is a Common Standard Emerging? Stockholm 7-8 May 2010 (Access to information Södertörn b 2010-05-07.doc).
- Tamminen, S., Bylund, M. and Johnson, M. 2010. The What and How of Privacy Research.
- Turunen, M., Hakulinen, J., Heimonen, T., Rajaniemi, J., Ovaska, S. and Rähkä, K. 2010. PrimaVista – A System for On-line Detection and Distributed Visualization of Discussion Topics from Spontaneous Spoken Conversations.

## 5.2 Talks and appearances (academic)

- NORDUnet 2006 conference, September 28, 2006. Markus Bylund presented the newly started PRIMA project.
- Seipel, P, UbiComp – ett nytt hot mot vår integritet (UbiComp – a new threat to privacy). Lecture at the Swedish Society for IT and Law 20 September 2007. (ADBJ ubiComp 2007-09-20.doc). In Swedish.
- NORDUnet 2008 conference, April 10, 2008. Sakari Tamminen presented the collaboration within the PRIMA project.
- Medienamateure: Wie verändern Laien unsere visuelle Kultur?, Universität Siegen, June 5-7, 2008, Asko Lehmuskallio talks about Managing Privacy on Social Network Sites.
- Seipel, P, Understanding the dynamics of privacy protection. Keynote at “e-Stockholm ‘08. IT Regulations and Policies. From Theory into Practice. (Keynote Privacy Dynamics 2008.doc).
- Digital World Research Center, University of Surrey, June 23, 2009, Asko Lehmuskallio talks about Non-professional Picture Practices. A media-anthropological study of the increasing role of pictures in various non-professional activities.
- OtaSizzle Plenary, Elisa, November 2, 2009. Asko Lehmuskallio talks about Social Publicity and Privacy.
- Imagine Goffman –Nordic Network for Visual Studies, Nordic House: University of Reykjavik, November 26, 2009, Asko Lehmuskallio talks about the agency of images. Online photo-sharing and interpersonal boundary regulation.
- Abschlussveranstaltung des DFG-Graduiertenkollegs “Bild-Körper-Medium. Eine anthropologische Perspektive”, Karlsruhe University of Arts and Design, November 29, 2009. Asko Lehmuskallio

talks about Zu Bildpraktiken und Bildwissenschaften im Umgang mit bildgenerierenden Hybriden.

PRIMA Activity Notes. Mer av samma men inte samma samma (More of the same but not the same same). Lecture at the Norwegian Center for Legal Informatics (SERI) 2010-03-19 (Mer av samma SERI-jubileum.doc). In Swedish.

## 5.3 Public outreach

### 5.3.1 Talks and participation in public debates

Seminar at IVA, September 4, 2008. Markus Bylund and Peter Sipel participated in a panel discussion about privacy and surveillance "Integritet--trygghet eller övervakning?" organized by IVA.

Almedalen, June 30, 2009. Markus Bylund participated in a debate about privacy organized by the Swedish IT & Telecom Industries and Computer Sweden.

Internetdagarna'09, November 3, 2009. Markus Bylund participated in a debate concerning end-user privacy "Användarnas integritet".

### 5.3.2 Op-eds articles

Seipel, P., 2006. Tre råd för en bra IT-politik. I: Computer Sweden 2006-11-10 (debattartikel).

Seipel, P. 2007. IT och rättssäkerheten. I: Computer Sweden 2007-12-03 (debattartikel).

Bylund, M. and Seipel, P., 2008. Är FRA-lagen ens möjlig? Svenska Dagbladet Brännpunkt (internet) 2008-07-08.

Klamberg, M., Nilsson, M., Petersson, A., Seipel, P., Flyghed, J., Magnusson Sjöberg, Cecilia and Karlgren, Jussi and Bylund, Markus and Palmås, Karl and Kullenberg, Christopher and Ström, Pär and Thorburn, Daniel and Westerholm, Johan 2008. FRA kartlägger vanliga svenskar. DN Debatt den 2008-09-03

### 5.3.3 Government reports

Kirchberger, C. and Seipel, P. 2007. Integritetsskydd – vad tycker folket? Ett planeringsunderlag. In *Skyddet för den personliga integriteten. Kartläggning och analys. Del 2*, SOU 2007:22.

Tsunamibanden (The Tsunami tapes). Swedish Government Official Reports (SOU 2007:44). In Swedish (P Seipel engaged as expert).

## 5.4 Software and systems

### 5.4.1 PrimaVista

A System for On-line Detection and Distributed Visualization of Discussion Topics from Spontaneous Spoken Conversations and Other Sensory Information. Intended to support awareness and meeting capture in a way that is unobtrusive and does not cause privacy concerns in meeting participants. Software is still under development, but records of its past use (showing the interface) are available at <http://prima.cs.uta.fi/login.php>

### 5.4.2 Hot Potato

Hot Potato is a pervasive game design intended for Bluetooth-enabled cell phones. The game design of HotPotato encourages players to search for people, known or unknown, with Bluetooth-enabled cell phones. Once such an individual is found, the player must follow her at close distance in order to attach a potato. After this the player has the option of following the individual with the potato long

enough for the potato to cool down so that it can be reclaimed. The Hot Potato game was originally developed for Sony Ericsson P900 smart phones, with a server part written in Java. For the purpose of being used in PRIMA studies, it was ported to run on JavaME enabled handsets, primarily Sony Ericsson K800i. The source code is available upon request (bylund@sics.se). However, due to the rapid development of handset APIs, it is unlikely that the game will run on later handsets without modification.

### 5.4.3 Pieces of Identity

The Pieces of Identity system was implemented for the purpose of being deployed during the inaugural event of the Mobile Life centre ([www.mobilelifecentre.org](http://www.mobilelifecentre.org)) in August 2007. The system was an integral part of the event, and *vice versa*. Thus, it could only run for real once. The system consisted of two different RFID sub-systems: one with short-range tags placed in mobile jewelry puzzle pieces handed out as gifts to the guests of the event, the other with long-range tags hidden in the name tags of the guests. A database part stored personal information about the guests retrieved from web mining, while clients for large-screen presentation and user interaction were implemented in Java and Flash.

The implementation and deployment of the system is further described in a conference publication (Bylund, Höök & Pommeranz 2008).

### 5.4.4 Mirroring Digital Identities

The Digital Identity Mirror is a tool to support user awareness, to allow users to track the image they project on the net, to support them to uphold the identities they wish to maintain, to enable them to identify and counter incorrect, inadvertent, or even unwanted facets of their personality made visible through their actions. A prototype implementation of the system was implemented in order to evaluate the feasibility of automatic *identity feature extraction* and exploring how to create *compound facets of identities*.

The implementation is further described in a conference publication (Bylund *et al.* 2008) and an MSc thesis (Arvidsson 2008).

## 5.5 Collaborating projects

### 5.5.1 IPerG

**Full name:** Integrated Project on Pervasive Gaming

**Grant holder:** SICS

**Funding agency:** EU (FP6-004457)

### 5.5.2 Mobile Life centre

**Full name:** Mobile Life VINN Excellence centre

**Grant holder:** Stockholm University

**Funding agency:** VINNOVA

### 5.5.3 Solid

**Full name:** Solid: Secure and robust personal information-based ICT services

**Grant holder:** SICS

**Funding agency:** VINNOVA (P28524-1)

#### **5.5.4 COMPANIONS**

**Full name:** Intelligent, Persistent, Personalized Multimodal Interfaces to the Internet

**Grant holder:** University of Tampere (project coordinated by University of Sheffield)

**Funding agency:** EU (FP6-IST-034434)

#### **5.5.5 Appropriation for sabbatical**

**Full name:** Using Eyegaze for Analyzing, Improving and Facilitating Interaction with Computers

**Grant holder:** University of Tampere

**Funding agency:** Academy of Finland

#### **5.5.6 Modeling and Simulating Changing Needs of Consumers**

**Full name:** Modeling and Simulating Changing Needs of Consumers

**Grant holder:** National Consumer Research Centre

**Funding agency:** Tekes (the Finnish Funding Agency for Technology and Innovation)

#### **5.5.7 End-User Preferences in Product Concept Development**

**Full name:** End-User Preferences in Product Concept Development

**Grant holder:** HIIT Helsinki Institute for Information Technology

**Funding agency:** Oy Keskuslaboratorio - Centrallaboratorium Ab

#### **5.5.8 User Driven Open Innovation Booster**

**Full name:** User Driven Open Innovation Booster

**Grant holder:** HIIT Helsinki Institute for Information Technology

**Funding agency:** Tekes (the Finnish Funding Agency for Technology and Innovation)

#### **5.5.9 Extreme Design**

**Full name:** Extreme Design

**Grant holder:** Soberit Software and Business Engineering Institute (+HIIT)

**Funding agency:** Tekes (the Finnish Funding Agency for Technology and Innovation)

#### **5.5.10 MCM**

**Full name:** Mobile City Moments

**Grant holder:** HIIT

**Funding agency:** EUREKA Celtic

#### **5.5.11 Privacy and Publicity**

**Full name:** Privacy and Publicity

**Grant holder:** HIIT

**Funding agency:** Emil Aaltonen Fund