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

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*.

While the first four aspects of privacy have by now been very well established in most legal frameworks around the world, often directly defined as constitutional rights, it is information privacy that creates most of the troubles today. Even though laws covering information privacy have been around for more than 30 years, the rapid progress

in technology, most recently the commercial success of the World Wide Web, continuously challenges legislation that has been initially devised in a time of room-sized mainframes and punch cards. The next section looks at two of the more influential pieces of privacy legislation – the US Privacy Act of 1974 and the EU Directive 95/46/EC of 1995 – and how they can influence the design of data processing systems such as ubiquitous devices and their infrastructure.

2.2 Legal Issues

While it was the small German state of Hesse that actually passed the world's first data protection law in 1970, one of the most influential pieces of early privacy legislation was the US Privacy Act of 1974. In defining the principles, the appointed governmental advisory committee created the notion of *fair information practices*, a significant policy development that influenced privacy policies worldwide. The principles of fair information practices, which in turn are based on work by Columbia University political economist Alan Westin, are basically as follows:

1. **Openness and transparency:** There should be no secret record keeping. This includes both the publication of the existence of such collections, as well as their contents.
2. **Individual participation:** The subject of a record should be able to see and correct the record.
3. **Collection limitation:** Data collection should be proportional and not excessive compared to the purpose of the collection.
4. **Data quality:** Data should be relevant to the purposes for which they are collected and should be kept up to date.
5. **Use limitation:** Data should only be used for their specific purpose by authorized personnel.
6. **Reasonable security:** Adequate security safeguards should be put in place, according to the sensitivity of the data collected.
7. **Accountability:** Record keepers must be accountable for compliance with the other principles.

Even though its principles of fair information practices were incorporated into all major pieces of privacy legislation worldwide, the Privacy Act of 1974 was no success at home [15]. In 1980, the Organization for Economic Co-operation and Development (OECD) codified the fair information practices in the OECD Guidelines [22] in order to prevent a proliferation of varied privacy protection laws that might harm economic growth by creating accidental trade-barriers.

While European countries continued to develop and refine omnibus protection acts covering both governmental and private data collection, US legislation followed up with a patchwork of sectorial laws that only addressed very specific needs as they arose (e.g., the Fair Credit Reporting Act of 1970, Video Privacy Protection Act of 1988, Family Education Rights and Privacy Act of 1994).

It took until 1995 before a similar influential piece of legislation would be passed again, this time in Europe. The European Union's *Directive 95/46/EC on the protection*

of individuals with regard to the processing of personal data and on the free movement of such data [14], often called "The Directive" for short, is for privacy legislation of the ending 20th century what the Privacy Act of 1974 was for the early privacy laws.

The Directive's main impact is two-fold. Firstly, its article 25/1 limits data transfers to non-EU countries only to those with "an adequate level of privacy protection." The lingering threat of being cut off from European data flows has prompted more than a dozen countries worldwide to revise their privacy legislation in order to comply with the provisions of the directive (in case of the US this resulted in a much debated self-certification framework called the Safe Harbor Principles [24] – more on this below).

Secondly, the Directive not only subsumes and refines the fair information practices described above, but its article 7 adds the notion of *explicit consent*: Personal data may only be processed if the user has unambiguously given his or her consent (exceptions are made for legal and contractual purposes). This practically disallows all types of data collection (except for when required by law) and requires a case-by-case explicit consent by the data subject.

As much as computing professionals would like to ignore legal issues when designing computer systems and only concentrate on the actual technical possibilities, the enactment of the Directive in 1998 created a milestone for privacy protection too large to ignore. While not all of the 15 EU member states have finalized their respective national legislation that will actually serve as an implementation of the Directive yet (the Directive only serves as a framework to create a common ground across legislation in all of its member states), its revised data protection requirements have long become a reality both within Europe and for countries doing business with Europe.

Already the e-commerce sector has begun pondering the implication of such legislation, and both new technology and regulation has been drawn up to support enactment of the Directive outside of Europe. The *Safe Harbor* agreement between the US and the European Commission serves as an experiment in self-regulation: in order to receive the designation "provides adequate level of privacy protection," companies willing to continue doing business with Europe need to self-certify adherence to a set of voluntary guidelines compatible with the spirit of the Directive, whose compliance will be overseen by the the Department of Commerce.

The effectiveness of this approach remains to be seen. US privacy advocates resent the Safe Harbor agreement in favor of a comprehensive, European-style privacy legislation for the private sector, while US companies itself are only slow to sign up for it: As of April 2001, only 30 companies have self-certified themselves to be in compliance with the agreement, the only major one being Hewlett-Packard [24].

No matter how well or quickly transnational agreements like Safe Harbor will get adopted: the Directive represents a new turn in the history of privacy legislation, both stressing the relevance of privacy protection in the age of digital data processing, and the importance of international cooperation in order to achieve it.

2.3 Does Privacy Matter?

"You already have zero-privacy anyway, get over it." This citation from Sun CEO Scott McNealy summarizes an increasingly common attitude toward privacy, as technology more and more allows comprehensive digital dossiers about every single person to be

compiled and queried in real time. While never before in history the average citizen has been more concerned with his or her personal privacy (as many public polls worldwide [8, 11, 17] repeatedly indicate), critics such as Amitai Etzioni, University professor at George Washington University, and Peter Cochrane, former head of Advanced Research and Technology at British Telecom Laboratories, argue that – more often than not – life is actually better without privacy.

Cochran [9] argues both from a technological and from an utilitarian point of view: "We have never enjoyed total anonymity in the past world of paper, so why should we expect it to be remotely possible in a world of bits?" Not only might it be infeasible to put into effect most of the well intended privacy legislation, it might actually do more harm than good: "Should I be knocked unconscious in a road traffic accident in New York – please let the ambulance have my medical record."

Etzioni [13] extends this argument for the better of society: If the FBI is able to decipher secret email messages, it can better prevent terrorists from planning their operations. If newborns are tested for HIV, immediate treatment can significantly increase their life expectancy while revealing information about their parents that those would rather avoid. With this approach, Etzioni is more in line with a traditional European perspective, one that puts much more trust in its governments than the US-American culture: Given sufficient democratic safeguards, governmental control benefits all citizens, as their representatives know what is good for society and will not abuse their powers.

Brin [7] has much of the same intent as Etzioni, but approaches it from a different, more traditional US perspective which distrusts government agencies, law enforcement, and big corporations per default. Brin argues that we can choose to make the increased surveillance of public places and buildings a setting for greater freedom. If not only a few powerful entities control such information, but if it is shared among all of us, everyone will be watching each other and thus have nothing to fear. He, too, suggests that surveillance technology could become a public resource to assure our safety and that of our children.

The issues raised by the authors above and their colleagues are as follows:

- **Feasibility:** what can technology achieve (or better: prevent)? All laws and legislation require enforceability. If privacy violations are not traceable, the much stressed point of accountability (as developed in the fair information practices) becomes moot.
- **Convenience:** the advantages of free flow of information outweighs the personal risks in most cases. Only highly sensitive information, like sexual orientation, religion, etc might be worth protecting. Semi-public information like shopping habits, preferences, contact information, even health information, might better be publicly known so that I can enjoy the best service and protection possible.
- **Communitarian:** personal privacy needs to be curbed for the greater good of society (trusting the government). Democratic societies may choose to appoint trusted entities to oversee certain private matters in order to improve life for the majority.
- **Egalitarian:** if everybody has access to the same information, it ceases to be a weapon in the hands of a few well-informed. Only when the watchers are being watched, all information they hold about me is equally worth the information I

hold about them. Eventually, new forms of social interaction will evolve that are built upon these symmetrical information assets.

The answer probably lies, as it does so often, somewhere in the middle. Clearly it won't be possible to provide a fail-safe, comprehensive privacy protection that can't be subverted. Clearly one has to balance privacy practices and goals with the convenience or inconvenience associated with them – if people need to go to great length to protect their privacy, they won't. Clearly there have been and there will be greater communitarian goods that should allow trusted entities to selectively curb some of our privacy – if they are properly overseen by independent organizations such as data protection commissioners common in Europe and many Commonwealth nations. And clearly society will and has to change, given the large changes that technology brings about – new forms of social interactions and ethics will evolve that will make things socially acceptable that haven't been so in the past.

What is important is to realize that all this still leaves much to be done in the field of privacy protection: Just where are the borders of technical feasibility when it comes to protecting our personal information? Just how much of our personal data should we be allowed to give up for the sake of convenience before society (or government, in most cases) steps in and prevents us from selling our soul? How are we to weight the greater good of society against our personal protection, and whom are we trusting with such sensitive issues? And last not least: how can we influence what will and what will not constitute acceptable social behavior in the future by designing our systems in a certain way that supports such behavior?

We will touch upon some of these critique in the Guidelines and Principles section further below, when we explore the design space for privacy-respecting ubiquitous systems. But first it might be in order to revisit the field of ubiquitous computing itself and examine it more closely in the light of the above-mentioned privacy issues: Why does work in the field of ubiquitous computing command a heightened awareness for privacy issues? What differences in our lives will an ubiquitous environment make, and how can we extrapolate from these changes on how future privacy codes must be implemented and used, given the existing ones?

3 Social Implications of Ubiquitous Computing

What is it that makes ubiquitous computing any different from other computer science domains with respect to privacy? Why should computer scientists in this particular domain be any more concerned with such vague notions of liberty, freedom, and privacy? Four properties come to mind:

- **Ubiquity:** Ubiquitous computing is everywhere – this is its essence, its explicit goal. Consequently, decisions made in ubiquitous system and artifact design will affect large, if not every part of our lives, from crossing a street to sitting in the living room to entering an office building.
- **Invisibility:** Not only should computers be everywhere, we want them to actually disappear from our views. With the ever shrinking form factor of computing and communication devices, this goal seems far from being science fiction. Naturally,

we will going to have a hard time in the future deciding at what times we are interacting with (or are under surveillance by) a computing or communication device.

- **Sensing:** As computing technology shrinks and processing power increases, so does the abilities of sensors to accurately perceive certain aspects of the environment. Simple temperature, light, or noise sensors have been around for quite some time, but next generation sensors will allow high quality audio and video feeds from cameras and microphones smaller than buttons. Even emotional aspects of our lives, such as stress, fear, or excitement, could then be sensed with high accuracy by sensors embedded in our clothings or in our environment.
- **Memory amplification:** Advancements in speech and video processing, combined with the enhanced sensory equipment available soon, make it actually feasible to perceive memory prosthesis, or amplifiers, which can continuously and unobtrusively record every action, utterance and movement of ourselves and our surroundings, feeding them into a sophisticated back-end system that uses video and speech processing to allow us browsing and searching through our past.

Database technology and (much later) the Internet already gave both researchers and implementers a taste of the social responsibility these systems entail. Lessig argues in [19] that technical decisions made during the design of any computer system, for example the TCP protocol, in effect constitute legal implications of what is and what is not possible to enforce or conduct in such a system. With the tremendous growth and ubiquity of the World Wide Web, computer technology affects far more than the rather small elite of techno-savvy academics, but reaches out to senior citizens and entire families as well.

Ubiquitous computing, with its far reaching implications described above, will take this entanglement of computer technology and society at large one step further (probably only the last step before we begin implanting computational devices into our body our even our consciousness). With a densely populated world of smart and intelligent but invisible communication and computation devices, no single part of our lives will per default be able to seclude itself from digitization. Everything we say, do, or even feel, could be digitized, stored, and retrieved anytime later. We may not (yet) be able to tap into our thoughts, but all other recording capabilities might make more than up for that lack of data.

In a sense, this might sound very familiar to those in the field of Artificial Intelligence, who have for almost half a century not only improved learning algorithms and devised ontologies, but also pondered the philosophical and social implications of thinking machines. Ubiquitous computing, in comparison, seems to come in low and fast under the radar screen: Most of its immediate applications sound far too mundane to excite the imagination of popular fiction authors in a way artificial intelligence has done. Philosophers and sociologists are not yet aware of the seemingly endless advances that processing power, storage systems, sensors, material science and miniaturization will offer us in the not too distant future. And legal scholars are still trying to make sense of the implications that todays or even yesterdays technologies such as border less hypertext (i.e., the World Wide Web) has brought upon national legislation created 20-30 years ago.

With only few people outside of the field being aware of the tremendous changes ahead, it falls upon ourselves to contemplate the effects of our doing. We cannot rely on lawmakers and sociologists to be fully aware of the vast possibilities and implications that the technology so obviously presents to us. It is us who need to understand the potential and danger of our advancements, and develop sound conventions and guidelines according to well-established principles that will help us drive technology into a responsible and socially acceptable direction.

4 Principles and Guidelines

Before we set out drawing up our guiding principles, we must focus on what exactly we are trying to accomplish, especially given the substantial critique set forth in section 2.3.

In particular, this means that we are *not* trying to achieve total security, let alone total privacy. Undoubtedly, professional surveillance by spies and private investigators will continue to happen, just as it has happened in the past. New technologies may be found that will be able to (partially) sniff out such surveillance devices. Eventually, better surveillance methods will counter this advantage again. The fact that there have been and always will be a few rotten apples will not spoil the whole batch of technical possibilities ahead for us.

What we can and will be able to achieve is prevent unwanted accidents – data spills of highly personal information that people who have never asked for it suddenly find at their doorstep. What we can do is allow people who *want* to respect our privacy to behave in such a way, so that we will eventually be able to build a long lasting relationship based on mutual trust and respect. And what should also be within our reach is achieving a good balance of convenience and control when interacting with ubiquitous, invisible devices and infrastructures.

Following the fair information practices and their recent enhancements through the enactment of the European Directive, we can identify seven main areas of innovation and system design that future research in ubiquitous computing will need to focus on. The next sections will elaborate each of the concepts in the order of both technical feasibility and relevance, ranging from the fundamental notion of notice and consent to the more general non-technical practices such as data minimization and use limitation.

4.1 Notice

The most fundamental principle of any data collection system (and ubiquitous systems will, in some respect, play such a role) is the Principle of Openness, or simply Notice. In most legal systems today no single data collection – be it a simple id tracking activity or a full fledged audio visual recording – can go unnoticed of the subject that is being monitored (that is, as long as the subject can be personally identified).

Again, ubiquitous devices will per definition be ideally suited for covert operation and illegal surveillance, no matter how much disclosure protocols are being developed. It will always take special detection equipment to be reasonably sure that a certain room or area is not being overheard by others. But openness goes a long way when we

want to prevent the mass-market "smart" coffee cup to turn *inadvertently* into a spy-tool par excellance! Imagine the casual user of a memory-amplifier-coffee-cup accidentally leaving her cup in her colleagues office – only to find in the evening that her colleague has spent most of the day gossiping about her, completely unaware of the spying coffee cup. Even though such accidental recordings for the most part cannot be upheld in courts, the damage is done and the social implications far outweigh the legal ones under such circumstances.

What would be helpful is some kind of announcement system, very much like a radio traffic announcement system, where car stereos will interrupt the playing of a CD or tape if an important traffic announcement comes up. Other analogies would be the `robots.txt` file on World Wide Web servers which allows Web robots to check for the "house rules" before excessively traversing a site, or the well-known emergency frequencies for radio communications that are reserved and constantly monitored for emergency communications. All these examples have in common the notion of a well-known mechanism, a well-known location for the publication of information. Clients interested in this particular information do not need to spend time and energy on searching for it, they can readily access it should such information be available (given that they know about the well-known location for publishing it).

Depending on the type of device, different announcement mechanisms would need to be found. Constant radio broadcasts, for example, would rapidly drain battery of small mobile devices, while it would be perfectly acceptable for rooms and buildings to ceaselessly announce such information. RFID tags could be used to passively announce data collection without using any batteries at all. The restricted storage size of such labels could be enhanced by outsourcing such information to a publicly available Web site and linking to it by merely placing its URI on the label.

As to what the format of such an announcement would be, a similar initiative for Internet Privacy has already covered a lot of ground in this area: The *Platform for Privacy Preferences* project, or P3P for short, has been developed at the World Wide Web Consortium (W3C) by a working group with representatives from industry, privacy advocate groups and universities [10]. P3P allows Web sites to describe their data collection practices in a machine readable way, which can then be read and displayed by P3P-enabled browser software. Users can configure their browsers to accept or reject certain types of policies (i.e., "reject any privacy policy that uses my home address for marketing purposes") and thus automate the nowadays tedious process of judging the acceptability of a sites practices.

Obviously, power consumption and connectivity problems in the field of ubiquitous computing will make it difficult to directly reuse results from Internet research projects. However, the main merit of this work lies in the carefully crafted privacy policy vocabulary: using XML as the encoding format, more than a dozen elements allow Web sites to accurately describe the data they collect, the purpose for doing so, the recipients of the data, their retention, and any dispute mechanisms they have in place in order to deal with customer complaints. The difficulties of coming to a consensus for a vocabulary that is acceptable to both privacy advocates and industrial marketers alike probably accounts for much of the 3 years this project has taken. It is currently in its final phase and

already a number of both Web sites and software developers have begun incorporating the protocol into their systems.

Using a declaration format like P3P and announcing it via one or more well-known mechanisms would form the bottom line for any privacy-aware ubiquitous system. Depending on the actual setup of the system, a single announcement might cover a multitude of devices. For example, an office building might make such an announcement for all of the devices that are installed inside, whenever someone enters through its front doors. Rooms in the building might repeatedly reference this main declaration for all sensors or devices the room is equipped with. A wearable system, on the other hand, might be represented by single declaration from its owner's cell phone. Single, autonomous devices that can be operated independently of such central services would require their own announcement capabilities. For example, a future coffee cup with a sophisticated memo function would need to be able to announce its data collection practices even in the absence of any central unit the holder might wear (as long as the cup would actually collect any data without such a central unit).

Not every single device would need to be identified in such an announcement. The goal is to exhaustively enumerate all *types* of data collected, not the individual devices doing so. It does not really matter how many sensors record audio data in a certain room - the fact that audio recording is done at all is the important information. Collation is always possible, and overstating the actual data collection perfectly legal. An office building could collectively declare that audio recording is done in all of its room, even if not all of them actually had sensors equipped. It is up to the owner of the device or system to decide if such overstatement is in her best interest. Of course, certain practices might not be legal in most countries, which place severe restrictions on surveillance such as wiretapping or video recording (see more about that in the use limitation section below).

4.2 Choice and Consent

With the enactment of the EU Directive that refined and extended the well-known fair information practices, it is not enough anymore to simply *announce* and *declare* data collection - it also requires collectors to receive *explicit consent* from the data subject. The Directive thus effectively prohibits any collection and usage of personal information, except for certain legal procedures (law enforcement, public health, etc) or when explicitly consented by the individual.

The most common form of explicit consent nowadays is still the written contract. By showing the signature of the data subject under a corresponding piece of text, collectors can in most cases effectively demonstrate that they have received the explicit consent of the subject. In the world of electronic transactions, however, explicit consent is not that easy to come by.

Even though digital signatures based on public-key cryptography are a well established concept, the actual usage of such signatures is still in its infancy. So far, no public-key-infrastructure (PKI) has actually achieved widespread usage, which makes the actual verification of signatures, as well as their revocation, difficult.

But it is not only a question of authenticity that makes digital signatures hard to use, it is also the requirement of explicitness: A certain statement may very well be

signed with the secret key of a certain individual, but had the individual actually any knowledge of signing that particular statement, or was it her personal software agent that handled the task in the background, without the user's knowledge?

In electronic commerce, such explicit consent is often achieved by requiring the press of a button to initiate data transfer. In a ubiquitous computing setting, a press of a button might not only be physically impossible (because none of the devices present support a tactile interface), it might also be unusable: With hundreds of devices from a multitude of collectors constantly querying my information as I walk down a busy street, pressing the OK button on my cell phone every time I want to authorize transfer will surely annoy even the most patient person.

Another often overlooked problem the notion of consent poses to system design is the requirement of choices: With only one option available, getting consent comes dangerously close to blackmailing. Imagine that in order to enter a public building, you must agree to completely unacceptable practices. Certainly you could always walk away from such a deal, but can you really? (Some might argue that this is no different from most supermarkets today, which already feature a comprehensive video surveillance system. In most legal systems, such surveillance is possible under very restrictive guidelines that place restrictions on purpose, use, and retention of such video feeds.)

In order to make consent a viable option, more than the "take it or leave it" dualism must be offered. Office buildings could offer me to track my position within the building in order to offer customized navigational services. If I choose to decline, it must be possible to selectively disable the tracking functionality without either shutting down the whole system for all other visitors, or me not entering the building.

Advancements in audio and video processing might make such choices available for selective recordings: Instead of requiring all participants of a meeting to consent to a comprehensive audio or video recording, the system could only track those who agree to the recording, while the voices of all others will be muted, their picture on videos anonymized. A simple solution along similar lines was used in the Classroom 2000 project at Georgia Tech, where classroom recordings would focus on the teacher and his replies, while voices and faces of students where deliberately of low quality [2].

4.3 Anonymity and Pseudonymity

Given the difficulties in asserting explicit consent in electronic communications, one viable alternative to personal data collection are the notions of anonymity and pseudonymity. Not only are they an important option when offering clients a number of choices (so that those who wish to remain anonymous can remain so), they also allow the legal collection of certain types of data without requiring user consent.

Anonymity can be defined as "the state of being not identifiable within a set of subjects." The larger the set of subjects is, the stronger is the anonymity [23]. A large number of both free and commercial anonymity services are already in widespread use on the World Wide Web. Using anonymizing proxies, for example the popular `www.anonymizer.com`, or more sophisticated "mixes", like the "Freedom" software product of the Canadian software company Zero-Knowledge, Internet users can already today hide their IP address from the Web site hosting the accessed page.

Even though the technology behind such services is already well established, such methods might not be feasible in a ubiquitous computing environment. Communications between small ubiquitous devices will often happen in a much more dynamic environment, where long chains of communication (like they are used in mixes) might not last long enough because devices constantly enter or leave the scene. Direct communications on the other hand often disclose my real identity, unless wireless protocols would be adapted to use one-time addresses instead of their fixed hardware (MAC) address (as it is done in the Bluetooth standard). Sensing hardware is also different from network cards: My real-world appearance, unlike my cyberspace one, cannot be disguised that easily – any video camera can get a clear enough shot of me if it's pointed at my face.

Anonymity has also disadvantages from an application point of view. Being anonymous prevents the use of any application that requires authentication or offers some form of personalization. Pseudonymity is an alternative that allows for a more fine grained control of anonymity in such circumstances: by assigning a certain ID to a certain individual, this person can be repeatedly identified until she changes to a different ID. Using the same pseudonym more than once allows the holder to personalize a service or establish a reputation, while always offering her the possibility to step out of that role whenever she wishes.

Whether anonymous or pseudonymous – if data cannot be traced back to an individual (i.e., if it is unlinkable), the collection and usage of such data poses no threat to the individuals privacy. Consequently, legal frameworks such as the EU Directive lay no restriction on the collection of anonymous (or pseudonymous) data. Determining when certain type of information can be linked back to a person, however, is more often than not subject of debate. For example, even randomly generated pseudonyms might be linkable under certain circumstances: In case a pseudonym is used in conjunction with a certain fact that is easy to identify in a sufficiently small set, linking becomes trivial. An active badge might be programmed to change its ID every five minutes, though the fact that the tracking system is able to exactly pinpoint its location would make this change obvious (and thus linkable) in the logs.

Data-Mining technology allows much more remote coincidences to be assembled into a single coherent picture, therefore greatly increasing the potential of *any* type of information to be used for linking. Although German privacy-commissioners have argued for placing severe restrictions on the use of data-mining applications [1], their call might not be realistic.

4.4 Proximity and Locality

It seems that our above observations regarding the feasibility of certain desirable aspects in a privacy-aware ubiquitous system – such as clear notices, explicit consent, and unlinkable pseudonymity – might prove too difficult for efficient and reliable implementation. One possibility to face this technological reality while still preserving some desirable state of protection, even when this means some form of sociological adjustment, are the principles of proximity and locality.

The idea of proximity is basically a practical solution to much of what makes notice and consent hard. Instead of announcing each and every data collection, taking care to

get the required consent, and handle those frequent cases where various people do not give their consent, imagine the following: Future society (and with it the legal system) will accept the fact that personal gadgetry (like coffee mugs or "smart" clothing) can record conversations and behaviors *whenever its owner is present*. Just as if people would never forget a thing they witnessed. Note that this does not mean that people would suddenly be omniscient – their memory prosthesis (i.e., their coffee mugs) would only grant them the gift of indefinite recollection (currently most legal systems treat any recording without the explicit consent of all parties as surveillance, which is only allowed by law enforcement in certain, court-ordered situations). In case the owner would accidentally leave such a device so that it could witness a conversation or meeting of other people in her absence, all sensory equipment would be turned off until the owner's presence would be detected again.

Such a detection mechanism could be simple. Of course, future advanced sensors could use biometry to check if the cup's owner is actually holding it. It could also use the presence of certain IDs in the clothing of the owner as a trigger: Only if a certain predefined signal would be emitted from the owner's wearable computer, its sensors would be operational. The problem would be further simplified if the cup's data storage would be outsourced to the holder's wearable computer: In this case it would be sufficient to simply check for the presence of any type of outsourcing facility, in effect acting as a collection device for anybody holding the cup (or sitting next to it).

Although this would alleviate a number of technical problems, recording each and every conversation and behavior would be more than just chatting with friends who suddenly have very good memory. Storage also allows your friends playing this information to people unknown to you, who then effectively witness events they were no part of. While one might still be comfortable with the idea of friends having a good recollection of past discussions together, one would certainly be less comfortable with their friends playing their recordings to a group of strangers for entertainment value.

Along similar lines as the idea of proximity aims the notion of *locality*. Instead of working out complicated authentication protocols that govern the distribution of collected information, so that it is in compliance with whatever recipient information has been previously announced, information could simply be tied to places at which it is collected. Should a table in a room on a ground floor be allowed to ask the flowerpot on the hallway outside to contact the light fixtures in the staircase for the information that the soda machine on the 3rd floor is currently acquiring? Should my printer tell everybody walking by what it is printing at the moment, only to have them pass this information on to the people they meet on the subway or at the airport, until this data ends up on the other side of the world?

In essence, one would require that information is not disseminated indefinitely, even not across a larger geographic boundary, such as buildings or rooms. Information collected in a building would stay within the building's network. Anybody interested in this information would need to be actually physically present in order to query it. Once present, however, no additional authentication would be required anymore – the printer in the hallway would be happy to tell anybody passing by and stopping for a chat which documents (and by whom) were printed on it last night.

This concept resembles privacy protection (or the lack of it) in small, rural communities: Everybody knows everything about each other, and is only too happy to tell. Once someone leaves the boundaries of the village, however, access to information about its inhabitants becomes difficult, if not impossible. Though word of mouth allows information to travel far beyond the originating locality, the information value drastically decreases with increasing distance.

In such a scenario, observing anything from a larger distance becomes impractical. Even though it is not impossible to acquire certain information, it ultimately requires physical locality to its source. This wouldn't be too far from our current status quo where law enforcement or private investigators routinely interview witnesses for their version of the events – only that coffee mugs and tables cannot talk. Not yet.

4.5 Adequate Security

Not surprisingly, talking about privacy almost always leads to security considerations. In most discussions, the significance of the latter is often perceived much higher than that of the former. The idea is tempting: once we solve security, that is, once we are able to achieve authenticity and trusted communications, privacy will be a by-product that follows inevitably from a secure environment.

Secure communications and storage methods have been around for quite some time, and security experts are constantly refining the algorithms to keep up with the rapid technological development. However, ubiquitous devices will introduce a whole new set of constraints, mainly in the areas of power consumption and communication protocols: there is only so much energy to power an embedded processor in, say, a felt pen, that it will perhaps not be enough to compute the product of two 2048-bit prime numbers. And a pair of smart shoes will probably pass a store front in a few seconds, barely enough time to go through with an orderly security protocol for establishing a secure communication.

Even with GHz Desktop power, security experts question if absolute security can ever be achieved. True, 2048-bit public key encryption is probably secure for the foreseeable future. But in order to prevent misuse, keys need to be encrypted by pass-phrase, which invites the usual problem of choosing nicknames of family members or friends, or writing them down next to the keyboard. Smartcards are often hailed as the ultimate personal security device, but these, too, need to be protected from unauthorized use once they fall into the wrong hands. And even if biometrics will ever allow us to use our fingerprints or retinas to replace personal passwords, key distribution and management for tens and hundreds of small and miniature personal devices (everything from socks to umbrellas to door knobs) will almost certainly challenge the most clever user interface.

We can reduce much of this complexity by employing robust security only in situations with highly sensitive data transfer, such as financial transactions, or the transfer of medical information. In most other cases, the principle of proportionality applies: cracking a 512-bit key might be feasible given the proper hardware, but if cracking the code would mean a reward of only $10, this would hardly be worth the effort. Similarly, sending temperature data from a sensor to its base station might not need to be encrypted at all. After all - if an eavesdropper is close enough to overhear its low-power

radio communication taking place, he might as well sense the current temperature by himself.

Here the principle of locality becomes relevant again: if we start broadcasting otherwise innocuous information like temperature or noise levels from a certain local context across many hops to physically distant (or separated) places, we effectively create surveillance devices. If, however, such data is sent only locally and not transmitted further, the lack of encryption is of no concern, therefore simplifying implementations at a reasonable level of compromise.

The important aspect to realize is that security might not be the panacea it appears to be, and it might not need to be that panacea either. If we consequently apply principles like proximity, locality, and proportionality, much of our basic infrastructure could indeed function without any explicit security model at all, while still adequately respecting the privacy needs of its users.

4.6 Access and Recourse

Trusting a system, and especially a system as far reaching as a ubiquitous one, requires a set of regulations that separate acceptable from unacceptable behavior, together with a reasonable mechanism for detecting violations and enforcing the penalties set forth in the rules. Both topics belong more into the realm of legal practice, where laws and codes of conduct will need to be revised or newly established in order to address the special requirements of typical ubiquitous computing environments.

However, technology can help implementing specific legal requirements such as use limitation, access, or repudiation. Augmenting a P3P-like protocol with something like digital signatures would allow for non-repudiation mechanisms, where parties could actually prove that a certain communication took place in case of a dispute. Database technology could provide data collectors with privacy-aware storage technology that would keep data and its associated usage practices as a single unit, simplifying the process of using the collected data in full compliance with the declared privacy practices. Sophisticated XML linking technology could enable the data subject direct access to his or her recorded information in order to enable the required access rights.

The principles of Collection and Use Limitation set forth in the fair information practices can further simplify such access requirements. In essence, they require data collectors to

- only collect data for a well-defined purpose (no “in-advance” storage)
- only collect data relevant for the purpose (not more)
- only keep data as long as it is necessary for the purpose

Together with anonymization or pseudonymization, these principles might save both time and effort that would otherwise be spent in order to properly collect, protect, and manage large amounts of sensitive personal information.

5 Summary and Outlook

What lies at the intersection of privacy protection and ubiquitous computing is easy to imagine: the frightening vision of an Orwellian nightmare-come-true, where countless

"smart" devices with detailed sensing and far-reaching communication capabilities will observe every single moment of our lives, so unobtrusive and invisible that we won't even notice! Ron Rivest calls this the "reversal of defaults": "What was once private is now public", "what was once hard to copy, is now trivial to duplicate" and "what was once easily forgotten, is now stored forever." Clearly, "something" needs to be done, as nearly all work in ubiquitous computing points out, yet little has so far been accomplished.

Some of the principles mentioned above seem readily implementable, given the proper protocols: limiting the number of communication hops any message can travel enforces locality; creating simple proximity behavior for personal devices prevents unwanted surveillance; and devising communication protocols that use temporary, random IDs can provide some base-line anonymity. Implementing other guidelines might require a good amount of work: finding the adequate security settings for a given scenario (there might be widely different requirements for certain parts of a system), deriving low-power transparency protocols that are both expressive and compact enough, and creating a simple mechanism for pseudonymity-based identity management. Some of this might be achieved by porting existing solutions to a low-power environment, others might need to be re-engineered from scratch. Some large research effort will probably be required to fulfill needed trust requirements (implementing digital signatures and their corresponding public-key infrastructure) and back-end systems (privacy-aware databases and access technologies).

As important as it is to take existing laws and codes of practices into account, which can and must serve as important guidelines for creating privacy-respecting infrastructures – it is equally important to remember that laws can only work *together* with the social and technological reality, not against them. If certain legal requirements are simply not enforceable, technological or procedural solutions need to be found, or the law changed.

Maybe it is indeed time that we face the new technological realities and accept the fact that personal data collection will continue to advance and erode privacy as we know today. But new paradigms will take place of old and unrealistic assumptions, and new forms of human interactions will evolve in society, just as we have learned to live with the specters (i.e., modern photography) that haunted Warren and Brandeis more than 100 years ago.

References

1. 59th Conference of Privacy-Commissioners in Germany. Data Warehouse, Data Mining und Datenschutz. See HTML version of the resolution passed at `www.datenschutz-berlin.de/doc/de/konf/59/datawa.htm`, March 2000.
2. Gregory D. Abowd and Elizabeth D. Mynatt. Charting past, present and future research in ubiquitous computing. *ACM Transactions on Computer-Human Interaction, Special issue on HCI in the new Millenium*, 7(1):29–58, March 2000.
3. Philip E. Agre and Marc Rotenberg, editors. *Technology and Privacy: The New Landscape*. The MIT Press, 1998.
4. Helmut Baeumler, editor. *E-Privacy*. Vieweg Verlag, Braunschweig, Germany, 2000.
5. Victoria Bellotti and A. Sellen. Design for privacy in ubiquitous computing environments. In *Proc. of the European Conference on Computer-Supported Cooperative Work*, 1993.

6. Oliver Berthold and Hannes Federrath. Identitaetsmanagement. In Baeumler [4], pages 189–204.
7. David Brin. *The Transparent Society*. Perseus Books, Reading MA, 1998.
8. Business Week/Harris Poll. A growing threat. *Business Week*, March 2000.
9. Peter Cochrane. Privacy. Sovereign, May 1999.
10. Lorrie Cranor, Marc Langheinrich, Massimo Marchiori, and Joseph Reagle. The platform for privacy preferences 1.0 (p3p1.0) specification. W3C Candidate Recommendation, HTML Version at `www.w3.org/TR/P3P/`, December 2000.
11. Lorrie Faith Cranor, Joseph Reagle, and Mark S. Ackerman. Beyond concern: Understanding net users' attitudes about online privacy. Technical Report TR 99.4.3, AT&T Labs-Research, April 1999.
12. Mike Esler, Jeffrey Hightower, Tom Anderson, and Gaetano Borriello. Next century challenges: Data-centric networking for invisible computing. In *Proceedings of MobiCom'99*, Seattle, 1999.
13. Amitai Etzioni. *The Limits of Privacy*. Basic Books, New York NY, 1999.
14. European Commission. Directive 95/46/ec of the european parliament and of the council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, November 1995.
15. Robert Gellman. Does privacy law work? In Agre and Rotenberg [3], chapter 7, pages 193–218.
16. Ruediger Grimm, Nils Loehndorf, and Philip Scholz. Datenschutz in Telediensten (DASIT). *DuD - Datenschutz und Datensicherheit*, 23(5):272–276, 1999.
17. Harris Interactive. IBM multi-national consumer privacy survey, October 1999.
18. Marit Koehntopp and Andreas Pfitzmann. Datenschutz next generation. In Baeumler [4], pages 316–322.
19. Lawrence Lessig. *Code and other Laws of Cyberspace*. Basic Books, New York NY, 1999.
20. James Michael. *Privacy and Human Rights: An International and Comparative Study, With Special Reference to Developments in Information Technology*. Dartmouth Pub Co. / UNESCO, 1994.
21. E. Mynatt, M. Back, R. Want, M. Baer, and J. Ellis. Designing audio aura. In *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI'98)*, Los Angeles, CA, April 1998.
22. Organisation for Economic Co-operation and Development (OECD). Recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data, September 1980.
23. Andreas Pfitzmann and Marit Koehntopp. Anonymity, unobservability, and pseudonymity – a proposal for terminology. In Hannes Federrath, editor, *Proceedings Workshop on Design Issues in Anonymity and Unobservability*, volume LNCS 2009. Springer Verlag, 2001.
24. US Department of Commerce. Safe harbor website. `www.export.gov/safeharbor/`.
25. Samuel Warren and Louis Brandeis. The right to privacy. *Harvard Law Review*, 4:193 – 220, 1890.
26. Alan F. Westin. *Privacy and Freedom*. Atheneum, New York NY, 1967.
27. William Pitt, Earl of Chatam (1708–1778). Speech on the excise bill.