

Personal Privacy and Popular Ubiquitous Technology

Niall Winters,
London Knowledge Lab, Institute of Education.
n.winters@ioe.ac.uk

Abstract

In Britain today, ubiquitous technologies are becoming an increasing part of people's lives. Using well-known exemplars (the Oyster Card, London's Congestion Charging System and the Mobile Phone), this paper addresses the issue of privacy in relation to people's use of such technologies. Privacy recommendations are proposed for the use, exchange and control of personal information, with the aim of stimulating public debate on this issue.

Introduction

In 1991, the late Mark Weiser coined the term ubiquitous computing [9] to refer to technology that weaved into the fabric of everyday life. He hoped that "ubiquitous computing will enable nothing fundamentally new, but by making everything faster and easier to do, with less strain and mental gymnastics, it will transform what is apparently possible". This idea is controversial: for all those who foresee the computer reinvented as an invisible tool, integral to our lives, there are those who foresee an Orwellian future, where we have no privacy and our every move is monitored by "Big Brother". This paper attempts to address these privacy concerns in relation to: (i) the Oyster Card, (ii) London's Congestion Charging System and (iii) the Mobile Phone.

Personal Privacy: Why Is It Important?

Informational privacy has been defined as "the claim of individuals, groups or institutions to determine when, how and to what extent information about them is communicated to others" [10]. It is a "hot topic", with concern about the collection and dissemination of personal information regularly being voiced. In this regard privacy laws, such as the Data Protection Act, have enjoyed widespread support. However, critics ask a valid question: is personal privacy desirable? In the author's opinion, it is desirable because computers are immensely powerful at searching large repositories of information, and society, as a whole, relies on laws to make sure this technology is not misused. These laws are not immutable: they can always be changed according to the political climate. Thus, some level of personal control is required. If people lose control over how their personal information is used, the possible misuse of technology can have grave consequences [3].

Several works have dealt with privacy and technology. A collection of essays debating privacy policy can be found in [2]. The potential risks of ubiquitous technology have been highlighted

[4,5,8] and possible solutions detailed [1,6].

Popular Ubiquitous Technology

Popular ubiquitous technologies are briefly summarised below, keeping in mind the Faustian [7] bargain: technological advances must be weighted against their corresponding disadvantages.

The Oyster Card is a smart travel card providing London Transport with an individual's journey data (station entered, time entered, station exited etc.) which can be viewed at touch-screen ticket machines. If registered, the information is collected: name, address, date of birth, telephone number, email address, and in some cases, mother's maiden name. The stated advantages of the card are increased ease-of-use, greater flexibility and increased security.

Transport for London's **Congestion Charging System** - the world's largest - works by using a network of ~700 CCTV-type cameras, in ~230 positions, to capture infra-red images of car number plates when drivers enter or exit the congestion charging zone. Automatic Number Plate Recognition (ANPR) software then matches the captured number against a database of drivers who have paid to enter the zone. Number plates of drivers who have not paid are manually checked against UK's Driver and Vehicle Licensing Agency (DVLA) database for penalty notices to be issued.

Among large sections of the population, **mobile phone** use is habitual. The billionth GSM user is expected to be connected during the first quarter of 2004, a testament to the era of convenient communication. One of the lesser-known features of GSM is its ability to determine a user's location to within a few hundred metres, depending on base-station density. From October 2004, US mobile phone networks shall be required to provide information on the tracking of emergency calls. Implementing this tracking also results in networks having the ability to provide for-profit services to businesses.

Public Concern

To provide an indication of people's views about the above technology and the companies that use it, a small survey was undertaken. Of the 13 people interviewed (8 men and 5 women, across differing age groups and income levels), it showed that:

69% were concerned about how ubiquitous technology affects their privacy.

54% were concerned about large-scale

surveillance.

92% thought habit profiling was possible.

30% felt they had control over how their personal information was used.

15% felt they did have adequate access to the information stored about them.

38% trusted companies with their personal information.

23% completed reading a company's privacy policy.

Note that, overwhelmingly, people were concerned about how ubiquitous technology affected their privacy. In particular, lack of access to, and control over, personal information was a significant issue. In general, people's concern was not strong enough to stop them using a particular service. However, a number of issues arose with regard to company and government use of ubiquitous technology, reflected by the interview quotes below. First, there is a general but significant feeling of privacy invasion:

"Companies and the government collecting my personal data to sell me crap and track my whereabouts under the banner of personalisation/reducing congestion/location-based services is worrying."

Secondly, based on some people's experience, there is concern about the accuracy of the information stored (travel patterns, people called etc.) and access to it:

"It's often wrong, misinterpreted and over-used."

"Not too bothered about them keeping it as long as it's correct and that I get access to it for my own use. I can't do my travel claim because I can't remember dates and places - but they have this!!"

Thirdly, with regard to ubiquitous technology, for some a "Big Brother" perception exists: *"It reminds me of 'Enemy of the State'!"*.

Finally, in line with other research undertaken, most people fell into the category of *privacy pragmatists* [10], in this case 46%. These people will accept a certain trade-off between the use of personal information in return for a particular service.

Privacy Recommendations

Arising from the above results, and in line with best-use, a number of privacy recommendations for the design of ubiquitous technology will now be made. Due to space considerations, only the key points are listed.

1. Ubiquitous technologies must be designed with a nobility of intended purpose. When using personal information, nobility means dealing with privacy in a forthright and full manner. Simply providing a privacy policy is not enough.
2. Privacy is not an absolute concept: it changes

based on multiple factors including user location.

3. Transparency is essential: learn from previous companies' mistakes. Concealment of technical affordances is not an option. Users are likely to find invasive, the sudden discovery of a function that affects their privacy.
4. No surprises: make users aware of functionality and let them learn how the system works. A knowledgeable user is an aware user.
5. Provide a simple interaction mechanism for user control of, and access to, personal data.
6. Provide convenience and flexibility but not at the cost of security.
7. Do not rely on user apathy.

If the above recommendations are followed beneficial acceptance of ubiquitous technology is possible. Users will know their privacy is safeguarded because the technology is **transparent** and they have **trust** in it.

Conclusions

This paper proposed seven privacy recommendations for the use, exchange and control of personal information, citing three exemplars of popular ubiquitous technologies. When such technologies are designed to work in harmony with user expectations and perceptions, the future adoption of new devices is likely to be greatly enhanced.

Bibliography

- [1] A. Adams and M. Sasse. *Privacy in multimedia communications: protecting users not just data*. In Proceedings of IMHHC'I'01, pages 49-64, 2001.
- [2] P. Agre and M. Rotenberg. *Technology and Privacy: The New Landscape*. MIT Press, 1997.
- [3] E. Black. *IBM and the Holocaust: The strategic alliance between Nazi Germany and America's most powerful corporation*, Little Brown, 2001.
- [4] S. Doheny-Farina. The last link: Default = offline or Why Ubicomp Scares me. In *Computer-Mediated Communication*, pages 18-24, 1994.
- [5] S. Garfinkel. *Database Nation: The Death of Privacy in the 21st Century*. O' Reilly & Associates, 2001.
- [6] M. Langheinrich. Privacy by design - principles of privacy-aware ubiquitous systems. In *Proceedings of the International Conference on Ubiquitous Computing*, pages 273-291, 2001.
- [7] N. Postman. Five things we need to know about technological change. In *Proceedings of the NewTech*, 1998. Talk.
- [8] S. Talbott. The trouble with ubiquitous technology pushers, or: Why we'd be better off without the MIT Media Lab. In *NETFUTURE: Technology and Human Responsibility*, January 2000.
- [9] M. Weiser. The computer for the twenty-first century. *Scientific American*, pages 94-110, 1991.
- [10] A. Westin. *Privacy and Freedom*. Atheneum, 1967.