Ubiquitous Social Networks

Sonja Buchegger
Deutsche Telekom Laboratories
Ernst-Reuter-Platz 7, D-10587 Berlin, Germany
sonja@ieee.org

When the terms ubiquitous computing and privacy have been mentioned together in scientific discourse on what the effect of technology is on society (and vice versa), these terms have been mostly presented as a trade off rather than in a positive relation to each other. This does not have to hold for all cases, ubiquitous computing does not necessarily have the side effect of surveillance and breaches of privacy. We are in fact claiming the opposite - that, given the right application, ubiquitous computing can actually help to enhance privacy for people.

By taking advantage of the distributed nature of ubiquitous computing and storage, it is possible to create owner-less community-driven services and applications. We mean that in the sense of a commons: there is no single (commercial or public) entity that controls both the service itself and the data collected by the service. There is no one who can dictate terms of use, analyse the data by data mining, push targeted advertising to the users or otherwise infringe on the users' privacy. By distributing the control over the community of users of the service, we can already reduce the threat to privacy that arises by collecting data centrally. When we add suitable mechanisms for encryption and access control, users can decide how much information to reveal to whom and thus limit the potential for privacy breaches not only by the service provider but also by other users. In addition to enhanced privacy, we can make use of other features provided by ubiquitous computing, such as proximity in the geographic sense and thereby enable location-based services.

The application that prompted our exploration of how ubiquitous computing can help alleviate privacy concerns is online social networks, where people interact with their real-life and their Internet friends via dedicated websites.

Online social networks like Facebook, MySpace, Xing, etc. have become extremely popular. Yet they have some limitations that we want to overcome for a next generation of social networks: the privacy concerns mentioned above and requirements of Internet connectivity, both of which are due to the services being implemented as web-based applications on a central site whose owner has access to all data.

While some online social networking sites follow up with corrective measures to address privacy concerns because of users' outcry, and one may also argue about legislative solutions to protect users' privacy, there is no guarantee that in the future the users' data will not be misused. The primary objective here is thus to aim for a system which makes it technologically harder (ideally, impossible) to violate the users' privacy and large scale data mining, even while the users continue to enjoy the advantages of social networking services.

To overcome these limitations, we envision a paradigm shift from client-server to a peer-to-peer infrastructure coupled with encryption so that users keep control of their data and can use the social network also locally, without Internet access. This shift gives rise to many

research questions intersecting networking, security, distributed systems and social network analysis, leading to a better understanding of how technology can support social interactions.

Centralised web-based social networks do not match the inherent peer-to-peer nature of both social networks themselves and of participatory media creation. User-provided content and participatory media creation suit themselves better to a community-driven peer-to-peer rather than a client-server model. By mapping a peer-to-peer application to a peer-to-peer infrastructure, direct connections can be exploited such that locality can be taken into account. Peers can carry information for each other in a delay-tolerant fashion and use local access points for local information. We thus have a matching of the distributed nature of human social networks with a distributed service, and we can also match the service to a local environment and make it a ubiquitous service. By supporting the direct exchange of information between devices, be it between users that meet or between adjacent nodes of a city mesh network, a peer-to-peer infrastructure can take advantage of real social networks and geographic proximity. In contrast to a centralised web server, local connectivity already facilitates social networking without Internet access.

In addition to addressing the privacy aspects in general, there is an opportunity to support a non-commercialised self-organised service. Web-based centralised online social networks today bring together the social sphere of family and friends with the commercial sphere. This combination enables targeted advertising thanks to profile information and data mining and thus based on a person's revealed preferences and extends it to a more precise targeting by taking into account social information. We envision a ubiquitous social network service that separates these spheres and enables users to maintain their social network without commercial prompting by advertisement.

User control of data, as provided by a peer-to-peer and secured social network, has consequences beyond privacy and freedom from advertisement. One such consequence is that users can also exercise control over the content they create in terms of intellectual property. User control in this sense means control over who can access their content and what they are allowed to do with that content, e.g. access control can be combined by licensing models of the user's choice (e.g. creative commons licenses) allowing for flexible content rights, as opposed to the current practice of copyright for the online social network providers.

Another aspect of control is how the social network can be accessed. Moving down the layers from application to network to physical access, there is another instance of peer-to-peer paradigm suitability that has been overlooked: decentralised access via various means (such as direct exchange, as in opportunistic networks) for ubiquitous social networks as opposed to those limited to the web.

This work is in the context of a joint project with Anwitaman Datta (NTU Singapore), Doris Reim (Deutsche Telekom Laboratories), and Le Hung Vu (EPFL). Our first task was to identify the core functionalities necessary to build social networking applications and services, and the research challenges in realizing them in a decentralised setting. We now have a simplified prototype implementation for testing.