Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems

Marc Langheinrich

Distributed Systems Group, Institute of Information Systems, IFW
Swiss Federal Institute of Technology, ETH Zurich
8092 Zurich, Switzerland
www.inf.ethz.ch/~langhein/

Abstract. This paper tries to serve as an introductory reading to privacy issues in the field of ubiquitous computing. It develops six principles for guiding system design, based on a set of fair information practices common in most privacy legislation in use today: notice, choice and consent, proximity and locality, anonymity and pseudonymity, security, and access and recourse. A brief look at the history of privacy protection, its legal status, and its expected utility is provided as a background.

1 Introduction

Privacy has been a hot-button topic for some time now. But so far its impact on a field where its relevancy is obviously high - ubiquitous computing - has been rather minimal. An increasing number of research projects are under way in the field of Internet privacy [6,16,18], some work has already been done in the field of Computer Supported Collaborative Work [5,21], but only a small amount of work has so far been accomplished in the area of ubiquitous or pervasive computing.

While some ubiquitous computing research projects explicitly address privacy [2,12], so far solutions in the field have been ad-hoc and specific to the systems at hand. One reason is surely the fact that ubiquitous computing is still in its infancy, with only a few dozen research groups around the world developing comprehensive systems. But it is also the privacy topic itself that is elusive: typically situated in the realms of legal studies, computer scientist have a hard time approaching a subject that is more often a social, even ethical issue.

This article tries to serve as an introductory reading for the interested computer science researcher, especially in the field of ubiquitous computing. It gives a brief background on privacy - its history and the issues surrounding it, touches on various legal implications, and tries to develop a comprehensive set of guidelines for designing privacy-aware ubiquitous systems.

2 Privacy

Instead of trying to give yet another definition for something for which "no definition ... is possible, because [those] issues are fundamentally matters of

G. D. Abowd, B. Brumitt, S. A. N. Shafer (Eds.): Ubicomp 2001, LNCS 2201, pp. 273–291, 2001.

values, interests, and power" [15], the following tries to look at privacy from three angles: its history, its legal status, and its utility.

Discussions about privacy have a long history, and various historical changes have brought about a change in perspective of our privacy needs. Consequently, much of this discussion has been incorporated into various regulatory and legal frameworks around the world, each with various effects. Last but not least, recent developments in technology have sparked a discussion about the necessity of strict privacy protection, which might not only be infeasible to administer, but also inconvenient to live with.

2.1 A Brief History

Privacy has been on people's mind as early as the 19th century, when Samuel Warren and Louis Brandeis wrote the influential paper "The Right to Privacy" [25], motivated largely by the advent of modern photography and the printing press. While Brandeis defined privacy as "the right to be let alone" (arguing against nosy reporters who would take pictures of people without permission – previously one had to sit still for a substantial amount of time, otherwise the picture would be all blurred), most people nowadays think of it more as "the right to select what personal information about me is known to what people" [26].

Privacy became a hot issue once again in the 1960s when governments discovered automated data processing as an effective means to catalog its citizens. Remembering the Nazi exploitation of detailed public records in World War II (allowing them to easily find the Jewish population of any city they raided), many European nations passed various "data-protection" laws in order to prevent any misuse of such centrally stored information. Lately, the increased use of credit cards, and last not least the dawn of the Internet, have made privacy protection a hot-button topic once again.

Over the course of time, the primary focus of privacy has shifted according to technological developments. Privacy issues can be traced as far back as 1361, when the Justices of the Peace Act in England provided for the arrest of peeping toms and eavesdroppers, establishing the first notion of behavioral, or *media privacy* [20]. In the 18th century, English parliamentarian William Pitt wrote, "The poorest man may in his cottage bid defiance to all the force of the Crown. It may be frail; its roof may shake; the wind may blow though it; the storms may enter; the rain may enter – but the King of England cannot enter; all his forces dare not cross the threshold of the ruined tenement" [27]. This form of privacy is often referred to as *territorial privacy*. With the increased use of the telephone system in the 1930s, *communication privacy* received much attention with the case of Olmstead vs. United States in 1928, which questioned the legality of wiretapping by the United States government. The privacy of the person, often called *bodily privacy*, was seriously violated only a few years later, when Nazi leadership decided to conduct compulsory sterilization, as well as gruesome medical experiments, on parts of the non-Aryan population. The increased use of governmental electronic data processing in the 1960s and 1970s finally created the issue of *information privacy*.