



NSF/EU Workshop on Future Directions in Pervasive Computing and Social Networking for Emerging Applications

[Type the document subtitle]

The NSF/EU sponsored workshop on Future Directions in Pervasive Computing and Social Networking for Emerging Applications was held in Mannheim, Germany on March 29, 2010. The workshop was attended by 26 scientists from the US and the EU. The workshop included presentations from US and EU scientists, an invited talk from a scientist from Facebook, and three breakout sessions. At the end of the breakout sessions, the group leaders of each session summarized and presented the highlights of the discussions.

Mohan Kumar and Marco Conti
1/18/2011

Table of Contents

Organizing Committee	...3
Introduction	...4
Executive Summary	...6
Grand Challenges	...7
Recommendations to the NSF and the European Commission	...9
Additional Recommendations to the NSF	...11
Breakout Sessions	...12
Social Networking Group	...13
Context Group	...16
Security and Privacy Group	...20
Infrastructure and Implementation	...24
Education	...25
Applications	...26

NSF/EU Workshop on Future Directions in Pervasive Computing and Social Networking for Emerging Applications

Preliminary Draft Report

Prepared by Mohan Kumar and Marco Conti (PIs)

Organizing Committee

Mohan Kumar (PI, US), UT Arlington, USA
Marco Conti (PI, EU), IIT, CNR, Italy
Krishna Kant, Program Director, NSF
Sajal Das, Program Director, NSF
Fabrizio Sestini, EU Project Officer

List of Participants

US

Ramon Caceres, AT&T
Kevin Fu, UMass Amherst
Mario Gerla, University of California, Los Angeles
Adriana Iamnitchi, University of South Florida
Christine Julien, University of Texas at Austin
Archan Misra, Telecordia
Klara Nahrstedt, University of Illinois, Urbana Champaign
Mahadev Satyanarayanan, Carnegie Mellon University
Gergely Zaruba, UT Arlington

EU

Christian Becker, University of Mannheim
Nigel Davies, Lancaster University
Peter Druschel, Max Planck Institute for Software Systems
Afonso Ferreira, CNRS
Valérie Issarny, INRIA
Marc Langheinrich, University of Lugano
Paul Lukowicz, University of Passau
Martin May, Technicolor Paris Research Center
Andrea Passarella, IIT-CNR
Bernhard Plattner, ETH Zurich
George Roussos, University of London
Albrecht Schmidt, University of Duisburg-Essen

Introduction

The emerging pervasive and social networks are drastically changing the (information) society. First of all, we are experiencing a **convergence between the cyber/virtual and physical worlds** -- the physical world is increasingly saturated with computing and communication entities that interact among them and with the users; in this environment, virtually everything can source information and respond to appropriate stimuli.

The convergent cyber/physical world will be **content-centric**, where content generated in the physical space is immediately transferred to the cyber space (e.g., multimodal sensing), and cyber outcomes have immediate impact on physical space. **Humans are at the core** of this convergence; each person has several (mobile) devices through which he/she can interact with the virtual world thus linking the physical world and the electronic world of user devices. Furthermore, **content is increasingly generated in a participatory fashion by the users themselves** (following the *User-Generated Content* model), who become content producers and consumers at the same time, and user devices are becoming main content repositories (in addition to content being available in fixed user devices, as well as being hosted and indexed on Internet servers or in P2P overlays as we see today). Device mobility (by expanding the Internet edges) is providing an additional spatial dimension to the creation, acquisition and dissemination of content. Much of this content will be **spatial and temporal in nature**, being referenced to a particular location and of value only around a particular point in time before becoming superfluous or less relevant. Moreover, such content may only be relevant to a small group of users, as commonly described by the phenomenon of the "long tail". **Context and social-awareness** will thus be important aspects in content characterization.

In this scenario, where information is increasingly generated by the users and/or available on the users' devices, **social networks** will play a very important role in distributing content in the network on a massive scale by establishing overlays that link together the physical world (the users) and/or the cyber world (the users' devices).

This increasing content availability has the potential to provide a **range of novel applications** from economics (e.g., new type of business based on content distribution), social life (e.g., sharing feedback about services) to entertainment (e.g., events or travel information). However, this requires novel approaches to effectively manage and acquire the ever-increasing amounts of content.

Social networking is growing rapidly in terms of applications, popularity and challenges. In parallel, pervasive computing research and development in the last decade has led to a number of applications. Ubiquitous presence of smart cell phones carried by gregarious individuals is leading to new applications that exploit the connectivity provided by human social networks and pervasive accessibility and availability to resources/services. Recognizing the need for encouraging collaborative research among US and EU scientists in this exciting area with potential for large number of diverse emerging applications, the US National Science Foundation and the EU Research Board sponsored a 1-day Workshop.

The participants included leading researchers from the US and EU. The Workshop is timely and appropriate as the two groups (US and EU) have complementary physical environments - from a social networking perspective, Europe has high population density, highly urban landscape, whereas the US is characterized by large distances and density variations. Moreover, sociological/behavioral/cultural differences as well as differences in wireless communications exist, thus providing a very broad set of user scenarios, critical for studying a variety of user and application cases.

Executive Summary

The participants of the workshop were charged with the task of identifying the grand challenges in pervasive social networking. In view of the growing importance and popularity of pervasive networks on one hand and social networking on the other, the National Science Foundation, USA and the European Research Commission cosponsored this workshop. The workshop was split into 3 breakout sessions – social networking, context-aware services, and security and privacy. The outcome of the breakout sessions is summarized in the set of research challenges and recommendations to the NSF.

The workshop participants highly recommend new initiatives from the NSF and the EU to support research in pervasive computing and social networking. The US and EU scientists have complementary physical environments - from the social networking perspectives Europe has high population density and a highly urban landscape, whereas the US is characterized by large distances and density variations. Moreover, sociological/behavioral/cultural differences as well as differences in wireless communications exist, thus providing a very broad set of user scenarios, critical for studying a variety of user and application cases. Social networks in the two continents exhibit different characteristics that will need to be incorporated in emerging pervasive social networks.

New guidelines must be established for exchange of data from online social networks between the EU and US. Collaborative research is expected to lead to: i) better understanding of the challenging problems associated with pervasive computing and social networking; ii) large scale gathering of data for multidisciplinary research; and iii) development of new applications and improvement of existing ones. Long-term collaboration with the EU groups will lead to: i) sharing of resources and data; ii) large scale experiments; and iii) exchange visits of scientists as well as students, between the US and EU countries.

Grand Challenges

Grand Challenge 1

Understand and characterize the inter-relation between real-world social structures and online social networks.

Understanding real world, online communities and their relationship require collaboration among interdisciplinary researchers. There is a need to create new cooperative tools for distributed collection, analysis, management and control. Interdisciplinary research will lead to better understanding of the relationship between information sharing and user privacy, and creation of models for privacy and trust. It is also necessary to establish guidelines for data collection, storage and usage of scientific research outcomes and to identify anonymization and privacy-preserving methods. US and EU collaboration will benefit by merging different viewpoints resulting from culture and population density diversities.

Grand Challenge 2

New paradigms for context determination

New policies and guidelines are needed for gathering context data in social networks. Methodologies for opportunistic collection of context data are needed to utilize opportunistic sensing through user devices. Determination of group contexts rather than individual context will be critical to new applications that will utilize social networks. At the same time, group contexts inferred from social networks can be utilized to determine individual contexts. Investigations into scalability issues for gathering context through a large number of devices/sensors will be necessary. Furthermore, context determination in the presence of a large number of individuals is a new dimension to research in context-aware computing. Algorithms for context recognition by analogy and methods for determining “hard to know” contexts, and for predicting complex behavior of entities and users will be essential to emerging applications. Addressing context uncertainty in social networking and ensuring the quality of context with the ensuing increase in scale are also significant challenges.

Grand Challenge 3

Finding the balance between conflicting pairs of issues in the specific application domain

In practice, security and performance, privacy and usability, information quality and delay have conflicting requirements and goals. It is critical to determine the balance to satisfy both points of view. We must define degrees of security, privacy, quality, usability, and performance and perform investigative fundamental research to determine metrics, models and trade-offs for defining the relationships between security and performance and privacy and usability. Oftentimes, cultural backgrounds, psychology, geographic locations/barriers and government policies and laws play critical roles. Methods for scalable solutions will need to be developed. Proactive approaches to solving security and privacy problems before rollout are critical to the success of this research.

Grand Challenge 4

Infrastructure, Experimentation, and Multidisciplinary Research and Education

Study of pervasive social networking requires large-scale experimental facilities that involve people of all ages from diverse cultural and professional backgrounds, heterogeneous devices, and dynamic contexts. It is critical to create appropriate infrastructure for experimentation. Standards are necessary for open online social networks, deployment for experiments and addressing privacy and security issues for data collection. Establishment of policies and guidelines (contractual frameworks) for collecting, accessing, sharing and storing of anonymized data securely is required. Certain data should be made available to the public. Approvals from IRB or similar bodies will be needed.

Creating new infrastructures for context-enabled applications supporting large-scale, very diverse context for individuals and groups will be a challenge. New methods and algorithms for deploying and utilizing social infrastructure “just-in-time” to aid applications will need to be developed. New methodologies for data collection in large, complex environments are needed to support diverse contexts for individuals and groups. Development of appropriate system metrics, benchmarks and methods to create repeatable low cost experiments will be necessary.

Multidisciplinary education and research is imperative to the success of pervasive social networks. As people are an inherent part of socio-technical systems, it will be critical to understand people, their contexts, their privacy and security concerns, their social behaviors, and their applications. Psychology of trust in transient social networks will require collaboration with sociologists and psychologists. Context knowledge from domain experts can be utilized for allocation of resources, determining the relationships between security and performance, and privacy and usability. Multidisciplinary collaboration will lead to educating people better in terms of privacy and security, economic incentives and situations, and cost versus quality of service. Within this domain, we must educate students to develop new algorithms and designs for pervasive social computing, develop safe and secure software, and to create new applications. Such education must start at entry level and continue with advanced level courses. It is critical to develop multidisciplinary curriculum for social computing and involve domain experts. Novel education based platforms for participatory games and sensing as a citizenship tool are necessary as every person holding a device performs some kind of sensing and collaboration by virtue of their context - geographic, social, and connectedness. New models to simulate and emulate social networks of large diverse groups would be required to enable research.

Recommendations to the National Science Foundation and European Commission

1. Encourage and support research on the following topics:

- *Interdisciplinary research for modeling real-world and online communities.*
- *New methodologies for determining and understanding context in ubiquitous social networking environments comprising large numbers of users and user devices.*
- *Investigations to find the balance between security and performance, and privacy and usability in pervasive social networks.*
- *Novel business policies and economic models that encourage users to contribute to social networking and participatory sensing.*
- *New mechanisms for application interfaces and context processing for new applications in social networks replete with pervasive devices and services.*
- *Facilitate and nurture multidisciplinary research among computer scientists, sociologists, psychologists and other domain experts to better understand the complex nature of social networks and their interaction with pervasive computing.*
- *New directives for enhancing availability and accessibility of infrastructure devices and sensors.*
- *Creation of multi-institutional experimental test beds, including heterogeneous devices with involvement of users from different walks of life.*

The above research will lead to the development of new applications, better utilization of resources and superior services to the people. Mechanisms to incentivize multidisciplinary research on one hand and collaboration with EU scientists on the other should be put in place at the earliest to foster result-oriented collaborative research. Furthermore, this kind of research should be geared to exploit the knowledge of domain experts (for example social scientists, psychologists) in developing new models and tools for understanding and characterizing on-line communities. Supplemental grants should be available to encourage collaborative research, infrastructure and data sharing and administer student exchange programs. It is imperative to create opportunities for collaborative research among US/EU scientists to exploit unique capabilities of partners.

Construction of a multi-institutional (including universities in the EU) test bed will be very useful to create new applications, carry out performance studies, and develop new policies. Availability of anonymized data to the public will encourage widespread participation, data collection and eventually better products.

2. Facilitate US/EU Collaborative Research

- New guidelines must be established for sharing existing and new infrastructure and for gathering experimental data.
- Existing programs such as PIRE and others through OISE should be augmented with new programs for pervasive social networking.

Additional recommendation for the National Science Foundation

New approaches to educating K-12 students and undergraduates on the importance, dangers and opportunities of participatory sensing and social networking should also be encouraged. Development of multidisciplinary courses leading to the better understanding of pervasive social computing and its applications should be supported. Support for developing new courses to educate undergraduates on how to utilize pervasive and social networks to develop new applications.

Breakout sessions

1. Social Networking

2. Security and Privacy

3. Context

Social Networking Group

Group Leaders

Ramon Caceres
Peter Druschel

Participants

Marco Conti
Sajal Das
Afonso Ferreira
Adriana Iamnitchi
Martin May
Andrea Passarella
George Roussos
Fabrizio Sestini

The Vision

In the convergent physical/cyber world, where being swamped by content is a likely reality, and information is increasingly generated by the users and/or is available on the users' devices, **human and online social networks** have a very important role for accessing and fusing the massive scale of content that is circulating in the network/society. Human social networks exhibit remarkable dynamism and structural properties that may significantly affect the quality of information (i.e., trust and reputation, relevance, reliability, etc.) and the way information may circulate -- it is conjectured necessary to traverse only a small number of human social relationships in order to connect *any* pair of people resulting in the "small world concept". Furthermore, social anthropology shows that human relationships have a hierarchical structure and, on average, an individual has up to 150 active social relationships, i.e., the Dunbar number.

In order to translate human relationships in the electronic world, on one hand we equip electronic devices with functionalities to enable humans to effectively handle and share large amount of information. On the other hand, by extending human social network with on-line social networks we possibly modify their structure/organization, thus affecting the way humans share the information in the physical world.

Human relationships can be exploited in the virtual world at different levels. Firstly, in a **physical** sense, relations can be defined between local devices carried by users by exploiting on physical interactions among users. This notion of social networks can be applied, for example, in the study of public health and epidemiology. Secondly, there is a **virtual** sense, in which a social network is defined by the common relevance of information to participants or their e-interactions. These participants are not necessarily physically co-located but are tied by common interests or behaviour. In summary, we identify the following types of social networks.

1. Physical (electronic) social network of users' devices, which we can refer to as *on-the-move social network* as they represent the network of contacts among the users' devices while users move in the physical space.
2. Virtual (electronic) social networks of users, which we can refer to as the *on-line social network*, where the interactions among users occur in the cyber world using any virtual connection (e.g., fixed and mobile Internet, etc.) without requiring physical proximity.

Both these definitions of social networks are useful because the *physical* notion can be exploited for fast and effective circulation of data with spatial temporal value; while the *virtual* notion can be exploited for content provision and personalised context, such as by sharing information of mutual relevance. It is worth noting that experimental results indicate that physical social networks can extend the connectivity of virtual social networks, by reducing the social distance among people because human mobility creates contact opportunities among users that are not part of an online social community.

Embedded in both the *physical* and *virtual* notions of electronic social networks are fundamental needs and new opportunities to provide **security, trust and privacy**. Security has particular relevance to preserving the integrity of physical interactions while trust is of relevance to the acquisition and dissemination of appropriate content. Establishing trust and security for an interaction between *a priori* unknown peers is a challenging issue. However, social network structures offer a basis to enhance trust and security provision by capitalising on existing social links. **Privacy** may be not perceived with various degrees of severity among people belonging to a social network, depending on the quality of the social relationship.

To summarize, the convergence of pervasive computing and social networking will lead to a convergence between virtual and real worlds where **human and on-line social networks will interact** to provide effective ways for handling and sharing large and increasing amount of information. This will have major impacts at different levels: technological, social, economical, governance, etc,

- Technological: new social computing and communication paradigms can be devised by exploiting social infrastructures and human in the loop;
- Social: human social communities will be enlarged/modified by the introduction of (mobile) on line social networks;
- Economic: emergence of new markets; see, for example, the possibility to exploit the long tail effect for creation of new markets.
- Governance: less control/more democracy on information creation and distribution through virtual social networks.

Grand Challenges

The group identified two grand challenges:

- ***Understand and characterize the inter-relation between real-world social structures and online social networks***
- ***Use pervasive social computing as a global tool for collaboration and awareness, a new citizenship for better society***

Fundamental Research

Following fundamental research problems are critical to addressing the grand challenges:

- Understand and model real-world & online communities (needs interdisciplinary collaboration)
 - Find novel ways for computers to model / emulate / simulate social dynamics of large groups
 - Establish guidelines for collection and use of data from online social networks for scientific research purposes, e.g., anonymization, privacy-preserving data mining.
- Understand and model security and privacy
 - Resolve tension between sharing and privacy
 - Create understandable and usable models of privacy and trust
- Create cooperative tools for distributed decision-making, e.g., collection, management, processing
- Enable social networking on a global scale
- Develop platforms for participatory games and sensing as a citizenship tool
- Business and economic models for pervasive digital society based on social networks
- Use pervasive social computing for learning

To support the above fundamental research we need a coordinated interdisciplinary research effort:

- Need to involve other disciplines now, e.g., sociologists, anthropologists, etc.
- Need to create incentives for multidisciplinary work, e.g., improve recognition of such work
- Develop a multidisciplinary curriculum for social computing

Context Group

Group Leaders

M. Satyanarayanan

Nigel Davies

Participants

Christian Becker

Mario Gerla

Christine Julien

Mohan Kumar

Paul Lukowicz

Albrecht Schmidt

Gergely Zaruba

Vision

Context is key to a number of challenges in pervasive computing and social networking. Acquiring context data from appropriate sources in time and space, leads to a better understanding of the underlying situation. Context knowledge can be utilized to provide better services, utilize resources efficiently and to alleviate information overload. To make efficient use of context and to deploy advanced applications that rely on it, better context modeling and reasoning methodologies must be developed through knowledge gained from extensive experimental studies. Context data from sensors and devices in real situations over large periods of time and under a multitude of situations must be gathered to understand the interrelations between users' social behavior and their usage of cyber resources.

Participatory sensing in social environments will lead to the acquisition of critical context data useful for establishing trust, managing resources, and service provisioning. Data from pervasive sensors will be acquired on a continuous basis to understand various types of contexts, social context is especially expected to play a significant role in provisioning trusted and autonomous, but unobtrusive, services and information to users. Furthermore, context knowledge will be exploited for better utilization of resources, QoS provisioning, and enhancing human quality of life.

Grand Challenges

The group identified three grand challenges that are critical to pervasive social networks:

- ***New paradigms for context determination***
- ***Need to establish policy for collection of context data (privacy vs. context sharing)***
- ***New infrastructure for context enabled applications***

In pervasive systems influenced by social networks, the collection of context data can be quite complex. First, context is hard to determine as it may be dependent on such hard to measure events as users' mood, activity, etc. Also there is a need to establish policies for collection of context data. Second, group context determination is a function of group membership, social activities, inter-relationships, and other factors. Third, currently there are no established mechanisms for large-scale context gathering. Fourth, the environment changes dynamically resulting in large volumes of data.

New mechanisms are needed for collection of context data, e.g., opportunistic and subconscious acquisition of context information. Also policies must be formulated to preserve privacy. This difficult problem is further complicated by group/social issues --- e.g. what is acceptable to share in a group of close friends may have to be modified temporarily if an outsider joins the group.

Predicting and recognizing hard to determine context is a challenge. Context determination and adaptation in dynamically changing environments requires distributed processing mechanisms, for example context recognition by analogy techniques such as similarity matching in a distributed context database. Understanding complex context aware applications and adapting to context in large systems are unknown territories.

To support applications associated with large scale, very diverse context, there is a need for new infrastructures. At the moment, there is a dearth of infrastructure that can support very large and diverse contexts and support individual as well as group dynamics in a scalable manner.

Fundamental Research

The following principal research problems are identified:

- Modeling and understanding contexts
- Preserving privacy while optimizing collection/storage/search efficiency
- Understanding context sharing and privacy
- Developing a comprehensive taxonomy of context and discovery mechanisms
- Programming and architectural frameworks
- Science and Engineering of context systems
- Socio-technical systems

While context modeling and understanding have been investigated in the past, context in social networks has new challenges. New methods must be investigated for gathering context data in social networks. Dealing with context uncertainty and predicting complex behavior in social networking systems are hard, due to increased ambiguities associated with decision making in scenarios or applications involving a group rather than individuals. Also, environmental or cyber context (that is, what computing and communication resources are available in the neighborhood), and their relationship with social context is important. **The efficiency of context determination mechanisms may be dependent on the density of people or devices.**

Ensuring quality of context data gathering, processing, and determination, despite the rapid increase in quantity of data, requires resources for storing, computation and programming. It is debatable whether we should employ cloud computing methods or some variations. Context sharing should be context – aware for privacy reasons. For example, a user may be willing to share their location information with everyone at 9-5 pm, but only with a certain social group at 5-7pm.

We need to formalize systems by creating appropriate systems metrics and benchmarks. To achieve this it is necessary to create repeatable, low-cost experiments that can be tested under varying conditions. Furthermore, to reduce cost and manpower requirements it is imperative to minimize user studies.

Understanding people, their contexts and applications is important as people are inherent part of the pervasive social network. Understanding systems to be created and the way people use them and their applications are critical to developing socio-technical systems. Ensuring acceptance of the systems by domain experts is necessary to prevent bad premature implementations. Understanding the applicability of context for resource (cyber as well as non-cyber) management, for example, for environmental sustainability is also an important research challenge. In context-aware systems, it should be possible to help users understand what their context-aware system just did and why. The adaptive behaviors of a system must be traceable.

Security and Privacy Group

Group Leaders

Klara Nahrstedt
Bernhard Plattner

Participants:

Valerie Issarny
Krishna Kant
Marc Langheinrich
Archan Misra

Vision

Communal Sensing: As we are moving towards communal sensing and participatory sensing with the pervasive social networking, security and privacy are becoming more important than ever. The value of the personal data that are being sensed is in the eye of the beholder. Incidental data being sensed can be valued by somebody else, hence we will need to have a synthesis and analysis of incidental data from **multiple users**. Combining sensed data from many mobile users in the communal sensing can be very powerful, but also *scary since one can infer from sensed data not only location, but also how long one stays at one place, whom a person met, where we might be going, and other contextual and personal information*.

We need security and privacy algorithms, protocols that protect the sensed communal data **against unwanted collection and distribution of personal information**. Hence, *tuning knobs* for adapting the levels of privacy and security will be of great importance. **Adaptive and personalized privacy and security algorithms** within our cell-phones will be necessary. It is very important to stress that in this space there is no 0 or 1 privacy and/or security approach as it is considered in the traditional security area. For example, an elderly person might want to give up privacy to a certain organization/other person/group in exchange for safety and protection. On the other hand, a middle-aged person might not wish to have all his/her steps sensed and reported to a certain organization within his/her consent.

We envision that algorithms that combine both **security and privacy issues will ensure reliability and validity of sensed data**. Note that, for example, *integrity of data and privacy of data might be/are orthogonal* to each other (since for privacy reason, data might be anonymized, fuzzified, changed through mathematical formulas), hence one needs to carefully consider when to change data for anonymity reason and what final data is needed for integrity check. Combining security/privacy approaches with data delivery can affect the **performance and energy usage** of the data/device. Hence, we must be mindful to design future integrated security and privacy approaches that deliver the sensed data in time-sensitive and energy aware manner. For example, the installed authentication mechanism must be energy efficient.

Ambient Context: The advanced capability of the future will be the ambient context of mobile devices around us which allows for localized correlation of context of multiple individuals, localized data management and retrieval, easy indoor location determination, real-time local information mining, and social tomography.

Again, as we aim towards future ambient context and future intelligent environments and monitoring in health care, environmental protection, and other applications, **privacy and trust** in the provided information must be **integral part of the application design**. Applications will struggle with several problems: (a) there is no centralized authority when group of mobile users with their devices meet, i.e., the authenticity of identity is difficult to achieve, (b) pseudonymity may be broken, users may run into each other, devices/users can easily infer location context of others. So the primary issue is privacy versus trust. How much privacy does one have to give up in such setups? How much privacy one should give up? Is it possible to leverage social bindings for increasing trust while retaining privacy? We envision that these questions will need to be solved and **models towards social trust**, considering explicit friendship graphs, and/or implicit social trust based on mobility properties, will be part of the solutions.

Social Information Collection: As it has been mentioned before collection of social information via communal sensing and other forms can be of great advantage for interest-based resource management, urban and environmental planning, however one needs to have social incentives and trust in the collection process. We envision **privacy of aggregated data** in this context to be necessary.

Another major issue in this context is **the social data ownership**. As we collect social data through participatory communal sensing, surveys, questionnaires, or other means, we manage this collected social metadata in a distributed fashion, services use social information for their task and resource allocation, and it is not clear who owns them, or should own them and how do we preserve the original ownership.

Mobile Online Social Networks: As these networks are becoming ubiquitous, they raise important privacy issues because (a) the services are often centralized, i.e., user data is being held under a single administrative domain, and hence this approach is vulnerable to large-scale privacy breaches, and (b) terms of service often grant providers rights to user data, i.e., provider may display and distribute data in any way it sees fit, and advertising driven business models create incentives to share data with third parties that diminish user privacy.

Hence, we envision that **individual virtualized environments in a paid cloud computing infrastructure** might help privacy. Individual would be better served to upload personal information to their **own virtual machine**, which would then store the sensitive data. The data is then distributed across many administrative domains and individuals maintain rights to their data. The approach of VIS (Virtual Individual Server) allows mimicking of privacy expectations and trust relations that we see in offline social networks.

Grand Challenges

The group identified two grand challenges that are critical to pervasive social networks:

- ***Mechanisms for addressing privacy, security and trust issues in order to facilitate uncoordinated group of strangers to participate.***
- ***Need for research in real-time security to find sweet spot between security and time performance***

The challenges within security and privacy mechanisms for communal sensing and pervasive phone-based social networks are, how to:

- (a) Allow a large uncoordinated group of strangers to participate,
- (b) Complément more favorable video surveillance,
- (c) Enforce limits on usage of contributed data,
- (d) Ensure authenticity of request,
- (f) Allow for integrity while yielding privacy;
- (g) Design security on embedded devices.

Challenges between Security/Privacy and Performance/Energy/Usage: These challenges need to find sweet spot between security and ***time performance***, presenting need for research in ***real-time security***. Also, as mentioned above, the challenge is between privacy/security and usage of other resources such as ***energy/bandwidth***, e.g., how to efficiently authenticate a user in a group of devices where there is no centralized PKI-like authentication mechanism in place and the authentication does not use large amount of energy and time.

It becomes very clear in the pervasive social networks, that modeling security and privacy through absolute binary value (privacy yes or no) will not work, and hence how to setup ***adaptive privacy and security*** through ***Quality of Protection and its degrees*** (tuning knobs) among security, privacy, performance, usage dimensions according to personal preferences, situation and needs, is a true challenge.

When considering collecting social information and communal sensing, challenge becomes how to avoid ***“sensing-spam”***, and how to apply ***updates in timely manner***, e.g., wireless updates of a car while driving, or updates of heart pacemaker or updates in embedded devices within a critical infrastructure.

Fundamental Research

Research needs to be made at many levels, but we have identified the following:

- (1) **Energy-aware Real-Time Security:** since security and privacy mechanisms/algorithms reside on resource-constrained devices, many of the existing security and privacy algorithms need to be researched under the resource-constrained situations, if it is ***real-time encryption***, or ***real-time authentication***, or ***memory-constrained key management***.
- (2) **Adaptive Privacy and Security via Quality of Protection Degrees:** Since concept of privacy and security in social context is very much a personal decision, the mobile social networks need to

be sensitive to this issue and allow tuning knobs and setting different quality of protection degrees to allow for adaptivity. Research in modeling this type of **adaptive privacy and security** algorithms, protocols, policies and systems is needed.

- (3) **Privacy vs. Trust:** Trust means opening social information to others, privacy means concealing the information from others. We need research on **social trust models** to understand how they influence the privacy mechanisms, when to invoke what type of privacy rules, and who needs to be involved.
- (4) **Privacy and Security Metrics and Models for Pervasive Social Networks:** It is crucial to conduct research on fundamental **metrics, modeling of behaviors and trade-offs** to define the sweet-spots between privacy, security, performance and usage dimensions.
- (5) **Scalability of Solutions:** Pervasive Social Networks have interesting phenomena. These networks can be very polymorphic and dynamic, i.e., the same group can end up in different topological formations (e.g., see first responders), number of devices change constantly in their scale, as people group, cluster, based on their interest, daily activities, and create **dynamic coalitions** over time. Hence, any of **the privacy and security approaches must morph**, i.e., scale up and down to different social network formations as users use the phones throughout the days, months, years.
- (6) **Proactive Approach in Privacy/Security Design:** Often privacy and security approaches are embedded into our computing and networking environments as an after-thought. With pervasive social networks and environments, privacy and security must be integral functions of any functionalities deployed on cell-phones and research needs to be then done to proactively embed these designs into the health-care, first responder or other users devices for future successful usage.

Infrastructure and Experimentation

(General Comments on I and E)

There should be mechanisms for open online social networks and standards to allow deployment of pervasive social computing experiments and collection of data to analyze: how people used the system? what was the quality of user experience? how popular is the network? did the users recommend the social networks to their peers?

Such experiments will be carried out with the approval of Institutional Review Board (IRB). Trace data must be securely available from platform operators through established framework for access and sharing. The data collected should take into account heterogeneous sources and devices. The conflict between privacy and pollution is a critical issue when personal devices of users are employed for collecting data.

Education

(General Comments on Education)

Educating people about the growing importance of security and privacy in the context of pervasive social networks is a challenge. There are several implications of giving away privacy information and even context information. For example, a user providing traffic information from a certain point in a city, is also inadvertently giving away her location.

From an economic perspective, users must be made aware of the tradeoffs between economic incentives and situation, privacy and price. New regulations are needed to ensure adequate participation, without compromising user privacy and anonymity.

It is important to create new courses at undergraduate and graduate levels to teach them the principles of developing safe and secure applications for mobile platforms.

Applications

There are many applications of Pervasive computing and social networks. In particular, applications in the broad areas of crisis management, healthcare and wellbeing, public safety and infrastructure security, and environmental sustainability are of importance.

Specific Applications include:

- Personalized recommendations that combine social networking and pervasive technologies, e.g., travel tips.
- Individual life footprint
- Transient social networking applications, e.g., on-the-spot crisis management
- Participatory design
- Healthcare and aging
- Global governance
- Cooperative transportation
- Supply-chain management, e.g., food