INTERNATIONAL TELECOMMUNICATION UNION

ITU WORKSHOP ON UBIQUITOUS NETWORK SOCIETIES

Document: UNS/05
April 2005

Original: English

ITU NEW INITIATIVES PROGRAMME — 6-8 APRIL 2005

PRIVACY AND UBIQUITOUS NETWORK SOCIETIES

BACKGROUND PAPER

March 2005

ACKNOWLEDGEMENTS

This background paper was prepared by Gordon A. Gow, Lecturer in the Department of Media and Communications at the London School of Economics and Political Science. The New Initiatives Project on "Ubiquitous Network Societies" is managed by Lara Srivastava <lara.srivastava@itu.int> under the direction of Tim Kelly <tim.kelly@itu.int>. Country case studies (Italy, Singapore, Japan and Korea) on ubiquitous network societies, as well as two additional background papers can be found at http://www.itu.int/ubiquitous.

The author wishes to acknowledge Sonia Livingstone, Robin Mansell and Lara Srivastava for their support during the various stages of this report. The author also wishes to thank Eija Kaasinen and Ilka Korhonen from the VTT Technical Research Centre of Finland, and Professor Kimmo Raatikainen, Martti Mäntaylä, and Patrik Floréen from the Helsinki Institute for Information Technology, for taking time to provide comments on the subject matter. Sulya Fenichel provided assistance with formatting and report preparation. The opinions expressed in this document are those of the author and do not necessarily reflect the views of the International Telecommunications Union.

TABLE OF CONTENTS

LIST OF BOXES

LIST OF TABLES

1 INTRODUCTION

The BBC News technology website recently reported on a consumer study indicating that a majority of people in the UK have serious privacy concerns related to radio frequency identification (RFID) tags, believing that these tags can be read from a distance and thereby exposing them to unwanted surveillance.[1] RFID tags are an emerging technology that combines a microchip with antenna, making it possible to read the contents of the chip with a radio scanner, and represent a powerful new innovation in micro-computing and wireless networking. Despite the privacy concerns, many of those responding to the survey also recognized that RFID tagging could provide real benefits in the form of, lower retail costs, convenience, and crime detection.

The ubiquitous network society, however, presents a more fundamental problem for privacy rights than what may be suggested by its early incarnation in the form of RFID tags; namely, that the very conceptualization of the systems that will make this vision possible require that personal information be collected, used, and disclosed on a massive scale and under very different conditions from which we are familiar with in today's world.

If we are to begin to understand the intimate link between personal information, privacy and ubiquitous networks, a first step is to understand the vision and its various social, technical, and regulatory dimensions. From here, it may be possible to structure an informed and progressive debate on this vital issue at the heart of emerging networks and the societies we wish to build with them.

1.1 Context and aim

This paper is one of three thematic papers to be presented at the New Initiatives Workshop on 'Ubiquitous network societies', held 6-8 April 2005 in Geneva Switzerland, and hosted by the International Telecommunications Union. In addition to the other thematic papers on RFID and network traffic management, there are country case studies from Japan, Korea, Singapore and Italy.

The aim of this paper is to stimulate discussion and debate on privacy in ubiquitous network societies by providing important background information and a sample of recent perspectives on the issue. As such, the paper does not attempt to provide clear answers to the problems identified, but instead has been written with a view to contributing to a better understanding of the subject matter, in part by reflecting critically on the issue of privacy as a cross-cutting concern that includes technical, regulatory, and social considerations.

The very term 'ubiquitous network societies», as many readers will acknowledge, is problematic given the variety of assumptions that might be brought to bear on it. As such, the paper sets out one particular interpretation of the term in the introductory section, and then uses it as a baseline concept by which to develop and discuss the issue of privacy.

1.2 Weiser's vision for third generation computing

In 1991 computer scientist by the name of Mark Weiser published a paper in *Scientific American* titled 'The computer for the 21st Century.' Weiser and his team at the Xerox Palo Alto Research Center (PARC) in California had in 1988 begun to invent a vision of a third generation of computing systems, and this article was its first introduction to a mass readership. Essentially the vision described the historical transition from large mainframe computers of the 1960s and 1970s, to the standalone desktop personal computer (PC) of the 1980s and 1990s, and finally toward the networked computing appliance of the future. Third generation computing was presented as an integrated system of advanced computing devices, intelligent interface design, and anytime, anywhere data communications.

Weisner (see Box 1.1) coined the term 'ubiquitous computing' to describe this third wave of computing systems, which marked the initial articulation of a vision looking toward future ubiquitous network societies. What is most significant about Weiser's vision is that while it pre-dated the Web by a few years, it clearly embodies the idea of pervasive networked computers, assuming all kinds of shapes and located in all kinds of unconventional settings. Essential to the vision is electronic networking, for without the ability of these computing devices to communicate with one another the functionality of such a system would be extremely

limited. In a later paper published in 1993, Weiser made this requirement clear, stating that the next generation computing environment would be one 'in which each person is continually interacting with hundreds of nearby wirelessly connected computers.'[2] At the time such forms of wireless networking were primitive at best, but today with the likes of WiFi and Bluetooth, the possibilities for such dense local area networks are entering the realm of commercial reality.

Box 1.1: Ubiquitous Computing
In 1991 computer scientist Mark Weiser set out a future scenario for information and communication technologies characterized by three main innovations:

- Computing devices will become embedded in everyday objects and places;
- Designers will develop intuitive, intelligent interfaces for computing devices to make them simple and unobtrusive for users;
- Communications networks will connect these devices together and will extend to become available anywhere and anytime.

Source: Text LSE; Image: http://www2.parc.com/csl/members/weiser/

1.3 An international perspective

While one side of the Atlantic Ocean was working on a vision known as ubiquitous computing, or 'ubicomp', the European Union began promoting a similar vision for its research and development agenda. The term adopted within this international setting is 'Ambient Intelligence' but it seems to share most of the same features as Weiser's ubiquitous computing scenario, while perhaps giving more emphasis to the vision as an integration or convergence of three key innovations in micro-computing, user interface design, and ubiquitous communications networks. See Box 1.2.

In May 2000, the Information Society Technologies Advisory Group (ISTAG) commissioned the creation of four scenarios 'to provide food for thought about longer-term developments in Information and Communication Technologies', with the intent of exploring the social and technical implications of Ambient Intelligence, and to provide a point of departure for structuring ICT research under the Sixth Framework Programme of the European Union. Among the findings, the scenarios suggested a set of 'critical socio-political factors' that will be critical to the development of Ambient Intelligence, including the issue of security and trust. In particular, the report stated that 'a key aspect is management of privacy: more open systems tend to lower privacy levels [where] technological developments are outpacing regulatory adjustments.'[3]

The scenarios developed for and assessed in the ISTAG report were regarded as a first step toward the creation of a research agenda in the EU that would contribute to the development of 'trust and confidence enabling tools' for the management of privacy within an Ambient Intelligence context.

Japanese policy initiatives in this field have adopted the term 'ubiquitous network society' to describe a vision that in many respects may be ahead of that in other parts of the world, suggesting a future initiative under the label 'U-Japan Strategy» to replace the current 'e-Japan' policy framework.[4] Similarly, a recently held policy roundtable titled 'Realizing the Ubiquitous Network Society' addressed a range of issues that appear to be closely associated with the EU's Ambient Intelligence research program. Results from the roundtable are intended as input to Japan's emerging technology policy beyond 2006 and centre on a normative view that the country 'must realize a ubiquitous network society in which convenient communications without restrictions will be allowed via broadband platforms, to which diversified equipment including [consumer equipment] will be connected.' The final report of this roundtable was

published in late 2004 and has been posted on the website of Japan's Ministry of Internal Affairs and Communications (Japanese only at the moment).[5]

Box 1.2: Ubiquitous Computing versus Ambient Intelligence?

'Ubiquitous Computing (Ubicomp) and/or Ambient Intelligence (AmI) refer to a vision of the future information society where humans will be surrounded by intelligent interfaces supported by computing and networking technology that is everywhere, embedded in everyday objects such as furniture, clothes, vehicles, roads and smart materials. It is a vision where computing capabilities are connected, everywhere, always on, enabling people and devices to interact with each other and with the environment. Computer devices are becoming increasingly small and cheap, interconnected and easy to use in order for them to find application in all aspects of our everyday lives. Computing capabilities will therefore not only be available in computing devices but also in everyday objects. These devices will be able to sense, think and communicate.'.

Source: Punie, Yves. (2003). A social and technological view of Ambient Intelligence in Everyday Life (Technical Report EUR 20975 EN): Institute for Prospective Technological Studies, Directorate General Joint Research Centre, European Commission.

1.4 A corporate vision

While IBM is credited with coining the term 'pervasive computing' to refer to a shift in corporate computing systems, Philips Research has chosen the term 'ambient intelligence' to describe a new paradigm for home computing and entertainment.

One of the first prototypes developed by Philips is a system that supports 'smart home' applications based on collection and use of personal information that allows the creating of user preferences and profiles for customizing entertainment and other applications. One example of this idea has been given the name 'PHENOM' and is designated as a long-term research project at Philips. The idea behind PHENOM is to create an in-home environment that is aware of the identity, location and intention of its users, and that might eventually perform like an electronic butler. To support this prototype, researchers have designed 'an intelligent Memory Browser system' that 'recognizes multiple users, devices and objects, and learns from their behavior.'[6]

Similar work is being done (see Box 1.3) at the crossroads between industry and academia under the name Project Oxygen at the Massachusetts Institute of Technology (MIT) in the United States.

Box 1.3: Project Oxygen at MIT

Perhaps one of the most well known corporate/academic partnerships for developing ubiquitous ICT prototypes and applications is located at the Massachusetts Institute of Technology (MIT) and called the Oxygen Lab. The name is intended to emphasize the 'ambient' quality of such technologies. Project partners include Hewlett-Packard, Nippon Telegraph and Telephone (NTT), Nokia, and Philips Research.

'Oxygen enables pervasive, human-centred computing through a combination of specific user and system technologies. Oxygen's user technologies directly address human needs. Speech and vision technologies enable us to communicate with Oxygen as if we're interacting with another person, saving much time and effort. Automation, individualized knowledge access, and collaboration technologies help us perform a wide variety of tasks that we want to do in the ways we like to do them.

Oxygen's device, network, and software technologies dramatically extend our range by delivering user technologies to us at home, at work or on the go. Computational devices, called Enviro21s (E21s), embedded in our homes, offices, and cars sense and affect our immediate environment. Handheld devices, called Handy21s (H21s), empower us to communicate and compute no matter where we are. Dynamic, self-configuring networks (N21s) help our machines locate each other as well as the people, services, and resources we want to reach. Software that adapts to changes in the environment or in user requirements (O2S) help us do what we want when we want to do it.'

Source: http://oxygen.lcs.mit.edu/

Whereas companies like Philips are engaged in an ambitious vision that involves the private domain within the walls of the home, more mundane scenarios marking an important step toward ubiquitous network society are being implemented today, often crossing into public space. One example is the growing use of RFID tags (radio frequency identification tags)[7] to enable supply chain and inventory management in the private and public sectors. These tags represent an early entry point into pervasively networked environment, involving a radio-enabled microchip attached to an object (e.g., item of clothing, or shipping container) that can be read by a radio receiving device.

A recent survey conducted for the Information Technology Association of America, for instance, revealed that of a large number of US government IT executives interviewed, over half of them 'described RFID as an emerging technology that would improve government processes, indicating that applications for RFID technologies within government organizations likely will support homeland security, asset visibility, business process and productivity improvements.'[8] Despite the fact that privacy concerns about its use remains controversial, there is a strong interest in the use of RFID systems within the asset management community. To the extent that RFID systems are the thin edge of the wedge in the move toward ubiquitous network societies has already started.

1.5 A growing area of attention

The essential qualities of the ubiquitous network society vision are invisibility and pervasiveness. The visionaries dream about the computer 'disappearing' into the background while at the same time becoming ever more central to our daily lives through the presence of pervasive electronic communications networks. Is this a utopian vision? Or perhaps it is more appropriate to describe it as dystopian? When Howard Rheingold first conveyed this vision to readers of *Wired* magazine in 1994, the response was clearly mixed with some readers taking issue with Weiser's use of the term 'dissent' to describe those who might refuse to participate in such a system. The point was that ubiquitous networks clearly do have 'Orwellian implications' as Rheingold plainly observed, and one critic of such a vision suggested that if we are to avoid slipping into an unprecedented society of near-total surveillance, our normative or 'default' stance on the design of such systems should be 'offline' or otherwise unconnected.[9]

These were early days for the ubiquitous network vision and the simple formulation of the 'offline' default stance may have seemed a valid proposal at the time but it is far less feasible today in a world where mobile phone ownership has exceeded fixed line connections globally, prompting an 'always-on' culture of electronic communications practices. Similarly, the ubiquitous network vision has had time to mature since its introduction in 1991 and our understanding of its privacy implications are far more sophisticated in part from the work of those involved in the technical fulfilment of Weiser's original vision. Research into privacy and ubiquitous networks, for instance, has been taken up by numerous research projects located around the world, in at least two special issues of academic journals, and is featured as a regular topic for papers and panels at numerous conferences (see Box 1.4).

Box 1.4: Selected research on privacy and the ubiquitous network society

- Swiss Federal Institute of Technology (Zurich), Institute for Pervasive Computing, http://www.vs.inf.ethz.ch/
- University of California at Berkeley, Information Privacy in Ubiquitous Computing, http://guir.berkeley.edu/projects/ubicomp-privacy/
- *Pervasive Computing* (IEEE journal), http://www.computer.org/pervasive/about.htm
- *Personal and Ubiquitous Computing* (ACM journal), http://springerlink.metapress.com/app/home/journal.asp?wasp=cmw755wgwq3kqkbukgur&referrer=parent&backto=searchpublicationsresults,1,1;
- Ubicomp.org (annual conferences since 2002), http://ubicomp.org/ubicomp2005/
- IEEE annual Conference on Pervasive Computing and Communications, http://ubicomp.org/ubicomp2005/
- European Conferences on Computer Supported Collaborative Work (papers and panels on ubiquitous computing and privacy), http://insitu.lri.fr/ecscw/
- ACM annual Conference on Computer and Communications Security, Workshop on Privacy in the Electronic Society (WPES), http://seclab.dti.unimi.it/~wpes/

Source: LSE

1.6 Ubiquitous Network Societies: A working definition

This background paper will adopt the term 'ubiquitous networks' to describe the convergence and interconnection of computing devices—some with advanced user interfaces others being simple sensors and detectors—with a pervasive communications network comprised of both wireline and wireless segments. A ubiquitous network society will also include both public and private information spaces, such as those that might provide real-time public information on traffic or public transit conditions versus virtual private networks for commercial fleet tracking, inventory management, or other forms of corporate communications.

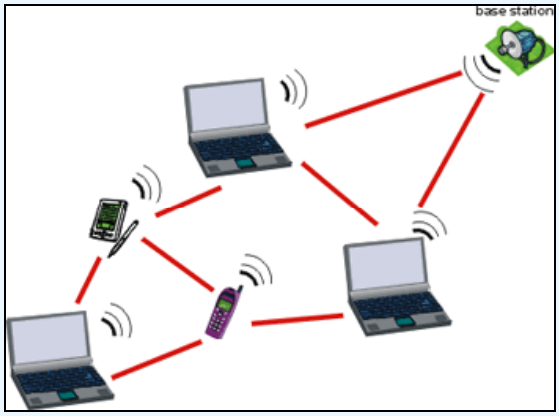
If we combine the public and private distinctions with another important classification based on the architectural design of ubiquitous networks, we create a basic classification scheme that divides the field into quadrants, each with possibly distinct privacy concerns. For example, some ubiquitous networks will be comprised of fixed to mobile connections, such as that with traditional mobile phone networks or the 'ActiveBadge' type system first developed by Weiser's team at Xerox PARC in the early 1990s. In each of these examples, a mobile client interacts with a fixed network infrastructure by using a wireless connection.

Other ubiquitous networks will be comprised of mobile-to-mobile connections (see Box 1.5). With this architecture, a mobile device interacts directly with another mobile device, sometimes referred to as 'ad hoc' networking. If more devices are introduced into the arrangement, a 'mesh network' may be created comprised entirely of mobile nodes. In most cases, particularly in commercial applications, much ubiquitous networking will include a gateway interconnection to a server over a fixed line infrastructure. Nonetheless, ad hoc networking will become more significant as protocols such as WiFi and Bluetooth continue to be adopted in the marketplace. In fact, a serious privacy concern for Bluetooth has already been observed in the case of so-called bluejacking of mobile phones. In a 'bluejacking' incident, a mobile phone user sends an anonymous message to another mobile phone in the vicinity—usually to a stranger whose mobile phone has been left in 'discoverable' mode. For some individuals, being bluejacked may simply be an annoying intrusion of privacy, but some experts have suggested that it could have more insidious consequences for the transmission of viruses and for attempts to gain unauthorized access personal information contained on mobile phones in public places.

Box 1.5: Ubiquitous Network Architectures

Ubiquitous networks will include two types of basic designs: fixed-to-mobile and mobile-to-mobile, also known as ad hoc networks. A fixed-to-mobile network resembles the current cellular mobile phone networks, where a mobile client interacts with physically situated base stations. In a mobile-to-mobile arrangement, mobile clients work together to act as repeaters, creating a mesh of interacting hubs.

The image depicted here shows an ad hoc network comprised of laptop computers, a PDA, and a mobile phone. These are connected to each other and to the Internet through gateway access provided by the base station. In a ubiquitous network society, such ad hoc networks might include a wide range of micro-computing devices and sensors located in both public and private spaces.



Source: http://www.ercim.org/publication/Ercim_News/enw57/santi.gif

2 INFORMATION PRIVACY AND UBIQUITOUS NETWORKS

2.1 Understanding privacy

Privacy is a central issue in ubiquitous computing vision and has been identified as such from its earliest inception. Many in the research and development community clearly recognize the inherent challenge that an invisible, intuitive and pervasive system of networked computers holds for current social norms and values concerning privacy and surveillance.

The inherent privacy challenge from ubiquitous computing, at least as it stands as a design concept today, stems from two innovations necessary to its success: the enhanced ability to collect data on people's everyday interactions (in multiple modalities and over large spans of time and space) and an enhanced ability to quickly search large databases of that collected data, creating greater possibilities for personal profiling, and other forms of data mining.[10] One leading researcher in the field has identified a set of generic privacy concerns that ubiquitous networks will very likely raise for users:[11]

- A pervasive network of interconnected devices and communications will mean that the sheer quantity of personal information in circulation will increase greatly;
- The introduction of perceptual and biometric interfaces for certain applications, will transform the qualitative nature of personal information in circulation;
- In order to personalized services, ubiquitous networks will require the tracking and collection of significant portions of users' everyday activities.

If users are to be persuaded to participate in a ubiquitous network society then they will need to be given a reason to trust that their privacy will be protected at all times (see Box 2.1). The challenge is daunting if we consider the privacy concerns and mistrust that have followed from the introduction of RFID tags and smart cards into the marketplace. For instance, an American group called Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) have been lobbying against the use of RIFD tags in consumer products, publishing an ominous warning on the website spychips.com:

> 'Unlike a bar code, [RFID] chips can be read from a distance, right through your clothes, wallet, backpack or purse—without your knowledge or consent—by anybody with the right reader device. In a way, it gives strangers x-ray vision powers to spy on you, to identify both you and the things you're wearing and carrying.'[12]

The rhetoric of 'x-ray vision' and corporate conspiracy that is sprinkled throughout CASPIAN's website could be criticized for being alarmist and even inaccurate with respect to the limits of current RFID technology, but given that these very early steps toward a ubiquitous network society have the ability to create such a furor, what might be in store for a the far more ambitious undertakings proposed by the visionaries?

Box 2.1: The Privacy Paradox

The following are excerpts from researchers working on the technical design of ubiquitous networks and devices. Their comments reflect the inherent privacy paradox created when designing pervasive, 'invisible' systems, such as those characterized in Mark Weiser's ubicomp vision or by proponents of Ambient Intelligence.

- 'Ubiquitous computing usually implies embedding the technology unobtrusively within all manner of everyday objects which can potentially transmit and receive information from any other object. The aims are not only to reduce its visibility, but also to empower its users with more flexible and portable applications to support the capture, communication, recall, organisation and reuse of diverse information. The irony is that its unobtrusiveness both belies and contributes to its potential for supporting potentially invasive applications.'[13]
- 'By virtue of its very definitions, the vision of ambient intelligence has the potential to create an invisible and comprehensive surveillance network, covering an unprecedented share of our public and private life...' [14]

Source: http://media.hunton.com/pracareas/photos/tech_privacy.jpg

2.1.1 What is privacy and why is it an important value?

From a political standpoint privacy is generally considered to be an indispensable ingredient for democratic societies. This is because it is seen to foster the plurality of ideas and critical debate necessary in such societies. In order to expand on this claim, some ubiquitous network developers have turned to legal scholar Lawrence Lessig's writing to identify specific reasons for protecting privacy.[15] The resulting list is based on four arguments:

- Privacy empowers people to control information about themselves;
- Privacy is a utility that protects people against unwanted nuisances, or the right to be left alone;
- Privacy is related to dignity in the reciprocal obligations of disclosure between parties;
- Privacy is also a regulating agent in the sense that it can be used to balance and check the power of those capable of collecting data.

Lessig's list of reasons for protecting privacy belongs to what Colin Bennett and Charles Raab have called the 'privacy paradigm'—a set of assumptions based on more fundamental political ideas: 'The modern claim to privacy … is based on a notion of boundary between the individual and other individuals, and between the individual and the state. It rests on notions of a distinction between public and private. It rests on the pervasive assumption of a civil society comprised of relatively autonomous individuals who need a modicum of privacy in order to be able to fulfil the various roles of the citizen in a liberal democratic state.'[16]

The importance of this observation is that it helps to put into question the notion of privacy, and suggests that our commonly accepted ideas may not be the only perspective. For instance, critics of the privacy paradigm may call into question the motives for wanting privacy in the first place, arguing that it supports tendencies toward anti-social behaviour or that it promotes selfish thinking whereby the welfare of the individual is placed above that of the community. Taking this idea one step further, Bennett and Raab point out that some critics 'might even argue that some of the most creative civilizations in history—such as ancient Greece and Rome, and Renaissance Italy—flourished despite, or maybe because of, the lack of individual privacy.'[17]

In spite of the potential for debate on the finer points of the issue, privacy is clearly a value that is important in modern societies and will likely remain so for some time to come (see Box 2.2). The difficulty lies in establishing a balance between the rights of the community and those of the individual, particularly in the face of new technologies that dramatically increase our ability to collect and use personal information. In many cases, this ability is a desirable innovation to the extent that it can improve the efficiency of governments and businesses, thereby reducing costs to citizens and consumers. On the other hand, such technological developments threaten to sustain a surveillance society involving pervasive data collection from our public lives and unwanted intrusions into our private actions through data mining of our ever-expanding information trails. Ubiquitous networks embody the potential for both, and it is this ambiguity which could transform privacy into an issue that computer scientist Mark Ackerman terms a 'killer threat' to their very success in the future.

Box 2.2: Changing Ideas about Privacy?

Is 'privacy' a universal value the same across all cultures and historical periods? Or does the idea of privacy itself change in relation to history and our technological developments? It appears that researchers working on ubiquitous network systems are asking these same questions, suggesting that we may need to re-examine our basic assumptions about privacy in the future.

'Designing policies that realize the full potential of pervasive technologies while simultaneously protecting privacy begins with understanding the interaction of these elements with one another. Such understanding *is a critical element in deciding what we, as a society, want the new social norms to be*.' [emphasis added] [18]

'What should smart things be permitted to hear, see, and feel? And whom should they be allowed to tell about it?' [19]

'…these emerging technologies have forced us to ask a very important question: What are the implications of these [technological] challenges for the meanings that we, as a society, want to assign to personal privacy and for the legal protections that we want to give to it?' [20]

Source: Various (see endnotes).

2.1.2 A point of clarification of terms

A number of terms are used when discussing privacy and privacy-related concerns and ubiquitous networks. Among these are five common concepts, each with slightly different connotations:

- Privacy
- Anonymity
- Surveillance
- Security
- Trust

'Privacy' and 'anonymity' are related concepts, but with some important differences. With respect to communications, privacy implies the possession of personal information and the subsequent terms and conditions by which it is used, retained, and disclosed to others. Anonymity, however, implies an absence of information about a person and relates to the terms and conditions by which such information might be collected in the first instance. Both concepts highlight the importance of empowering people to control information about themselves.

'Surveillance' is also related to privacy, but implies something quite specific as the intentional observation of someone's actions or the intentional gathering of personal information in order to observe actions taken in the past or future. Unwanted surveillance is usually taken to be an invasion of privacy. This concept highlights the importance of privacy as a utility that protects people against unwanted intrusions and the right to be left alone.

'Security' is a term often used in software development to describe the capability of a technical system to protect and maintain the integrity of personal data circulating within that system. Privacy violations can occur when a system is not secure and it leaks personal data to unauthorized parties. This concept highlights the importance of providing regulating mechanisms to balance and check powers of those that provide and those that collect data.

Finally, the term 'trust' suggests the quality of a reciprocal relationship between two or more parties with respect to the use and disclosure of personal information and the respect of privacy rights. This concept highlights the importance of dignity and mutual obligations between human beings (often interacting through corporate or other bureaucratic systems.

Each of these concepts has a distinct emphasis, which is important in the range of considerations affecting ubiquitous networks; however, for the sake of simplicity in this paper the term 'privacy' will be used to refer to them as a bundle of related issues and concerns.

2.2 Studying privacy and emerging technologies

Insofar as the ubiquitous network society remains a vision of the future, it poses a challenge for identifying and debating specific privacy implications today. Such an undertaking therefore calls for a bit of technological foresight on the one hand, which leads to its own pitfalls in terms of predicting how a technological system might develop and become adopted by a society. On the other hand, however, this situation also poses a unique opportunity to the extent that the ubiquitous network vision represents a technology project in its earliest stage of development and which is therefore most open to social shaping in accordance with social norms and desires.

The work of Wiebe Bijker is often cited in studies that consider the social shaping of technological systems, especially those that emphasize the indeterminate character of such systems in the early stages of research and development.[21] The method used in researching this paper was adapted from Bijker and is based on 'the principle of symmetry,' which is a core tenet of the social shaping approach to technology policy research. Essentially, the principle of symmetry states that investigators should accept all problem formulations as equally valid during the early stages of a technology project. The idea contrasts with other research approaches that seek to identify the correct solution as something that only needs to be uncovered, rather than something that is 'constructed' through the interactions of various stakeholder groups with an interest in the technology. With the issue of privacy and ubiquitous networks, however, it is the case that there are

many different problem formulations found in the technical and social policy literatures, and reflected in the focus of various research projects. The principle of symmetry proscribes fair regard for all of these formulations, with the idea that each of them may offer critical insights into the future possibilities of this technology project.

In this paper the term *technology project* has been adopted to make an important distinction between relatively 'closed' technological systems (e.g., GSM for mobile phones) with open-ended, contingent, and indeterminate efforts such as those that characterize the current state of ubiquitous networking.

Respecting the principle of symmetry, the 'ubiquitous network society' is a technology project—a site where social actors and technical elements come together, and where stakeholder groups attempt to persuade other groups as to the merits their *problem formulation* (often drawing on empirical research to support a claim to 'truth') and the consequent *design propositions*. Design propositions emerge from problem formulations and represent attempts by stakeholder groups to establish a specific technical system, usually with intended (as well as unintended) implications for social practice and public policy. When several stakeholder groups have different problem formulations, it is likely that a number of alternative design propositions will also be put forward.

This theoretical approach to studying technology projects is useful to the extent that it frames the issue of privacy and ubiquitous networks as an ongoing project of many possible outcomes, and suggests the some specific questions that may shed light on this complicated socio-technical process:

- Who is interested in the privacy issue as it relates to ubiquitous networks?
- How is the problem of privacy formulated in relation to the various elements and actors involved in ubiquitous networks?
- What are the proposed designs to solve the privacy problems that have been identified?

In addressing these questions, the research for this paper has involved a detailed review of peer-reviewed literature and informal consultations with those in the research and development community involved in activities variously termed 'ubiquitous' or 'pervasive' computing, or 'ambient intelligence' as the case may be. A growing number of journal articles are now reporting on the problem of privacy in ubiquitous network systems and a growing community of researchers is now at the forefront of this technology project, defining the problem of privacy as it might be imagined, and proposing solutions intended to support the viability and adoption of future commercial systems.

2.3 Three domains of information privacy

It is helpful to acknowledge that there are three domains of information privacy, each of which is distinct but also necessarily related to the others:

- The technical domain
- The regulatory domain
- The sociological domain

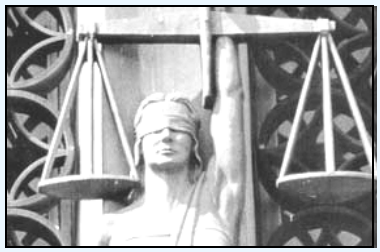
Within the technical domain privacy is taken up as a design issue related to such areas as network security and user interface design. The regulatory domain takes up privacy as an issue in the context of data protection and related statutes and regulations. The sociological domain, by contrast, considers privacy as a social issue related to cultural practices, ethics, and institutions (see Box 2.3). Problem formulations and design propositions for privacy and ubiquitous networks will assume some proportion of these three domains. For example, a research study that considers the importance of gaining consent in the collection and use of personal information will make assumptions about the feasibility of technical solutions based on perceptions of social behaviour and cultural norms, and perhaps counting on the presence of certain regulatory obligations to provide a legal framework favourable to the proposed technology.

The following section will discuss each in turn, noting a number of subdomains to further develop the framework for studying privacy and ubiquitous networks.

Box 2.3: Three Domains of the Privacy Problem

It is useful to divide the problem of privacy and ubiquitous network societies into three distinct domains. While each of these domains raises its own unique set of problems and proposed solutions, they are also interdependent:

Technical solutions



Regulatory Solutions

Social solutions

Source: http://www.eurocosm.com/Application/images/Innovations/fingerprint-lock-2.jpg; http://www2.sjsu.edu/justicestudies/images/justice.jpg; http://www.mnstate.edu/schwartz/

2.3.1 The technical domain

The technical domain can be subdivided into four layers that correspond roughly to the functional building blocks of all communication systems, including ubiquitous networks. This so-called layer model approach is based on the OSI-reference model used in system design and recently adapted for technology policy research.[22]

All layer models share the same basic feature of classifying electronic services into a set of distinct but interconnected functional strata. In some cases, the layer model is put forward as an enhancement to the traditional 'silo' model used where communication systems have been traditionally conceived of as separate systems more or less divided into standalone vertical stovepipes such as voice telephony, radiocommunications, and broadcasting. Within the layer model, these vertical silos are replaced by a series of horizontal, functionally distinct, but interacting, subsystems. The layer model may be more appropriate for ubiquitous networks, given the centrality of digital convergence to their design.

One version of this model, for instance, consists of four layers arranged from bottom to top (following the OSI convention), from physical systems based on hardware elements to more logical systems based on software elements. The primary layer is that of 'physical infrastructure,' which includes the provision of transmission capacity and basic physical interfaces. The second layer is that of 'network services,' which includes the provision of routing and gateway services. At the third layer is 'value-added services' that provide access to information content. Finally, at the fourth layer is 'information services' where content is created and supplied to or from the end user.[23]

A simple example of the layer model in action is the delivery of a weather bulletin to a mobile phone through short message service (SMS). A combination of wireline and wireless infrastructure (layer one) must enable end-to-end connectivity between a content provider and a handheld wireless device; network services (layer two) then enable the correct routing (and perhaps billing) for the data from the content provider's network, perhaps through a series of gateways, on to an intermediary public network and eventually to the appropriate wireless service provider and the correct cell-site location for radio transmission to the mobile client device that has requested the information.

In this scenario a variety of suppliers are required to support this relatively simple service. At layer one, a physical infrastructure operator is required to provide end-to-end connectivity. In some cases where large distances or organizational boundaries are crossed, several layer one operators may be involved in the physical delivery of the data through routers and other software elements (layer two). The wireless carrier, or perhaps a third party service provider, must operate a portal (layer three) that enables access to weather bulletins for its customers by creating a special user profile account. Finally, a content provider (e.g., a national meteorological bureau) must supply weather data either in a raw or customized form (layer four).

All the layers must work together in a secure fashion order to provide customers with a trusted communications service.

Using this model it is possible to identify a number of distinct subdomains of privacy concerns that tend to reside in each of the layers. For instance, at the physical layer, privacy concerns may revolve around the need for encryption of transmissions over public and private infrastructure; at the network layer, the question of anonymity is often raised particularly with respect to spam and the use of "anonymizing" servers; at the value-added services layer, privacy concerns range from the placement of cookies on web browsers to more insidious threats of spyware and trojan horses entering through insecure backdoors of applications, and at the information services layer, we often come across privacy issues related to consent and the use of personal details gathered at websites or through other forms of electronic transactions.

2.3.2 The regulatory domain

In order for the otherwise technical domain of 'data processing' to crossover into the regulatory domain of information privacy, a number of actions must take place. For example, a report from the Electronic Privacy Information Center at Duke University looking at location-based services in mobile environments distinguishes three discrete operations needed to transform raw data into personal information.[24] The first of these is the initial gathering of transaction-generated data, the second is the processing of that data in order to transform it into useful information, and the third is the application of that information to enhance commercial or public services. In a ubiquitous network setting, for instance, a service provider might collect raw location data (e.g., in the form of geographical coordinates) from a mobile client device and transform it into a visual representation on a map using Geographic Information System (GIS) software, and then supply that information back to the customer as a value-added service for personal navigation.

This discrete set of actions is reflected in the regulatory and policy domain as four distinct subdomains of information privacy: (1) the initial *collection* of personal information and (2) subsequent *use* and (3) *disclosure* of that information, and (4) the *preservation* and *retention* of information. With these distinctions in mind, it is also important to recognize that transaction-generated data unto itself is not necessarily equivalent to 'personal' information, although it has been argued elsewhere that in some instances it should be regarded as equivalent.[25] For example, location information gathered as part of routine traffic data in mobile phone networks might be interpreted as both transaction-generated information and personal information, to the extent that it indicates the presence of an individual. Where the latter classification provides for more extensive privacy protection, which is often the case in regulatory arrangements, the distinction may be important for consumers and operators alike.

Nevertheless it is clearly the case that the gathering of such data and its use and disclosure in combination with other kinds of information—what one privacy scholar has termed the 'coordinability' of identity traits—could provide the basis for the creation of personal, even intimate, profiling of customers and users of ubiquitous networks.[26] Moreover, stakeholder groups looking to the development of commercial location-based services for mobile phones (and other mobile client devices) have clearly identified this data-matching operation as essential to their business plans. The technical function of data processing in communication networks is therefore an activity closely aligned with information privacy concerns in the regulatory domain (see Box 2.4).

Indeed, this vital aspect of data-capture and data-matching for customer profiling is behind both the blessed vision and dreaded 'Orwellian' curse of the ubiquitous network society, or what we might call the privacy paradox. More significantly, however, the layer model described in the section above suggests that privacy concerns may not be of the same magnitude or type within each segment or operation of a ubiquitous network. Each discrete operation might involve a different set of actors and network elements handling customer or transaction-generated data, thereby creating a hand-off or boundary problem for the management of security and privacy in such networks (see Box 2.5).

Box 2.4: Data Matching for Location Based Services

Location information by itself is of little value to service providers. It is only by data-matching that location information with other customer properties that a profile can be created for delivering value-added services. It is this data-matching process that transforms raw impersonal data into privacy-sensitive information.

Those working in the location-based services sector for mobile clients clearly understand the importance of being able to carry out data-matching as integral their business plans:

'… knowledge of the user's location is only part of the problem. Depending on where, when, how, with whom, and why customers are navigating in physical space, their needs will vary. … Even if the LBS [location-based services] provider was able to push information or advertising with great reliability to these customers, they might have an extremely difficult time figuring out what the customer is doing or want at that location in real time.

… There is an urgent need for sophisticated mobile marketing techniques based on detailed knowledge of customer profiles, history, needs, and preferences. Information existing in customer databases developed by retailers like Amazon.com, for example, can be used in parallel with location-based information.[27]'

Source: http://www.esri.com/news/releases/03_1qtr/graphics/orangecell-lg.jpg http://www.bargainpda.com/assets/2718.jpg

Those stakeholder groups with an interest in promoting ubiquitous network services must address this boundary problem in both technical terms (network security) and in terms of harmonization of regulation and policy across various jurisdictions by taking into account transnational, domestic legal, industry self-regulation and other instruments currently in force or under consideration. In the not too distant future, ubiquitous network services will likely be provided within a diverse range of contexts, ranging from local areas networks, urban environments, and ultimately encompassing global roaming. Privacy protection in one setting must be assured in other settings if these services are to be viable, which suggests that regulation and policy on transborder data flows, encryption and security will have a powerful influence on their development and scope of deployment.

Box 2.5: The Problem of Trust Boundaries

'At the heart of the ubiquitous computing vision lies an inherent contradiction. On the one hand, a computing environment must be highly knowledgeable about a user to conform to his or her needs and desires without explicit interaction—almost reading the user's mind. On the other hand, a system that is truly ubiquitous will encompass numerous users, physical regions, and service providers. At such large scale, perfect trust among all parties is an unattainable ideal. Trust boundaries thus represent seams of discontinuity in the fabric of pervasive computing'.

Source: Satyanarayanan, M. (2003). Privacy: The Achilles Heel of Pervasive Computing? *IEEE Pervasive Computing*, 2 (1), 2-3.

Finally, the potential availability of transaction-generated data and personal information profiles is of considerable interest to law enforcement, national security and public safety organizations. The regulatory and policy domain can be therefore subdivided into two further subdomains, one stemming from state interests and referred to as 'lawful access' and/or 'public safety' provisions, the second to private commercial interests in the general area of 'electronic commerce' (see Box 2.6).

The current regulatory domain consists for four predominant types of policy instruments: data protection laws, anti-spam laws, freedom of information policies, and lawful access provisions. For instance, in the UK there are four distinct statutes governing information privacy concerns. The UK Data Protection Act which applies to all organizations that process personal information. It provides a set of enforceable principles intended to protect personal privacy and gives individuals the right access information about themselves held by those organizations. All organizations that handle personal information in the UK must register with the government as data controllers.[28]

The Freedom of Information Act in the UK gives people the general right of access to information held by or on behalf of public authorities. It introduces publication schemes to improve the amount and quality of information routinely made available to the public by public bodies, and establishes the right to ask public authorities for any information they hold.[29]

The UK Privacy and Electronic Communications Regulations are based on a European Commission Directive and cover network and service providers and individuals, using public available electronic communications service, particularly for direct marketing purposes. It is primarily concerned with direct marketing activity by telephone, fax, or email. In terms of the layer model, it addresses concerns raised at layers two and three, by establishing provisions that discourage anonymous distributions systems and provide an accountability regime for those involved in direct marketing activity by electronic means.[30]

The Regulation of Investigatory Powers Act governs the interception of communications, including setting the terms and conditions by which the UK government and designated agencies can acquire lawful access to communications data, conduct intrusive or covert surveillance, and gain access to encrypted data. In terms of the layer model, this statute addresses a number of concerns at the physical layer (layer one) subdomain.[31]

In countries where steps toward a ubiquitous network society are perhaps farther along, new policy guidelines and types of legislation have been introduced in an effort to address new challenges to information privacy. For instance, Japan has embarked on policy efforts to reduce social anxiety and threats to privacy caused by the widespread adoption and use of RFID tags in that country. The Japanese Ministry of Public Management, Home Affairs, Posts and Telecommunications (Soumu-Sho) and Ministry of Economy, Trade and Industry (Keizai-Sahgo Sho aka METI) jointly released a set of RFID Privacy Guidelines in 2004, including provisions for consumer awareness, regulations on collection and use of data gathered by RFID tags, and accountability provisions for data handlers using RFID tags.[32]

Recent advances in mobile phone technology have also created an information privacy problem for those visiting saunas or swimming pools, or trying to protect access to other forms of visual information. A security expert speaking about the situation in Korea is quoted as having said, 'You should think that at least three cameras are watching you when you're in public.' In response, the Korean Ministry of Information and Communication (MIC) and Telecommunications Technology Association now requires all camera phones to have clicking noises as loud as 60db to 68db, and major handset makers such as Samsung and LG, are now required to add clicking sounds that are activated when their camera phones take a picture. However, it seems that users have already come up with several ways to mute the clicking noise, making this information available to others through the Internet.[33]

Box 2.6: Privacy, Electronic Communications and Emergency Access

In the European Union a distinction is made in Article 10 of the EC Directive on Privacy and Electronic Communications (2002/58), which on the one hand requires subscribers to actively consent ('opt-in') to the use of their location information while, on the other hand, directing network operators to ignore '… the temporary denial or absence of consent of a subscriber or user for the processing of location data, on a per-line basis for organisations dealing with emergency calls and recognized as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of responding to such calls.[34]'

While the Directive assumes a telephone call as the primary mode of contact, it is reasonable to assume that other network client devices, such as those that might become prevalent in a ubiquitous network would not be exempt from such requirements. A similar provision is contained in American legislation passed following the launch of the FCC mandate to create nationwide Wireless E9-1-1 capability. The Wireless Communications and Public Safety Act was passed in 1999 and requires a service provider to disclose any and all subscriber information that 'is in its possession or control' including information pertaining to subscribers whose have chosen to be otherwise 'unlisted' in a public directory.[35] Again, this statute appears to be aimed principally at telephony but it has clear implications for any form of wireless communications service that might be useful in responding to an emergency or aiding in an investigation.

Source: European Commission

2.3.3 The sociological domain

The sociological domain of information privacy can be subdivided into at least three subdomains: (1) the differences between activities that take place in public versus private space; (2) the importance of social power relations in the control over personal information *inflows* as well as information *outflows*; and (3) the importance of consumer education and awareness related to information privacy threats and protections.

The distinction between public and private spaces, and the related privacy concerns, is a matter far less straightforward than one might think. Sociologist Gary Marx, for instance, has made this case in describing privacy as a 'border crossing' problem—similar in some respects to the boundary crossing problem found in the technical domain. Clearly data-matching and legitimate customer profiling in a ubiquitous network environment will require the assembly of bits of information from a range of sources collected in both public and private domains. One simple example is the use of RFID tags to track an inventory of groceries in the kitchen as a means of communicating to a commercial server that supports 'smart' shopping application in a grocery store. In this case, information is collected in the private domain of the customer's home, is then transited across a public telecom network, and then used by a commercial service provider to provide a value-added service in a retail space.[36] Several boundaries or borders are crossed in providing this service, each of which raised serious concerns with trial participants and which have distinct implications for the protection of information privacy.

Marx's work in this area has attempted to highlight the problem of establishing a fixed distinction between public and private spaces, stating that 'the public and the private involve multiple meanings over time and across cultures, contexts, kinds of persons and social categories». One simple example is the treatment of email in corporate settings, where security policies may vary widely. A strong policy might treat all email over the corporate network as 'public' in the sense that administrators and managers may request access to such communications. In a different office setting, however, such communications might be treated as personal and 'private' and thereby given a higher order of protection from third party interceptions. To sort out the conceptual difficulties that arise in determining public and private distinctions, Marx has identified a set of parameters for consideration, three of which are particularly relevant for the problems created by ubiquitous networks: [37]

- Legally defined places, either geographical or in terms of information access;
- Customary expectations concerning public and private distinctions;
- Accessibility of information to non-enhanced senses (i.e., without an artificial detection device)

Based on these parameters, a more nuanced formulation of the public/private space model might include the idea of unique information spaces within, for example, an office building where various levels of permissions and privacy requirements are established based on the activities and resources present in those physical locations. Similarly, it would raise the problem of the status of data produced by human bodies and possibly detected by network-enabled sensors to measure presence or movement.

The key to the privacy problem as it pertains to notions of public and private space is in the violation of personal borders, regardless of how it is done. These personal borders may be natural ones (clothes, walls or closed doors, or sealed packages that contain information), or these borders may involve social norms (expectations as to confidentiality with certain people such as doctors or lawyers); or they may involve spatial or temporal borders related to old information (e.g. deleted files) or bits of history of one's past. Ubiquitous networks may permit new opportunities for violations in each of these types of border crossing, particularly in the spatial and temporal factors. Computer scientist Frank Stajano, for instance, has noted that with the running costs of data storage dropping so dramatically in recent years, 'there is no economic requirement ever to delete anything. Whatever was once digitized is now stored forever. This property, which I shall call *denied oblivion*, is the source of many new privacy problems.'[38] Stajano's denied oblivion describes a scenario in which events from one's past are forever potentially retrievable, creating an emergent border crossing threat. Some in the research and development community have drawn explicitly on Marx's border crossing model to structure their work on information privacy for ubiquitous networks.[39]

A related problem to privacy in the sociological domain is that of 'anonymity', where people wish to interact with others but to conceal some features of their identity. In addition to his border model of privacy, Gary Marx in a related study suggests that there are several discrete forms of identity knowledge. When used in

combination these traits may reveal relatively unique patterns of behaviour, thereby rendering anonymity difficult to achieve in practice: [40]

- Legal name given to a person
- "Locatability" of a person in space
- Pseudonyms (traceable or untraceable) used by a person
- Patterned behaviour of a person
- Social or physical attributes of a person
- Symbols of eligibility/non-eligibility (e.g., member of a club)

As regards issues of power relations in the micro-social settings of everyday life, an early and widely cited paper on privacy in ubiquitous computing environments establishes a framework for assessing the design of networked systems and control over personal information. Examining the social domain from the perspective of system design, Belloti and Sellen identified 'two classes' of problems related to information privacy in ubiquitous network environments. The first of these is related to what we might term the 'hostile observer' and is primarily a security-related concern. The second type of problem, however, addresses a more difficult problem related to everyday life of the user and control over the flows of personal data that a ubiquitous network system may enable:

> 'Mediated interactions between people via technology are prone to breakdowns due to inadequate feedback about what information one is broadcasting and an inability to control one's accessibility to others. This disrupts the social norms and practices governing communication and acceptable behaviour.'[41]

Further in the paper, Belloti and Sellen identify two concepts to explain how such breakdowns might lead to potential privacy intrusions:

> 'The underlying causes of such problems lie in the fact that the technology results in *disembodiment* from the context into and from which one projects information … and *dissociation* from one's actions. These phenomena interfere with conveying information about oneself or gaining information about others.' [emphasis in original][42]

While the authors are concerned primarily with human-computer interface (HCI) design as a method of preventing intrusions on privacy, their paper also highlights inherent tensions in the relationship between information inflows versus outflows that are likely to be present in a ubiquitous network environment. For instance, the paper formulates the privacy problem as one of information *control* and *feedback*. More specifically, the authors refer to these as 'two important principles,' that seek to empower the user to stipulate what information about them is being collected, used, disclosed, and retained. While the principles are clearly desirable from a social and human rights standpoint, the feasibility of putting them into practice is another story, as will be seen when this paper turns to consider the range of design propositions put forward by the community of ubiquitous network experts.

Consumer education and awareness is another subdomain of information privacy concerns that falls within the sociological domain (see Box 2.7). The growth of electronic communications systems and massive collection of personal information even in today's world, makes it extremely difficult for consumers to know when information about them may be collected or to understand their rights with respect to the collection or use of their personal information. Such challenges extend to the complicated privacy policy statements found on websites or in service agreements that are routinely ignored by people and even when carefully examined may not be fully comprehended by those without some degree of legal training.

To further complicate this subdomain, there may be instances of individuals who clearly show a blatant disregard for their information privacy, and simply ignoring warnings. An often cited study by Westin suggests, for instance, that it is possible to identify three distinct groups of attitudes in relation to information privacy: the marginally concerned, the privacy fundamentalists, and the privacy pragmatists. Whereas the marginally concerned are mostly indifferent to privacy concerns, the privacy fundamentalists are uncompromising and proactive in their protection of personal privacy. Most people tend to fall into the pragmatist camp, willing to trade personal information if the benefit seems appropriate.[43] Given the

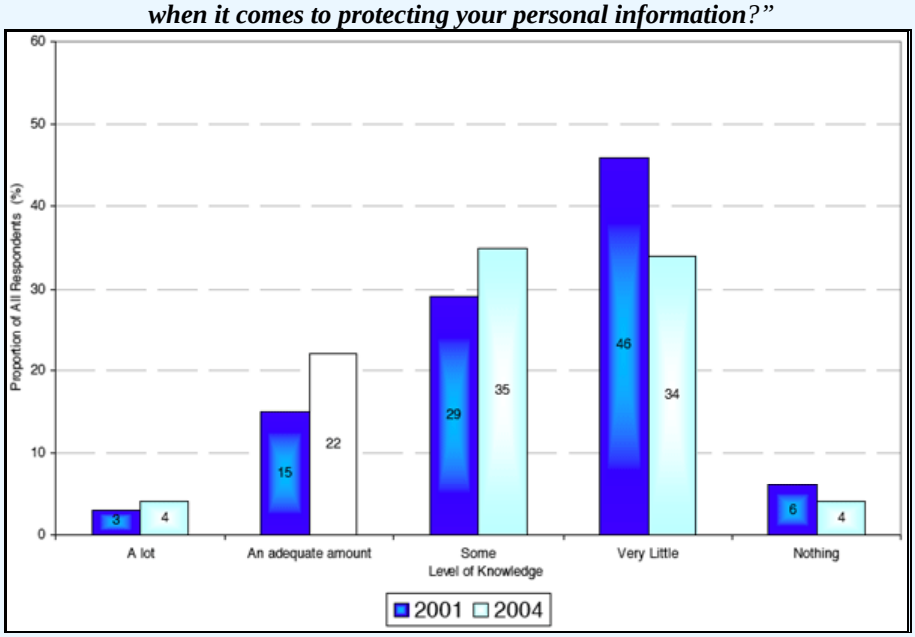
prominence of this utilitarian motive, it seems all the more important to make consumers aware of the pitfalls in order that they can make informed judgements.

Box 2.7: Knowledge about Rights to Personal Information Protection

Responses to an Australian Privacy Commissioner 2004 survey on community attitudes toward privacy indicate that members of the public may not be well informed about their rights when it comes to the protection of personal information. For instance, the study asked respondents: *How much would you say you know about your rights when it comes to protecting your personal information?* The results were then compared to those obtained in a 2001 survey. The 2004 report states:

'Since 2001, respondents report a greater knowledge about their rights to protect their personal information. However levels of knowledge are still low, with only one in four respondents claiming to know an adequate amount or more about their privacy rights as a whole. One group that appears to have better knowledge now than in 2001 is the 18-24 year olds. In the 2001 study, 52% of the younger respondents (18-24) claimed to know very little about their rights to protect their personal information. By 2004, this had reduced to 36%, which is not significantly different to the rest of the population 18+.'[44]

Responses to the question asked: "How much would you say you know about your rights when it comes to protecting your personal information?"



Source: http://www.privacy.gov.au/publications/rcommunity/chap4.html

3 ADDRESSING PRIVACY CONCERNS IN A UBIQUITOUS NETWORK SOCIETY

The following section considers the privacy paradox from the point of view of those in the research and development community, and divides the current field into a number of distinct areas for consideration. These involve a range of problem formulations and design propositions, each taking up the privacy problem in a slightly different manner depending in part on the domain that is most emphasized (e.g., technical versus regulatory or sociological).

3.1 The consent problem

The consent problem is apparent in a recent survey that examined public views on privacy and 'popular ubiquitous technology' that includes the London Underground Oyster Card, the London Congestion Charging System, and mobile phones.[45] The paper offers seven 'privacy recommendations' that echo four assertions shared among similar studies: ensure full disclosure and transparency in design of the systems as it relates to collection, use and disclosure of customer information; simplicity of interaction for user access to

and control over personal data; seek active consent from users (to address user apathy); employ mutable privacy conditions depending on context of use.

On the one hand these assertions correspond closely to the control and feedback principles espoused by Belloti and Sellen and, for the most part, are already expressed in existing legal instruments. On the other hand, however, they represent a starting point from which to ask important follow-up questions that begin to deepen our appreciation of the consent problem as it relates to ubiquitous network systems. For instance, the seven recommendations overlook the fact that personal information is not simply that which has been explicitly collected from an individual but may also include transaction-generated information (TGI) that may not be apparent or known to the user. Moreover, asking a user to approve or consent to every tiny ping for data makes the ubiquitous network vision unwieldy, hence the need for mutable privacy conditions depending on context of use. Yet, how are boundaries established to distinguish context of use, who determines such boundaries, and on what grounds might we designate a third party or software agent to give consent to release personal details on our behalf? Under what circumstances might we want to supersede our agent and how will it/we know when those kinds of situations have arisen?

3.2 The challenge of anonymity

Work done using the Active Bat at AT&T Lab in Cambridge, has considered the problem of anonymity in ubiquitous networks. For these researchers, the primary focus is on location privacy, defined as 'the ability to prevent other parties from learning one's current or past location.'[46] In effect, the research contributes a formulation of the data-matching problem, particularly in public or otherwise insecure environments where 'hostile observers' can collude and share information to build profiles on users.

The typical solution to such a problem is to develop a technique for assigning pseudonyms to users to create an opaque identifier and thereby protect the matching of location data with personal information. However, it also finds that even when pseudonyms are being employed to protect privacy it is still possible to track users movements and to match those interactions with other kinds of transaction-generated information to produce a unique profile. The experimental approach used in the study has two components: frequently changing pseudonyms and mix zones. A mix zone is a connected spatial region in which no user has registered with any specific application. Users enter and exit a mix zone from application zones, where they may be registered under a pseudonym to obtain service. To avoid tracking a single pseudonym from place to place and matching it with other data that may be generated in association with applications, the pseudonym is changed whilst in the mix zone, where some form of "anonymizing" proxy is used to carry out this operation. The idea of this solution is to prevent linking of old and new pseudonyms, thereby rendering them untraceable.

In this system, the border-crossing problem is turned to an advantage for the user by enhancing their anonymity as they move from one space to another. However, the limits of anonymity are reached depending on the size of the mix zone and the number of people in it at the time a user makes a visit. The fewer people present in a mix zone, the lower the anonymity factor. In response, users may refuse to provide location updates to an application until the mix zone they are in achieves a certain level of anonymity.

3.3 What your body might betray about you

Others in the R&D community have identified the problem of user awareness and the ability of ubiquitous systems to collect data from a wide range of sensors, both active and passive. One ethnographic study, for instance, looked at an 'eldercare facility' in the USA, which finds that users are most unaware (and likely to remain so) of the potential and actual uses of sensor data gathered in the residence.[47]

A report on the study begins with the premise that 'too little empirical research exists to inform designers about potential users.' Complicating this is that ubiquitous systems are intended to be invisible, making it more difficult for users to understand or even become aware of the impact such systems might have on their personal privacy. One typical example is the use of so-called load cells in the eldercare residence, installed on each leg of the residents' beds, 'primarily to track trends in weight gain or loss over time.' While these sensors may play an important role in tracking the health of the residents, they may also be used in conjunction with other kinds of collected data for either intended or unintended purposes. Sensors that report changes in mass of an object, for example, can be used to determine when residents get into or leave

their beds, and if sensitive enough they might detect the fitfulness of sleep, or indeed if more than one person is sleeping in the bed. Used in conjunction with other information, such as sensors to detect the use of doors, such load cells might inform unwanted observers of the presence or absence of a person in a room, thereby opening up an opportunity for theft or other intrusion.

Our bodies emanate a great deal of information that may be collected, unbeknownst to us, about our behaviours. In most cases, this data will need to be matched with other forms of information to produce useful profiles for intended services. In other cases, however, such data may be collected and used without our knowledge or for purposes that are clearly unintended.

3.4 Autonomous computing

Related to the passive capture of data in ubiquitous networks is the problem of establishing trust relationships using established procedures and techniques:

> 'User authentication and access control are cornerstones of traditional information security systems, and are aimed at ensuring that information is neither disclosed nor modified improperly. Given the long history of research in this space, these mechanisms are, obviously, the natural counterparts of what we require for pervasive systems. Thus the obvious first approach to our problems is to attempt to deploy traditional mechanisms in this new environment. Sadly, this approach is flawed.'[48]

The authors of this paper argue that empirical evidence points toward the difficulty of ensuring certainty in user identification and, moreover, to a fundamental shift in the foundations of computing systems characteristic of ubiquitous networks, where underlying elements and interactions are not relatively stable but, on the contrary, highly dynamic and radically scaleable:

> 'Emerging network technologies repeatedly stress and provide functionality that supports the mobility of components, dynamic and distributed program execution, heterogeneity of services and a massive increase in the numbers of components and their geographical distribution. Consequently, an unreasoning reliance on traditional security mechanisms simply because they are traditional is, at best, flawed and, at worst, life threateningly dangerous.'[49]

Establishing trust relationships is linked to privacy inasmuch as the creation and maintenance of such relationships will depend to some degree on willingness and ability to collect and disclose information between parties, be they individuals in a direct exchange or perhaps software agents acting on behalf of individuals. Where ubiquitous networks are characterized by an absence of centralization, 'network resources are forced to make trusting decisions locally, in light of the information that they themselves can gather.' [50]

This radically decentralized architecture of autonomous, or 'autonomic', computing systems that are proposed for ubiquitous networks have serious implications for privacy, although these implications are often presented as a penultimate slide problem, meaning that they appear as closing thoughts in much of the literature on system design.[51] Nonetheless, we can glimpse some of the implications by looking at how developers have put into question various aspects of ubiquity and invisibility by looking at the challenges of linking the physical world with information networks, and in particular the crucial necessity of enabling network nodes to operate autonomously. As one observer puts it, 'perhaps more than any other dimension, autonomy is most significant in moving us from embedding instruments to embedding computation in our physical world.'[52]

The need for such decentralized systems as the underpinning of ubiquitous networks, suggests that individual nodes in such networks will require the migration of user consent and authorization away from centralized databases and toward the peripheral elements:

> '... we cannot realize long-lived autonomous systems by simply streaming all the sensory data out of the nodes for processing by traditional computing elements. ... we must construct distributed systems whose outputs are at a higher semantic level—compact detection, identification, tracking, pattern matching, and so forth.' (p. 67)

Among other things this raises the problem of privacy as it relates to machine-to-machine communication (sometimes called 'telematics') in ubiquitous networks, where human intervention is largely relegated to

setting policy and implementing it through software systems. Table 3.1 summarizes some of the problems identified in such autonomous architectures and the foreseeable privacy issues that might arise.

Table 3.1: Autonomous Computing and Privacy

Design Factor	Problems Identified	Privacy Concerns
Immense scale of ubiquitous network architecture	Need to use a vast number of small devices, each with limited capacity but achieving reliability from a large quantity of partially redundant measurements and their correlations.	Boundary crossing and insecure gateways; data matching and profiling necessary to produce reliability from small, partial samples.
Limited access to nodes and some devices	Inaccessibility of some embedded devices requires that they perform autonomously, with limited human attendance. For example, increased miniaturization means that every tiny sensor and controller may need to have its own processing and communication capabilities.	Information sharing with unknown systems (e.g., ad hoc network or in a mobile context); and data retention (e.g., multi-task and memory requirements); location privacy with mobile systems.
Devices and networks exposed to extreme environmental dynamics	Sudden and relatively high-level flows of data must be accommodated, which means that components must be capable of rapid coordination and adoption, often involving some form of information sharing.	Data retention at decentralized points to avoid need for active consent; data matching permissions related to multi-modal sensors and consent (e.g., biometric data used to trigger a flow of another mode of personal data).

Source: LSE

3.5 Hard security problems

The problem of establishing trust and protecting privacy in ubiquitous networks has numerous dimensions, many of which are nicely summarized as a set of 'hard security problems'.[53] An interesting observation about these problems is that they reside within overlapping domains of technical, regulatory, and social factors. As such, they help to illustrate the complex nature of addressing privacy concerns while attempting to realize the ubiquitous network vision of invisibility and pervasiveness.

The first problem is a fundamental matter of establishing trust, with the question 'Who or what am I talking to?' This is a basic 'trust-bootstrapping problem,' in relation to the user having confidence that the other party or device with which they are interacting is indeed what it claims to be. For instance, a customer using a mobile client to conduct an e-commerce transaction will want to have some a priori assurance that the server is part of a bona fide service and will not be engaged in illegal skimming of credit card details. A more problematic situation might be one in which a malicious device masquerades as a seemingly innocuous device, say perhaps a remote printer, and under that guise gains access to a user's private account information stored on their mobile client. Perhaps ironically, this problem of establishing certainty as to the device identity on electronic networks, is intractable without 'an initial exchange of information via a trusted physical channel', which may require initial exchanges to take place beyond the boundaries of a ubiquitous network, perhaps requiring the physical presence of other people or devices or through some other embodied form of contact.

Related to the initial problem of establishing trust at the outset, is the other problem of trusting the integrity of a device once its identity has been determined. Such a problem may require the development of trust-negotiation protocols that can assess the reputation/trustworthiness of devices. Some form of security assurance, for instance, may be necessary to categorize devices based upon their various technical properties, in particular those combined elements in the lower layers (physical, network access and application). Early work in this area has been done by the Trusted Computing Group (TCG), setting out specifications that include: 'support for mandatory controls, trusted runtimes, hardware-based software integrity reporting,

secure storage, support for non-repudiation in transactions, tamper-resistance, domain-based isolation, network-immunity, self-healing mechanisms, theft-deterrence, and fail-secure capabilities» (see Box 3.1).[54]

Box 3.1: Security and Ubiquitous Network Systems

Privacy and trust are related to the security of network systems. If devices and networks cannot provide certain minimum levels of security assurance, then users will not have the confidence to use them. In response to the hard security problems of ubiquitous networks, industry stakeholders have formed the Trusted Computing Group to develop and promote security assurance solutions. Although many consumers may never become aware of these solutions, they will no doubt play a major role in establishing trust by promoting minimum standards of security assurance in the marketplace.

'The Trusted Computing Group (TCG) is a not-for-profit organization formed to develop, define, and promote open standards for hardware-enabled trusted computing and security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals, and devices. TCG specifications will enable more secure computing environments without compromising functional integrity, privacy, or individual rights. The primary goal is to help users protect their information assets (data, passwords, keys, etc.) from compromise due to external software attack and physical theft.'[55]

A growing concern addressed by TCG is the threat of software attacks that may lead to incidents of identity theft and industrial espionage. The threat is seen to be increasing due in part to three continuing developments:

- Increasing sophistication of hackers and hacking techniques, including automated attack tools
- An increase in the detection of vulnerabilities in complex computing environments
- The increasing mobility of users

The TCG, citing data from the Software Engineering Institute at Carnegie Mellon University, notes that reported vulnerabilities doubled each year between 2000 and 2002.[56] With the deployment of ubiquitous network systems, it is conceivable that these vulnerabilities will continue to increase in numbers and in terms of difficulty of detection. Each point of vulnerability in a ubiquitous network is a potential threat to privacy, but perhaps more importantly the perception of vulnerability promulgated in media reports and rumours could seriously erode the trust of consumers.

Source: TCG

3.6 Encryption and shared consent

An interesting proposal for the problem of intrusive devices, such as camera phones and other portable recording devices is to combine encryption with an algorithm that requires shared consent to enable access to collected images or other forms of information. A number of proposals have already been developed to address the growing problem of portable recording devices, including an idea called Safe Haven, which proposes to transmit a disabling signal to camera phones in a specified area as a means of preventing unauthorized recording of images. Candidate locations for such a system might be a change room at a public swimming pool or in cinemas or other entertainment venues.

Critics of this proposed solution suggest that it may have several drawbacks; namely, that it is a relatively crude system that ignores the possibility that certain occasions may arise where it is reasonable and perhaps necessary to permit portable recording devices in an area. Concerns about the use of mobile phone silencers (radio jamming devices that render mobile phones useless in a specific area) in public locations, for instance, have centred on the fact that in some instances, such as during an emergency, having access to a working mobile phone may be a matter of life and death. It may not be so far-fetched to suggest with portable recording devices, that privacy may in some cases be a matter of context and that there may be legitimate reasons for capturing images or sounds in otherwise prohibited areas.

Another critique levelled at the Safe Haven type solution is that 'in practice, the usefulness or sensitivity of a recording is sometimes only apparent long after it is created and may depend on who it allowed to replay it.»[57] As such, the privacy concern with portable recording devices may not be with the actual moment of data collection but rather with later moments of use and disclosure. One proposal to address the drawbacks of existing privacy protection methods would encrypt data as it was being recorded by a device. The resulting file would be effectively sealed against use or disclosure, even if it were removed from the original

device, until all parties to that recording provided consent for its de-encryption. This proposal errs on the side of privacy and is based on two underlying principles:

- Unanimous consent. All parties to the recording must consent to its use; otherwise it effectively remains encrypted and relatively useless.
- Confidentiality of policy. Any party's decision to grant or withhold consent is not revealed to any other party to the recording.[58]

The solution, while perhaps viable in theory, faces some formidable challenges in practice. For instance, it involves a sophisticated architecture that would require all devices present in the recording situation to be aware of each other and to have sufficient computing power to carry out compatible cryptographic operations. In effect it is established on the assumption that all devices present in a situation will have similar features and capabilities and, moreover, will be activated.

Assuming that devices are compatible and activated—however unlikely it might be in practice—there is another and more difficult problem with this kind of shared consent design proposition. Let's take a look at what the designers consider to be a simple scenario to see just how problematic this concept might be when introduced into a public location:

> 'Some cases are easy. For example, an audio recording of two people conversing obviously implicates the privacy interests of both participants. We [can] generalize this by assuming that whenever a recording is made, every person who is present at the time of recording has a privacy interest in it. We [can] include even people who, though present, are not directly recorded, such as participants in a group conversation who never speak. We do this on the conservative assumption that speech addressed to a person may implicate his privacy interest whether or not he speaks. … we believe that … giving each person present a veto over creating recordings, and over the subsequent release of such recording, is the best available course.»[59]

Whereas the intent of the unanimous consent approach is to ensure a democratic authorization when it comes to disclosing information, it appears to overlook the scenario of unintended disclosure of information to unknown parties. For example, in the above scenario it is easy to imagine that there could be someone who is neither part of a conversation nor part of a group but is nevertheless within the vicinity of a recording. As such, if this person has a mobile client that is activated with the appropriate application they may be included by default in a shared consent request (simply because they are in the vicinity of the recording). This person may have no interest in denying consent and so gives approval. If all parties approve, then the recording may be released to all including, unbeknownst to the intended parties, the unknown individual(s) that happened to be in the vicinity of the time it was made. In other words, unanimous consent in this instance might in fact result in unintended disclosures of personal information to third parties.

Nonetheless, the shared consent approach, using encryption to protect personal information is important to the extent that it recognizes the principle noted earlier in this paper that privacy is a collaborative undertaking among two or more parties and that design propositions should take this into account as a fundamental consideration if they are to be effective when dealing with the complex social and technical interactions enabled by ubiquitous networks.

3.7 The sticky policy paradigm

Problem formulations that emphasize the need to minimize undesirable boundary crossings as threats to information privacy may adopt a sticky policy paradigm based on a system of unified privacy tagging. Research efforts that draw on the previously described border crossing model of privacy, for instance, establish a concept of 'information space' to describe a means of creating virtual boundaries that interact with 'sticky' privacy tags assigned to a device or application.

The sticky policy is established on three operations that can be applied to objects interacting with an information space:

- The capability of being able to read and write (to and from) an object regarding its privacy status.
- The capability to promote and demote an object's status (e.g., its visibility to the network; the longevity of the privacy tag)

- The capability of aggregation of data through an object (e.g., access to multiple information sources, the level of information detail an object is permitted to collect, use and disclose).

Owners assign permissions to each operation for each object within an information space and boundaries may be identified by physical presence (e.g., location-aware devices); and/or social activity-based criteria (e.g., application being used).[60] For instance, a sensitive digital document might be tagged with a set of specification that allow it be uploaded and accessed by specific individuals while they are in a specific location, such as a meeting room. When the individual leaves that room, the document then becomes unreadable or is deleted from their laptop computer. Similarly, the document may be tagged to permit certain levels of detail depending on the individual in possession of it. Whereas as a corporate CEO might have full access to all financial details in a digital document, a clerk might be authorized to see only certain less sensitive sections of the same document.

In essence, the sticky policy paradigm means that a privacy policy is assigned to a device or other data object and then travels with it over time and space. Proposals for this system of 'unified privacy tagging' would be based on a form of metadata that would consist of at least three parameters:

- a 'space handle' specifying the information spaces to which an object belongs;
- a 'privacy policy' specifying permissions for different types of operations (see list above);
- a 'privacy property list' specifying an object's lifetime, accuracy, and confidence parameters.

The privacy tagging approach tends toward an administrator-centred design proposition as contrasted with other possibilities that place greater control with the individual user.

3.8 Privacy enhancing technologies (PETs)

The term 'privacy enhancing technologies' or PETs describes a range of technological solutions to privacy management for the individual user, that attempt to provide direct control over the revelation of personal information, such as cryptographic systems, "anonymizers", and cookie management software.[61] Despite their promising role in protecting personal privacy, PETs have not been widely accepted by individual consumers and are subject to at least four types of criticism coming primarily from the social domain: one, that PETs are often too complex for many users; two, that PETs are not well suited to the contextual shifts in identity management that take place when users move from one kind of interaction to another (e.g., from a familiar website to an unfamiliar website); three, that they place the burden of privacy protection on the individual in the face of commercial pressures to surrender personal information in exchange for products and services; and, four, that PETs reinforce the notion of privacy as an issue about individual rights rather than it being a wider community or social value.[62]

Findings from studies that have examined the problem of privacy management and new technologies suggest that the limitations of PETs will be exacerbated in a ubiquitous network society and that new or different models for control of personal information will need to be adopted. For instance, the authors of one report claim that 'effective solutions will not come solely from repairing the usability problems associated with existing technologies, because the very nature of those technologies—the ways in which they conceive of the problems of [privacy]—is a source of the trouble ... effective [privacy] will require that we examine the conceptual models on which our systems are built.' [63]

More specifically, in studying the everyday activities of PETs users, researchers have confirmed that privacy management is a highly contextualized activity, where 'it may be inherently implausible for typical users to specify, in advance of particular circumstances, what their security needs might be; [and that] those needs arise only as a result of specific encounters between people, information and activities.'[64] One of the problems with PETs today is the requirement for users to specify their privacy preferences in an abstract manner, away from the intuitive and situated context in which many of these kinds of decisions are often made.

Design considerations that stem from this finding are threefold: first, information sharing and information protection mechanisms are two sides of the same coin, as it were, and should be available in combination; second, privacy protection applications need to be highly visible as part of the routine work flow of the user, rather than being preset and then disappearing into the murky depths of the device's operating system; third,