Design: Guidelines

Presented by: Aleksandr Khasymski

Papers

- Design for privacy in ubiquitous computing environments
  - Victoria Bellotti, and Abigail Sellen, 1993
- Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems
  - Marc Langheinrich, 2001
- Security in the wild: user strategies for managing security as an everyday, practical problem
  - Dourish, P., Grinter, E., Delgado de la Flor, J., and Joseph, M. 2004
- Personal privacy through understanding and action: five pitfalls for designers
  - Lederer, S., et al. 2004

Presentatio Outline

- Overview
- Contributions
- Outline of the framework/case study
- Conclusion

  x4

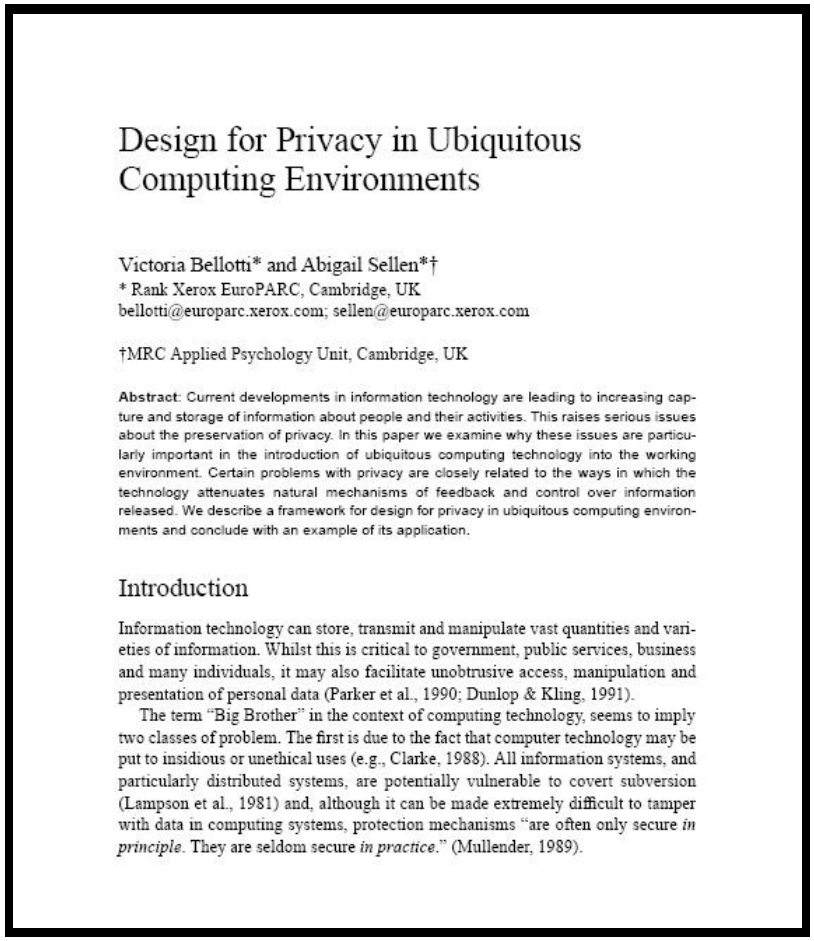
- Class Discussion

Design for privacy in ubiquitous computing environments

Victoria Bellotti

Abigail Sellen

EuroPARC, Cambridge, UK



Design for Privacy in Ubiquitous Computing Environments

Victoria Bellotti* and Abigail Sellen*†
* Rank Xerox EuroPARC, Cambridge, UK
bellotti@europarc.xerox.com; sellen@europarc.xerox.com

†MRC Applied Psychology Unit, Cambridge, UK

Abstract: Current developments in information technology are leading to increasing capture and storage of information about people and their activities. This raises serious issues about the preservation of privacy. In this paper we examine why these issues are particularly important in the introduction of ubiquitous computing technology into the working environment. Certain problems with privacy are closely related to the ways in which the technology attenuates natural mechanisms of feedback and control over information released. We describe a framework for design for privacy in ubiquitous computing environments and conclude with an example of its application.

Introduction

Information technology can store, transmit and manipulate vast quantities and varieties of information. Whilst this is critical to government, public services, business and many individuals, it may also facilitate unobtrusive access, manipulation and presentation of personal data (Parker et al., 1990; Dunlop & Kling, 1991).

The term "Big Brother" in the context of computing technology, seems to imply two classes of problem. The first is due to the fact that computer technology may be put to insidious or unethical uses (e.g., Clarke, 1988). All information systems, and particularly distributed systems, are potentially vulnerable to covert subversion (Lampson et al., 1981) and, although it can be made extremely difficult to tamper with data in computing systems, protection mechanisms "are often only secure *in principle*. They are seldom secure *in practice*." (Mullender, 1989).

Overview

- One of the classic papers in privacy in ubiquitous computing
  - Cited 132 times (including the last two papers)
- Proposes one of the first design frameworks for privacy in ubiquitous computing.
  - Framework is applied to RAVE a Computer supported cooperative work (CSCW) environment.

RAVE

- RAVE is a media space
- RAVE nodes in every office
  - Cameras, monitors, microphones, and speakers (think Skype)
- Cameras in public spaces
- Features
  - Glance
  - V-phone call
  - Office-share

Principles and Problems in RAVE

- Principles
  - **Control** – over who gets what information
  - **Feedback** – of what information is captured by whom
- Problems
  - **Disembodiment** – when *conveying information*
    - You cannot present your self as effectively as in a face-to-face setting
  - **Dissociation** - when *gaining information*
    - Only the results of you actions are conveyed, “actions themselves are invisible”. (think touch)
    - Results from the disembodied presence of the person you are trying to interact with.

The Design Framework

	Feedback About	Control Over
Capture	When and what information about me gets into the system.	When and when not to give out what information. I can enforce my own preferences for system behaviours with respect to each type of information I convey.
Construction	What happens to information about me once it gets inside the system.	What happens to information about me. I can set automatic default behaviours and permissions.
Accessibility	Which people and what software (e.g., daemons or servers) have access to information about me and what information they see or use.	Who and what has access to what information about me. I can set automatic default behaviours and permissions.
Purposes	What people want information about me for. Since this is outside of the system, it may only be possible to infer purpose from construction and access behaviours.	It is infeasible for me to have technical control over purposes. With appropriate feedback, however, I can exercise social control to restrict intrusion, unethical, and illegal usage.

Design Criteria

- Trustworthiness
- Appropriate Timing
- Perceptibility
- Unobtrusiveness
- Minimal intrusiveness
- Fail-safety
- Flexibility
- Low effort
- Meaningfulness
- Learnability
- Low Cost

Applying the Framework

- Evaluated existing solution based on the criteria and propose new solutions if necessary
  - Eg. A confidence monitor next to a camera
    - Trustworthy, meaningful appropriately timed
  - Mannequin with camera
    - Less obtrusive, but less meaningful
  - Viewer display of people watching
    - Expensive, intrusive

Conclusion

- Constructed a framework for design for privacy in a ubiquitous environment
- It can be used to:
  - Clarify existing state of affairs
  - Clarify shortcomings of existing solutions
  - Assess proposed solutions as well!
- There needs to be delicate balance between awareness and privacy
  - Too much feedback can be intrusive.

Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems

Marc Langheinrich

Swiss Federal Institute of Technology,
Zurich Swtizerland

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 values, interests, and

Overview

- An introductory reading to privacy issues in ubiquitous computing
- Brief history of privacy protection and its legal status
  - US Privacy Act of 1974
  - EU's Directive 95/46/EC
- Does privacy matter?
- Is Ubiquitous computing different?
- Six principles guiding design
- Outlook

A Brief History

- Privacy has been on peoples minds as early as the 19th century.
  - Samuel Warren and Louis Brandeis paper “The Right to Privacy”, in response to the advent of modern photography and print press.
- Hot topic again in 1960s in response to governmental electronic data processing.
- US Privacy Act of 1974 created the notion of *fair information practices.*

US Privacy Act of 1974 – principles

- **Openness and transparency** - no secret record keeping
- **Individual participation**
- **Collection limitation** – proportional to purpose
- **Data quality** – up to date
- **Use limitation** – for specific purpose, by authorized personnel
- **Reasonable security**
- **Accountability**

- The 1995 EU Directive adds the notion of **explicit concent**

Does privacy matter?

- As technology inevitably advances, critics question the merits of privacy
- **Feasibility** – what can technology achieve (or prevent!). Is accountability possible?
- **Convenience** – advantages of free flow of information outweigh personal risks. Should semi-private information like shopping habits be public for better service? (Kroger plus card)
- **Communitarian** – trust government with private information.
- **Egalitarian** – information not a weapon in the hands of well informed.

- As with many things the answer lies in the middle.

Social implications of Ubiquitous Computing

- **Ubiquity** – its design can affect our whole life.
- **Invisibility** – shrinking computer features will make it hard to know if a device is present.
- **Sensing** – sensors the can detect stress, fear, etc.
- **Memory Amplification** – still a little Sci-Fi

Principles and Guidelines

- Based on above discussion total security and privacy is ***not*** achievable.
- Principles designed to prevent “unwanted accidents”
  - notice,
  - choice and consent,
  - proximity and locality,
  - anonymity and pseudonymity,
  - security, and
  - access and recourse.

Principles and Guidelines cont.

- **Notice** – employ technologies like RFID tags, and P3P on the Web.
  - Examples of the “smart mug” that inadvertently spies on a colleague.
  - Notice should apply to the *type* of data collection.
- **Choice and Consent**
  - Providing consent needs to be *efficient* or risk to be *annoying.*
  - Only one choice = blackmail!
- **Anonymity and Pseudonymity**
  - Anonymity is hard in the context of ubiquitous computing.
  - Data-mining can be threat as well.

Principles and Guidelines cont.

- **Proximity and Locality**
  - Devices activate only in the presence of owner.
  - Locality – modeled by a “small rural community”.
- **Adequate Security**
  - Can be hard to implement.
  - Maybe its not a panacea, if we consider alternatives like locality and proximity.
- **Access and Recourse**
  - Define access requirements.
  - Sufficient technology, eg. P3P.

Outlook and Conclusion

- There is a lot to be done in ubiquitous computing or we risk a Orwellian nightmare-come-true
- Some principles are readily implementable, while others like anonymity can be quite hard.
- The paper highlights that some principles can be chosen over others.
  - eg. Locality vs. Security

Security in the wild: user strategies for managing security as an everyday, practical problem

Paul Dourish

Rebecca E. Grinter

Jessica Delgado de la Flor

Melissa Joseph

Pers Ubiquit Comput (2004) 8: 391–401
DOI 10.1007/s00779-004-0308-5

ORIGINAL ARTICLE

Paul Dourish · Rebecca E. Grinter
Jessica Delgado de la Flor · Melissa Joseph

Security in the wild: user strategies for managing security as an everyday, practical problem

Received: 2 December 2003 / Accepted: 6 July 2004 / Published online: 22 September 2004

Abstract Ubiquitous and mobile technologies create new challenges for system security. Effective security solutions depend not only on the mathematical and technical properties of those solutions, but also on people's ability to understand them and use them as part of their work. As a step towards solving this problem, we have been examining how people experience security as a facet of their daily life, and how they routinely answer the question, "is this system secure enough for what I want to do?" We present a number of findings concerning the scope of security, attitudes towards security, and the social and organizational contexts within which security concerns arise, and point towards emerging technical solutions.

1 Introduction

Weiser's [30, 31] vision of ubiquitous computing—a third wave of computation, displacing the era of mainframes and personal computers—implies radical transformations in many aspects of our computational world. By moving interaction beyond the desktop, it transforms the settings within which interaction occurs, and the forms of that interaction; by emphasizing the role of trends in miniaturization and power consumption, it transforms the nature of the computational devices themselves. At the same time, it also transforms the nature and boundaries of the "system." Where conventional computer use is focused on a single device, perhaps linked to a few others across a network, ubiquitous computing is typically manifest through collections of many devices—some mobile, some static, some embedded in the infrastructure, and some carried by individuals—brought together to form ad hoc coalitions in specific circumstances of use [11]. Holding a meeting in an interactive workspace may involve bringing together tens of devices or more, including mobile, handheld, and wearable devices belonging to meeting participants, as well as components managing the input, monitoring, recording, and display capabilities of the space (e.g., [18]). Ubiquitous computing, then, implies ubiquitous digital communication, as the devices that make up a ubiquitous computing system communicate in order to identify each other and their capabilities, achieve effective configurations of functionality, and interoperate in support of user needs.

However, while ubiquitous communication offers the possibility of achieving more effective coordination in a world of computational devices, it also introduces a range of problems regarding the security of these systems. Information system security has always been an important issue in military and corporate settings, but in mobile and ubiquitous computing settings, it becomes a central concern for casual and end users. Networked and e-commerce systems bring with them the dangers of disclosing credit card numbers, social security information, bank transaction details, client records, and other electronic artifacts; context-aware and mobile systems carry with them the possibility of disclosing information about activities and locations. Ubiquitous computing, as Weiser [30, 31] noted, anticipates that an individual's computational needs will be met by tens or hundreds of computational components working together; security is both an inherent problem in this sort of combinatorial system, and a practical concern for end users. Systems must be not only secure, but usably and practically secure.

In order to understand security as a user concern as well as a technical concern, our approach has been to look at the practical, everyday aspects of security as they

P. Dourish (✉) · J. Delgado de la Flor · M. Joseph
School of Information and Computer Science,
University of California, Irvine,
CA 92697-3425, USA
E-mail: jpd@ics.uci.edu

R. E. Grinter
College of Computing, Georgia Institute of Technology,
Atlanta, GA 30332, USA
E-mail: beki@parc.com

Overview

- A study of how people *experience* security in their daily lives.
- How do people answer the question: “is this system secure enough for what I want to do?”
- Exploring the *human factor* in security and shed some light why users can become the “weakest link”.
  - Observer and interview people in a academic institution and an industrial research lab.
- Reframe security for ubiquitous computing.
- Conclusion

The experience of Security

- **Attitude towards security**:
  - **Frustration** – older vs. younger people.
  - **Pragmatism** – identify cost vs. benefit.
  - **Futility** – the “hackers” always one step ahead.
- **Security as a barrier** - for “everything”.
- **Security online and offline** – practicing security is not a purely online matter, it extends in the physical world.

Practice of Security

- **Delegating security to a :**
  - **Individual**, eg. knowledgeable colleague.
  - **Organization**, eg. Helpdesk.
  - **Institution**, eg. Expectation of a financial institution.
- **Security actions**
  - Encryption vs. “Cryptic” messages.
  - Media switching, eg. E-mail vs phone call.
- **Holistic security management**
  - Physical arrangement of space, eg. Computer monitor in an office
- **Managing identity**
  - Maintaining multiple online identities.
  - Problem when an individual turns out to be a group, eg. A person’s email is automatically forwarded to their assistant.

Security for Ubiquitous Computing

- Instead of focusing on mathematical and technical guarantees, we need to address security as a *practical problem.*
  - Provide the *resources* so that people can answer the question – "is this computer system secure enough for what I want to do now?"
- Place security decision (back) in the context of a practical matter or goal.
- Instead of **transparent** security technology needs to be **highly visible**.

Conclusion

- The “penultimate slide” problem.
  - Success of ubiquitous computing relies on designing for security and privacy.
  - Both are currently poorly understood.
- This study highlight some of the importance of HCI research.
- Protection and sharing of information are *to aspects of the same task.*

Personal privacy through understanding and action: five pitfalls for designers

Scott Lederer

Jason I. Hong

Anind K. Dey

James A. Landay

Pers Ubiquit Comput (2004) 8: 440–454
DOI 10.1007/s00779-004-0304-9

ORIGINAL ARTICLE

Scott Lederer · Jason I. Hong · Anind K. Dey
James A. Landay

Personal privacy through understanding and action: five pitfalls for designers

Received: 10 December 2003 / Accepted: 21 May 2004 / Published online: 16 September 2004

Abstract To participate in meaningful privacy practice in the context of technical systems, people require opportunities to *understand* the extent of the systems' alignment with relevant practice and to conduct discernible social *action* through intuitive or sensible engagement with the system. It is a significant challenge to design for such understanding and action through the feedback and control mechanisms of today's devices. To help designers meet this challenge, we describe five pitfalls to beware when designing interactive systems—on or off the desktop—with personal privacy implications. These pitfalls are: (1) obscuring potential information flow, (2) obscuring actual information flow, (3) emphasizing configuration over action, (4) lacking coarse-grained control, and (5) inhibiting existing practice. They are based on a review of the literature, on analyses of existing privacy-affecting systems, and on our own experiences in designing a prototypical user interface for managing privacy in ubiquitous computing. We illustrate how some existing research and commercial systems—our prototype included—fall into these pitfalls and how some avoid them. We suggest that privacy-affecting systems that heed these pitfalls can help users appropriate and engage them in alignment with relevant privacy practice.

Keywords Privacy · Interaction design · Design guidelines · Ubiquitous computing

S. Lederer (✉) · J. I. Hong · A. K. Dey
Group for User Interface Research,
Computer Science Division,
University of California,
Berkeley, CA, USA
E-mail: lederer@cs.berkeley.edu
Tel.: +1-510-6430943
Fax: +1-510-6425615
E-mail: jasonh@cs.cmu.edu
E-mail: anind@intel-research.net

A. K. Dey
Intel Research, Berkeley, CA, USA

J. A. Landay
DUB Group, Department of Computer Science
and Engineering, University of Washington,
Seattle, WA, USA
E-mail: landay@cs.washington.edu

J. A. Landay
Intel Research, Seattle, WA, USA

1 Introduction

One possible reason why designing privacy-sensitive systems is so difficult is that, by refusing to render its meaning plain and knowable, privacy simply lives up to its name. Rather than exposing an unambiguous public representation for all to see and comprehend, it cloaks itself behind an assortment of meanings, presenting different interpretations to different people. When sociologists look at privacy, they see social nuances that engineers overlook. When cryptologists consider privacy, they see technical mechanisms that everyday people ignore. When the European Union looks at privacy, it sees moral expectations that American policymakers do not. Amidst this fog of heterogeneous practices, technologies, and policies that characterize the current state of privacy, designers of interactive systems face increasing market pressure and a persistent moral imperative to design systems that support users' privacy needs: systems that are *privacy-sensitive*.[1]

This article cannot dispel that fog, but it does attempt to shine some light through it by offering a partial set of guidelines for designers of privacy-affecting interactive systems, on and off the desktop. We say *partial* set of guidelines because this article does not aspire to be a

[1] We will use the term *privacy-affecting* as a general description for any interactive system whose use has personal privacy implications. We will use the term *privacy-sensitive* to describe any privacy-affecting system that—by whatever metrics are contextually relevant—reasonably avoids invading or disrupting personal privacy. This article is intended to help minimize the number of privacy-affecting systems that are *not* privacy-sensitive.

Overview

- A meaningful privacy practice requires two things:
  - Opportunity to **understand** the system, and
  - Ability to perform **sensible social actions**
- Five pitfalls (not guidelines) for designing interactive ubiquitous systems.
- Case study – “Faces” prototype
- Conclusion

Five pitfalls when designing for privacy

- An effort to reconcile *theoretical insights* and *practical guidelines* (established by the previous papers).
- Honor fair information practices
- Encourage minimum information asymetry
- Fall into two categories
  - Understanding
  - Action

Concerning Understanding

- Pitfall 1: Obscuring potential information flow
  - Types of information
    - Personae (name, SSN, etc.)
    - Monitorable activities (actions or contexts, eg location)
  - Kinds of people information is conveyed to
    - Third-party observers
  - Important to note that **potential** involves **future** and **past** information flow
- Example:
  - Gmail's content driven adds.
  - Tribe.net information clearly shared with members only at a certain degree of separation (also Facebook)

Concerning Understanding

- Pitfall 2: obscuring actual information flow
  - **What** information is conveyed to **whom,** as the interaction with the system occurs.
- Examples
  - Websites obscure information storage in cookies.
  - Symmetric design in IM systems.

Concerning action

- Pitfall 3: emphasizing configuration over action
  - Privacy management should be a natural consequence of ordinary use of system; it should not rely on extensive (prior) configuration.
  - In real settings user manage privacy semi-intuitively.
- Examples
  - E-mail encryption software, P2P file-share.
  - Embedding configuration in a meaningful action within the system.

Concerning action

- Pitfall 4: lacking coarse-grained control
  - Design should offer obvious, top-level mechanism for halting and resuming disclosure.
  - Users are remarkably adept at wielding coarse-grained controls to yield nuanced results
    - Setting door ajar, using invisible mode in IM, etc.
- Examples
  - Cannot exclude a purchase from an online history
  - Cell-phones, IM

Concerning action

- Pitfall 5: inhibiting established practices
  - People manage privacy through a range of established, often nuanced, practices.
  - Plausible deniability – was lack of disclosure intentional
  - Disclosing ambiguous information
- Examples
  - Location-tracking systems
  - IM

Faces

- Ubicomp environment that can display a person's location
- Privacy maintained by configuring 3-tuples of inquirer, situations, faces.
- Faces determines the precision of information disclosed, eg. None, vague, precise, etc.
- Faces particularly suffered from the action pitfalls.
- Converted to *precision dial.*

Class Discussion

- Do these guidelines actually apply to ubiquitous computing, given that it didn't really exist at the time that they are created?
  - The last paper comes closest.
- Are the design solutions already there as the last paper suggest?
  - IM and Cell phones are well accepted.
- Does a system need to support *existing practices*? Aren't practices *significantly* changed by some systems?