Privacy Invasions in Ubiquitous Computing

Marc Langheinrich

Distributed Systems Group
Institute for Pervasive Computing
Swiss Federal Institute of Technology, ETH Zurich
8092 Zurich, Switzerland
www.inf.ethz.ch/˜langhein

Abstract. While recent surveys often cite people who have experienced some form of *privacy invasion*, the exact nature of such invasions remains elusive. Yet in order to build ubiquitous computing systems that will respect the privacy of the individual, it is crucial to understand when it is exactly that people feel their privacy has been invaded. This paper motivates why privacy is necessary, describes an approach called *privacy boundaries* that tries to capture the various reasons a certain flow of personal information is perceived threatening, and looks briefly at how ubiquitous computing intensifies these problems.[1]

1 Introduction

As the field of ubiquitous computing matures, more and more of the key issues start shifting away from mere technical problems to those that have a fundamentally *social* background: How are we to use those smart devices in our daily routine? When should they be turned on and off? What should they be allowed to see, feel, or hear? And whom should they tell about it?

Among such questions, privacy is probably the most prominent concern when it comes to judging the effects of a widespread deployment of ubiquitous computing. This is certainly due to the already imminent threat to privacy caused by the ever growing use of distributed commercial databases that record large parts of our daily electronic transactions. By virtue of its very definitions, ubiquitous computing has now the potential to create an even more invisible and comprehensive surveillance network covering an unprecedented share of our public and private life. Consequently, much has been written about privacy in light of automated data processing [3, 5, 6], though less so in the context of ubiquitous computing [2, 9, 10].

The following article tries to add a more differentiated view on the impact of ubiquitous computing on personal privacy by first examining *why* personal privacy is desirable, describing *when* we feel that it has been violated, and then assessing *how* ubiquitous computing affects all that.

[1] This article is based on material from an earlier paper of the author [11] that has been published elsewhere.

2 Motivating personal privacy

Along with articles covering privacy aspects, a range of definitions for what actually constitutes privacy are given, the most prominent probably being judge Brandeis' "The right to be left alone" [24] and Alan Westin's "The claim of individuals... to determine for themselves when, how, and to what extent information about them is communicated to others" [26]. These definitions certainly help to illustrate that privacy not only has different goals in different contexts, but also that personal limits for privacy differ according to factors such as geography (e.g., whether we are at home or in a public park), informational access rights (e.g., anti-mask laws in certain states/countries prohibit hiding ones face in public), or expectations and manners (e.g., expecting people not to openly stare at you in public) [13]. Depending on any of these dimensions, individuals can both expect a reasonable level of protection from the prying eyes and ears of their fellow citizens, or be required to disclose certain parts of their own information when necessary by law or custom.

A valuable avenue for exploration when trying to assess the implications of new technology on something as old as the concept of privacy, might be to look at the *motivations* behind privacy, as it is far from undisputed that societies in fact need the level of privacy protection that its most ardent proponents would like to have. Scott McNealy's infamous "You have no privacy anyway, get over it" [21] and Peter Cochrane's "All this secrecy is making life harder, more expensive, dangerous and less serendipitous" [4] indicate a growing backlash among those tired of hearing the constant warnings coming from privacy advocates.

Privacy is often seen as a fundamental requirement for any modern democracy [20]. Only if people can freely choose according to their interests and believes, without fear of repression from their fellow citizens, the necessary plurality of ideas and attitudes can grow that prevent bringing the general public into line by charismatic leaders. Harvard law professor Lawrence Lessig [12] takes this requirement a step further and differentiates between a number of motivations for privacy protection in our present-day laws and norms:

- **Privacy as empowerment:** Seeing privacy mainly as informational privacy, its aim is to give people the power to control the dissemination and spread of information about themselves. A recent legal discussion surrounding this motivation revolves around the question whether personal information should be seen as a private property (which would entail the rights to sell all or parts of it as the owner sees fit) or as intellectual property (which would entitle the owner to certain unalienable rights, preventing him for example to sell the rights to his name to anybody).
- **Privacy as utility:** From the data subject's point of view, privacy can be seen as a utility providing more or less effective protection from nuisances such as unsolicited calls or emails. This view probably best follows Brandeis' "The right to be left alone" definition of privacy, where the focus is on reducing the amount of disturbance for the individual.
- **Privacy as dignity:** Dignity can be described as "the presence of poise and self-respect in one's deportment to a degree that inspires respect." [17] This not only entails being free from unsubstantiated suspicions (for example when being the

target of a wire tap, where the intrusion is usually not directly perceived as a disturbance), but rather focuses on the *balance* in information available between two people: analogous to having a conversation with a fully dressed person while being naked oneself, any relationship where there is a considerable information imbalance will make it much more difficult for those with less information about the other to keep one's poise.

- **Privacy as constraint of power:** Privacy laws and moral norms to that extend can also be seen as a tool for keeping checks and balances on a ruling elite's powers. By limiting information gathering of a certain type, crimes or moral norms pertaining to that type of information cannot be effectively enforced. As Stunz [22] puts it: "Just as a law banning the use of contraceptives would tend to encourage bedroom searches, so also would a ban on bedroom searches tend to discourage laws prohibiting contraceptives."
- **Privacy as by-product of imperfect surveillance tools:** While law enforcement in many democratic countries can in principle search any private premises, listen in to any private phone call, and open any number of private letters, given a proper search warrant, their actual ability to do so is often quite limited: searches and surveillance takes both time and money, so officers usually try to make sure they spend their efforts on some reasonably suspicious target. The larger, unsuspicious looking general public must thus rarely consider themselves the target of such a surveillance or search, simply because the effort would hardly be worth it. The resulting level of privacy they consequently enjoy stems inasmuch from the required court-ordered warrant, as from the imperfection of the employed search and surveillance tools.

Depending on what kind of motivation one assumes for preserving privacy, ubiquitous computing can become the driving factor of changing the reach and impact of privacy protection as it exists today, and create substantially different social landscapes in the future. It can do so because ubiquitous computing influences two important design parameters relating to privacy: the ability to *monitor* and the ability to *search* [12].

3 Ubiquitous computing and surveillance

Monitoring people and their actions and habits is a human trait as old as humanity itself. In the "good old days", such monitoring would constantly be done within small villages and settlements by our close social peers, who would immediately notice anything out of the ordinary and disseminate it in society. It was this close monitoring that often enough drove people into the big cities, where the sheer number of citizens and their constant mobility effectively put an end to the watchful eyes of the neighbors. Yet with the advent of automated information processing, machines took over the role of the watchers and began to store more and more of our daily routines, not only when they happened to be "out of the ordinary." With ubiquitous computing, monitoring capabilities can obviously be extended far beyond credit-card records, calling logs, and news postings. Not only will the *spatial* scope of such monitoring activities be significantly extended with ubiquitous computing but also their *temporal* coverage will vastly increase: starting from pre-natal-diagnostics data stored on the baby's health-id-card, to activity feeds in kindergarten and schools, to workplace monitoring and senior citizen health monitoring.

Such comprehensive monitoring (or: surveillance) techniques create new opportunities for what MIT professor emeritus Gary T. Marx calls *border crossings*: "Central to our acceptance or sense of outrage with respect to surveillance ... are the implications for crossing personal borders." [13]. He goes on to define four such border crossings that form the basis for perceived privacy violation:

- **Natural borders:** Physical limitations of observations, such as walls and doors, clothing, darkness, but also sealed letters, telephone calls. Even facial expressions can form a natural border against the true feelings of a person.
- **Social borders:** Expectations about confidentiality for members of certain social roles, such as family members, doctors, or lawyers. This also includes expectations that your colleagues will not read personal fax messages addressed to you, or material that you left lying around the photocopy machine.
- **Spatial or temporal borders:** The usual expectations of people that parts of their life, both in time and social space, can remain separated from each other. This would include a wild adolescent time that should not interfere with today's life as a father of four, or different social groups, such as your work colleagues and friends in your favorite bar.
- **Borders due to ephermal or transitory effects:** This describes what is best known as a "fleeting moment," an unreflected utterance or action that we hope gets forgotten soon, or old pictures and letters that we put out in our trash. Seeing audio or video recordings of such events later, or observing someone sifting through our trash, will violate our expectations of being able to have information simply pass away unnoticed or forgotten.

Putting ubiquitous computing systems into place will most certainly allow far greater possibilities for such border crossings in our daily routines. Consider the popular vision of a wearable *memory amplifier* [14, 18], allowing its wearer to constantly record events of her daily life in a lifetime multimedia diary. While at first sight such a technology promises great help for those of us who tend to forget a lot of small details it also has substantial consequences for our privacy borders stemming from *ephemeral and transitory effects*: Any statement I make during a private conversation could potentially be played back as a high-quality audio and video feed if my conversation partner would give others a peek into her multimedia diary. Even if this information would never get disclosed to others, just the thought of dealing with people who have a perfect memory and in theory would *never* forget anything, will probably have a sizable effect on interpersonal relationships.

The problem of *spatial and temporal borders* on the other hand is well known from the area of consumer profiles. Profiles are often enough the focus of public concerns, but so far social and legal attitudes have been relatively relaxed about them. Consumer acceptance is also much higher than the often negative news coverage might indicate, mostly because their harm is often perceived as being small (such as unsolicited spam) compared to their advantages (e.g., monetary incentives in the form of discounts or rewards). However, there are well-known risks associated with profiles, and their widespread as the basis for a ubiquitous computing infrastructure will only intensify such problems. Besides the obvious risk of data spills [8], profiles also threatens universal equality, a concept central to many constitutions, basic laws, and human rights, where "all men are created equal." [23].

The innocuous frequent flyer miles are a good example: While mileage programs allow airlines increase customer loyalty and provide consumers with free flights and other rewards, they associate different values to each customer (e.g., "gold member," "silver member"), dependent on their prior flight behavior. Independent of my monetary means, sales agents will be able to asses my "net worth" to the company once they have my frequent flyer number, and consequently provide me with special services (if I am "valuable") or withhold from me certain options (if I am not, since they are reserved for more privileged customers).

So even though a thoroughly customized future (using ubiquitous computing) where I only get the information that is relevant to my (very comprehensive) profile holds great promise, the fact that at the same time a large amount of information might be deliberately *withheld* from me because I am not considered a valued recipient of such information, constitutes a severe privacy violation for many people.

Applying ubiquitous computing technology in areas with primarily *social borders* – for example where a close social group interacts only among themselves, such as families [15, 25] or co-workers – might seemingly alleviate some of the above concerns. Most participants share already close relationships and tend to know a great deal about each other, without needing a system to compile a profile of their communication partner. Such systems, however, also raise the ante as to what *type* of information they handle. While a communication whiteboard for families may facilitate social bonding between physically and temporally separated members, it also increases the risk for unwanted social border crossings by accidentally allowing Mum to read a message you left for your sister, or a visiting friend to appear in the house activity log even though you told grandma you would spend the weekend alone. A similar problem is raised through more efficient information gathering and dissemination in the health care sector, where your comprehensive health record both improves information flow between your various physicians and their personnel, yet threaten to facilitate data sharing beyond your local clinic staff to include your health insurer and employer.

Natural borders, then, might be easiest to respect when designing ubiquitous computing systems. Here, the concept of surveillance is well known and usually fairly straightforward to spot, after all: If others are able to watch your actions behind closed doors, they are most certainly intruding on your privacy. Proponents of wearable computing systems often cite the fact that information could both be gathered and stored *locally* (i.e., on the users belt, or within her shirt) as a turnkey solution for privacy conscious technologists [19].

Border crossings, however, are not only about *who* does something, but *what* is happening. Even though a context-aware wearable system might keep its data to itself, its array of sensors nevertheless probe deep into our personal life, and the things it might find there might easily startle (and trouble!) us, once such systems would start anticipating our future actions and reactions. The feeling of having someone (or something) constantly peeking over our shoulder and second guessing us would certainly constitute a natural border crossing for most of us. And the temptation of law enforcement subpoenaing such information not only to determine your physical data (were you at the crime scene?) but also your *intentions* (by assessing the data feed from our body sensors) would certainly motivate legislation that would make the deletion of such information a crime (just as recent laws against cybercrime [16] do this for computer log files).

4 The power of search

All these examples serve to show that ubiquitous computing systems, even when installed for the greater good and with the best of intentions, will run a high chance of involuntarily threatening our personal borders that set apart private from public, simply because their monitoring capabilities will facilitate more of the border crossings described above. Whether or not such crossings ultimately occur, given the opportunities created, will to a large extend also depend on the type of *searching* capabilities that such ubiquitous computing systems might offer.

Search technology is traditionally not a particular focus of ubiquitous computing, mainly since its core methods are more likely to be developed in the fields of information retrieval or databases. However, what *will* become relevant in ubiquitous computing is how the chosen architectures will support such search techniques. Chances are high that such technology will be a basic building block of future ubiquitous computing systems, as most of the envisioned applications in the fields of *context-awareness* and *memory augmentation* require just these capabilities. An automated diary collecting 24/7 audio and video-feeds will not be of much use unless being combined with a powerful search and retrieval technology that lets us comb large amounts of data for very specific information. And the ability to combine different information sources, especially large, innocuous ones such as walking patterns or eating habits, is the backbone of any envisioned "smart" system, which must make best use of a large variety of different sensor input to come to decisions that make it appear as if it would *understand* what was happening around us.

Having thus both monitoring and search capabilities at the very core of their architecture, ubiquitous computing system will very likely provide their developers, owners and regulators with a significant tool to drive the future development of privacy concepts in society. Depending on the actual systems that receive large-scale deployment, some of the motivating aspects of privacy as discussed in section 2 might become more or less prominent, thus influencing corresponding legal and social norms.

For example, imagine law enforcement having a low-cost ability to search a large number of homes without effort in short time, for example by having all home automation manufacturers build in hooks into their software that would allow police to register certain behavioral patterns and let motion, audio and video sensors report in when they detect a suspicious match. The temptation to try one's luck in order to find a certain suspect might very well lure policymakers, judges and police into giving up today's relatively cumbersome privacy laws, marking privacy as it exists today as a simple residue of inefficient tools that can be abandoned in favor of national security. By motivating privacy instead as a simple *utility* with a bit of *dignity* thrown in, these searches could still be considered privacy-friendly as they would neither inconvene those subject to such a search, nor would they report any personal actions that would not fit the registered suspicious behavior.

Examples for consequences in ubiquitous systems design then, given the above findings, are numerous. They could include commendations to use sense-enhancing technologies only sparsely in ubiquitous computing, and only in limited, well-defined environments (e.g., emergency room, aircraft hangars). Communication concepts could be evaluated according to the existent social borders of all participants, in order to prevent unwanted data spills. Searching capabilities that allow spatial and temporal border crossings would need to be questioned, and the concept of ephemeral, transitory effects be re-introduced into ubiquitous computing architectures, allowing for example that information slowly decays over time.

5 Conclusions

The deployment of ubiquitous computing systems in the real-world will in many cases have implications beyond the technically obvious ones. Whether it be personal privacy, national economies, or social acceptance – designers of ubiquitous computing systems can greatly benefit from evaluating the effects of putting ubiquitous computing into the real-world using existing concepts in disciplines such as social, economic, and legal sciences.

In our previous discussions, we hopefully helped to identify and motivate key concepts in personal privacy that should influence the design and implementation of what we would call *privacy-aware* ubiquitous computing systems, i.e., systems that take the social fabric of everyday life into account and try to prevent unintended *personal border crossings*. Even though we are yet far from presenting technical implementations of these concepts, we nevertheless believe that a proper analysis of such non-technical aspects will provide beneficial to the overall system design in the field of ubiquitous computing.

References

1. Philip E. Agre and Marc Rotenberg, editors. *Technology and Privacy: The New Landscape*. The MIT Press, 1998.
2. Victoria Bellotti and A. Sellen. Design for privacy in ubiquitous computing environments. In *Proc. of the European Conference on Computer-Supported Cooperative Work*, 1993.
3. David Brin. *The Transparent Society*. Perseus Books, Reading MA, 1998.
4. Peter Cochrane. Head to Head. *Sovereign Magazine*, pages 56–57, spring 2000. Available at: www.cochrane.org.uk/opinion/papers/prof.htm.
5. Amitai Etzioni. *The Limits of Privacy*. Basic Books, New York NY, 1999.
6. Simson Garfinkel. *Database Nation*. O'Reilly, Sebastopol CA, 2000.
7. Robert Gellman. Does privacy law work? In Agre and Rotenberg [1], chapter 7, pages 193–218.
8. Robert O'Harrow Jr. Prozac maker reveals patient e-mail addresses. *The Washington Post*, July 4, 2001.

9. Marc Langheinrich. Privacy by design – principles of privacy-aware ubiquitous systems. In *Proceedings of Ubicomp*, pages 273–291, September 2001.
10. Marc Langheinrich. A privacy awareness system for ubiquitous computing environments. In *Proceedings of Ubicomp*, September 2002.
11. Marc Langheinrich, Vlad Coroama, Juergen Bohn, and Michael Rohs. As we may live – real-world implications of ubiquitous computing. Available at: www.inf.ethz.ch/vs/publ/papers/uc-implications.pdf, September 2002.
12. Lawrence Lessig. *Code and other Laws of Cyberspace*. Basic Books, New York NY, 1999.
13. Gary T. Marx. Murky conceptual waters: The public and the private. *Ethics and Information Technology*, 3(3):157–169, 2001.
14. Robert N. Mayo. The factoids project. Available at www.research.compaq.com/wrl/techreports/abstracts/TN-60.html.
15. Kristine S. Nagel. Family intercom: Developing a context-aware audio communication system. Presentation at Ubicomp 2001. Available at www.cc.gatech.edu/~kris/research/intcomm/ubi1/sld001.htm, September 2001.
16. Council of Europe. Convention on cybercrime. Available at: conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm, November 2001.
17. Joseph P. Pickett, editor. *The American Heritage College Dictionary*. Houghton Mifflin Co, 4th edition, April 2002.
18. Bradley Rhodes. The wearable remembrance agent: A system for augmented memory. *Personal Technologies Journal. Special Issue on Wearable Computing*, 1:218–224, 1997.
19. Bradley Rhodes, Nelson Minar, and Josh Weaver. Wearable computing meets ubiquitous computing - reaping the best of both worlds. In *Proc. of The Third International Symposium on Wearable Computers (ISWC '99)*, pages 141–149, San Francisco, CA, October 1999.
20. Mark Rotenberg. Testimony and statement for the record. Hearing on privacy in the commercial world. Available at www.epic.org/privacy/testimony_0301.html, March 2001.
21. Polly Sprenger. Sun on privacy: 'Get over it'. *Wired.com*, January 26, 1999. Available at: www.wired.com/news/politics/0,1283,17538,00.html.
22. Stunz. Privacy's problem and the law of criminal procedure. As cited in [12].
23. United States of America. *The Declaration of Independence and the Constitution of the United States*. Bantam Classic and Loveswept, August 1998. Text also available at www.nara.gov/exhall/charters/declaration/declaration.html.
24. Samuel Warren and Louis Brandeis. The right to privacy. *Harvard Law Review*, 4:193 – 220, 1890.
25. Bo Westerlund, Sinna Lindquist, and Yngve Sundblad. Cooperative design of communication support for and with families in Stockholm. Available at interliving.kth.se/papers.html, September 2001.
26. Alan F. Westin. *Privacy and Freedom*. Atheneum, New York NY, 1967.