Shaping Ubiquity for the Developing World

Paper presentation and Panel Discussion

At

International Telecommunications Union (ITU)
Workshop on Ubiquitous Network Societies
http://www.itu.int/osg/spu/ni/ubiquitous/
Geneva, Switzerland
On
6-8th April 2005

Author: Rakesh Kumar
Rakesh.kumar1@cognizant.com

And

Co-Author: Riti Chatterjee
Riti.Chatterjee@cognizant.com

Cognizant Technology Solutions
India

www.cognizant.com

Table of Contents

Abstract

Across the world today, ubiquitous technologies are becoming an increasing part of people's lives. The issues and challenges for the development of such technologies not only encompass a broad spectrum of research topics but also involve envisioning new multi-disciplinary applications and legislations that will change the way in which we live and work.

The paper addresses the issue of **privacy policies**, especially for developing countries, in context of RFID and similar ubiquitous technologies for wider applicability and adoption by consumers, Governments and industries.

1. Audience and Purpose of the paper

The audiences for the paper's recommendations, towards ubiquitous technologies, are: Government, public and private bodies (implementing and using ubiquitous technologies) and consumers (end users of ubiquitous technologies).

The paper's public policy recommendations, to the above-mentioned audience, are proposed with the aim of rapid usage and acceptance of ubiquitous technology in developing countries by developing widely acceptable framework/legislation to alleviate privacy concerns on use, exchange and control of personal and related information, collected through RFID and other ubiquitous technologies.

2. Ubiquitous Technology- What does it mean?

Ubiquitous technology (alternatively known as pervasive computing) is the trend towards increasingly ubiquitous, connected computing devices in the environment, a trend being brought about by a convergence of advanced electronic - and particularly, wireless - technologies and the Internet. Pervasive computing devices are not personal computers as we tend to think of them, but very tiny - even invisible - devices, either mobile or embedded in almost any type of object imaginable, including cars, tools, appliances, clothing and various consumer goods - all communicating through increasingly interconnected networks.

Ubiquitous technology is pervasive in nature and unobtrusively embedded in the environment, completely connected, intuitive, effortlessly portable, and constantly available. Among the emerging technologies expected to prevail in the pervasive computing environment of the future are wearable computers, smart homes and smart buildings. Among the myriad of tools expected to support these are: Automatic Identification Technology (AIT) (Appendix 1), Application-Specific

Integrated Circuitry (ASIC); speech recognition; gesture recognition; system on a chip (SoC); perceptive interfaces; smart matter; flexible transistors; reconfigurable processors; Field Programmable logic Gates (FPLG); and microelectromechanical systems (MEMS).

Leading technological organizations are exploring pervasive computing where they envision a future of ubiquitous computing devices as freely available and easily accessible as oxygen is today (Appendix 2).

3. Ubiquitous technology – Impact on Intelligent Society

The sociological impact of Ubiquitous technologies in form of computers may be analogous to two other technologies that have become ubiquitous. The first is writing, which is found everywhere from clothes labels to billboards. The second is electricity, which surges invisibly through the walls of every home, office, and car. Writing and electricity become so commonplace and indispensable that we forget their huge impact on everyday life. Similarly, for Computers and RFID, users would start taking for granted the advantages offered by both in our daily running lives.

Computer as a tool for ubiquitous technologies has undergone many changes in last fifty years; Mark Weiser and John Seely in an article "Coming Age of Calm Technology" have described role and relationship between computers and people from mainframe era to ubiquitous computing era. The authors' forecasts in ubiquitous era, there would be many to many relationships between computers and users.

The Major Trends in Computing	
Mainframe	Many people share a computer
Personal Computer	One computer, one person
Internet - Widespread Distributed Computing	. . . transition to . . .
Ubiquitous Computing	Many computers share each of us

Fig 1: The Major Trends in Computing

Source: Coming Age of Calm Technology, Mark Weiser and John Seely Brown. Xerox PARC

Advantages of Ubiquitous technology (UT)

An individual with Ubiquitous technology (UT) enabled device, in near term, can use it as an authenticating device or could use it to control all the devices in his/her home. Ubiquitous technology (UT) enables accurate and timely automatic capture of actionable logistics data with little reliance on human intervention.

Some of the major areas identified for **immediate benefit** of ubiquitous technologies (RFID, GPRS etc) are:

a. Asset Tracking
b. Goods Trace ability
c. Enhance and streamline business processes
d. Seamless Supply Chain Management
e. Efficient Remote Monitoring System
f. Retail
    i. Out of Stocks reduction
    ii. Automated replenishment

By using RFID in retail scenario, goods will be located along the entire process chain – from production all the way through to the shelf in the store. Managing orders can be optimized, losses reduced and out-of-stock situations avoided, assuring an even more consistent availability of goods for the customer.

Similarly, in future, it is predicted with the help of ubiquitous technology a user could be informed automatically about the status of the food in his/her refrigerator (smart appliances). The Smart home (Appendix 3) would maintain data on inventory levels as well as consumption. Periodically, the consumer would give permission to his/her home server to upload her new shopping list to the system.
Thus it's hypothesized, that a user, in near future would interact with reality in **real time, anywhere, anytime** in ubiquitous technologies environment.

4. Role of RFID in Ubiquitous technology environment

RFID is perceived as a backbone for ubiquitous technology environment, in which information and communication flows everywhere, for everyone, at all times. RFID is supported by other similar technologies such as wireless, ad hoc and sensor networks, which already play important roles in pervasive computing. Sensing devices, such as RFID connected through wireless communication can capture, process and disseminate useful information surrounding human beings.

According to Dan Russell, director of the User Sciences and Experience Group at IBM's Almaden Research Center, by 2010 computing will have become so naturalized within the environment that people will not even realize that they are using computers. Russell and other researchers expect that in the future *smart* devices (RFID) all around us will maintain current information about their locations, the contexts in which they are being used, and relevant data about the users. Privacy advocates claim, the ubiquitous nature of RFID makes it as a most potent tool for privacy intrusion.

Methodology for privacy intrusion

RFID tags can be attached without knowledge of consumer and this is major concern for privacy advocacy groups. According to them, consumer privacy is enhanced when consumers are aware of information practices and are given a choice over information provision and use. In contrast, consumer privacy is decreased when there is unwanted marketing contact or information gathering without consent

According to privacy advocates, marketers and retailers can develop detailed profiles of their customers, based on their own records of transactions with an individual as well as on that individual's transactions with other institutions with help of RFID and other ubiquitous technologies. Even when these databases contain only transactional data, such as name, address, and product or service used or inquired about, they serve as the **basic source for development** of detailed profiles by interconnecting each other, now very easily with help from ubiquitous RFID.

5. A brief discussion on Privacy

Privacy has been discussed in past in different format, and various historical changes have brought about a change in perspective of our privacy needs. Consequently, much of this discussion has been incorporated into various regulatory and legal frameworks around the world, each with various effects.

Over the course of time, the primary focus of privacy has shifted according to technological developments. With the increased use of the telephone system in the 1930s, **communication privacy** received much attention with the case of Olmstead vs. United States in 1928, which questioned the legality of wiretapping by the United States government. The privacy of the person, often called **bodily privacy**, was seriously violated only a few years later, when Nazi leadership decided to conduct compulsory sterilization, as well as gruesome medical experiments, on parts of the non-Aryan population. The increased use of governmental electronic data processing in the 1960s and 1970s finally created the issue of **information privacy**.

The first two aspects of privacy have by now been very well established in most legal frameworks around the world, often directly defined as constitutional rights, issues surrounding **information privacy** are still not resolved both in developed and developing countries.

Importance of Privacy

Privacy is important because it is:

a. A way of controlling the power which people or organizations gain through collecting and storing information about others,

b. A means of securing the trust which people expect in return for providing accurate information about themselves,
c. A necessary condition for living in a society which values freedom and diversity, and
d. The basis on which we form meaningful relations with other people by deciding how much of ourselves to reveal or conceal to any given person.

Information privacy being important, the approach towards it also has changed with advent of new forms of technology (RFID) and communication (cell phones, PDAs) that have overcome the physical boundaries that used to separate the domestic and public spheres. Greater recognition of the rights of customers and citizens has also altered some traditional views and treatment towards privacy.

6. RFID and Privacy

RFID is used in many retail stores that sell small expensive goods such as CDs, videos, and DVDs to deter shoplifting. However, the tag functions are disabled or the tags are removed from the goods when the goods are purchased.

If the tags are affixed to all products and their functions continue to work outside the store, then a person with a compatible RFID reader can obtain information about those products and purchasers of these products.

By monitoring tagged products, the privacy advocacy groups, such as CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering) and FoeBuD, cautions that the Government and other unauthorized third parties (marketing agencies, Insurance Companies etc.) could possibly track individuals more easily and these corporations could intrude individual's private lives.

As a result, according to privacy advocates, the potential for widespread dissemination, misuse, unauthorized access, and disclosure of personal information about consumers would increase exponentially and create a new source of privacy intrusions in daily lives.
Such 'Orwellian scenario' hypothesized by privacy advocates have sparked reactions, from one extreme- strict Government regulations, to other extreme of boycotting the organizations (Benetton, Gillette) dealing in RFID.

Feasibility of not using RFID

One of the suggestions by privacy advocacy groups is to boycott the retailers/manufacturers using RFID to tag individual products. This is because, consumer groups fear that unique identifying data in an RFID tag could be used to track and profile individuals.

For the consumers, boycotting might not only be infeasible and cost-ineffective, but also inconvenient to live with. For e.g. live RFID tags post POS (Point of Sale)

would offer a consumer benefits in terms of efficient Warranty Claims Management, effective disposal (non- biodegradable and radioactive medicines etc.) and integration with 'Smart Appliances' in future.

7. Learning's for developing countries in context of RFID privacy

With Integration of the world's culture, economy, and infrastructure driven by the lowering of political barriers to transnational trade and investment, and by the rapid proliferation of communication and information technologies, developing countries are fast learning both best practices and mistakes of retailing giants in developed countries.

Though, organized retailing in developing countries constitutes two to twenty percent of total retailing, there is a greater impetus for growth in organized retailing by both Government and private sector.

According to Indian minister of commerce and industry, Kamal Nath, the benefits of a larger organized retail sector are many: the consumer gets a better product at a cheaper price, there is expanded reach and increased volume which means more manufacturing, more jobs, more prosperity, but best of all, it helps the farmer get better prices for his products by providing forward linkages for mass-marketing of processed and packaged goods.

a. State of Retailing in developing Countries

For countries like India, Brazil and China, usage of RFID in retail stores is minimal; nonetheless these countries are gearing up to meet Wal-Mart and other retailer's mandates.

China

Today Wal-Mart is the single largest corporation to buy Chinese products (if Wal-Mart were a nation, it would be China's eighth-largest export destination).

Also, Recently in news, Wal-Mart announced that SE Asian Global Procurement operations to be headquartered at Shanghai. The news has following ramifications:

i. Wal-Mart is not only looking China as manufacturing base but also a huge market in coming near future. This would entail framing policy on RFID data collection, usage and control that would be acceptable to socio-cultural needs of that country (China).
ii. Wal-Mart has to comply not only with US standards but also with Chinese Government's RFID standards (Frequency spectrum, power of readers etc.). This requires resolving inter-operatibility issues over frequency allocation over RF usage across different trading countries.

India

Similarly, Metro has opened first cash & carry outlet stores in India at Bangalore, The 6,500 square meter store in Bangalore offers a range of 17,500 articles to local customers, with around 90 per cent of these coming from local producers and suppliers. Some 10,500 of the goods on offer are non-food. Many more retailers are predicted to follow footsteps and open their base out of India and other developing countries. The chart from Deloitte (Retail Industry- Top ten issues 2004-2005) below shows decrease in number of retailers operating only in one country.

Retailers Today: Multi-Country, Multi-Format		
200 Largest Retailers	1997	2002
Countries of operation, avg.	3.7	5.3
Retail formats, avg.	1.9	2.6
Retailers that operate in only 1 country	103	84
Retailers with sales >$25 billion	13	23
Source: "Global Powers of Retailing," 2004 and 1999, Deloitte		

Source: Deloitte

All these developments, predict an increase in organized retailing across developing countries.

Thus, with rapid advent of organized retail in developing countries, the issues such as privacy invasion and unwanted marketing solicitations, due to ubiquitous technologies such as RFID, prevalent in developed countries is bound to slowly creep in developing countries.

b. State of RFID adoption in developing countries

In developing countries, RFID and other ubiquitous technologies is still in a state of experimentation. The customers in these countries are now warming up to the idea of the RFID technology.

There are few success stories like the delegate tracking done at 'NASSCOM: 2005: *India Leadership Forum'* in Mumbai (Appendix 4) and Chitale Dairy Farms. The latter implementation has achieved an increase in the milk yield up to 20% by using RFID technology to manage their livestock (Appendix 5).

Despite of these success stories, like all new technologies, which require a good hard look at their implications, RFID also requires a pre-emptive scrutinization on its usage and other related issues. The laws and regulations (mandatory) are still to be framed for 'RFID privacy' related issues.

Despite industry self-regulation efforts, according to privacy advocates, commercial firms both in developed and developing countries, collecting personal and related information are not following fair information practices (described in later part of the paper). It is argued further; that even firms worldwide who make a commitment to privacy may at times compromise privacy standards if it is competitively necessary, and thus legislations must be enforceable on these commercial firms.

c. Privacy Legislations across the world

One of the most influential early privacy legislation, in USA, was the US Privacy Act of 1974. In defining the principles, the appointed governmental advisory committee created the notion of fair information practices, a significant policy development that influenced privacy policies worldwide. The Privacy Act of 1974, controls and limits collection and disclosure of personal information by the US government, the Family Educational and Privacy Rights Act of 1974, enforces similar controls over educational institutions, and the Right to Financial Privacy Act of 1978, prevents financial institutions from providing federal authorities unfettered access to customer financial records (and requires such institutions to notify customers when their records are handed over to the authorities).

The principles of fair information practices, are based on the work by Columbia University political economist Alan Westin, are as follows:

a. Openness and transparency
b. Individual Participation
c. Collection limitation
d. Data Quality
e. Use Limitation
f. Reasonable Security
g. Accountability

In 1980, the Organization for Economic Co-operation and Development (OECD) codified the fair information practices in the OECD Guidelines in order to prevent a proliferation of varied privacy protection laws that might harm economic growth by creating accidental trade-barriers.

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

In 1995 an influential piece of legislation was passed in Europe. The European Union's Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, often called "The Directive" for short, is for privacy legislation of the ending 20th century what the Privacy Act of 1974 was for the early privacy laws.

8. Privacy Concerns in developing Countries vs. developed countries

The concern for privacy in developing countries compared to developed countries has undergone a sea change in last twenty years.
The first cases to recognize a right to privacy, in India, involved police surveillance. In Govind v. State of Madhya Pradesh,21 the court recognized such a right, and **cited American privacy cases from a variety of distinct areas**, including search and seizure, but also including the Fourteenth Amendment privacy right cases Griswold and Roe.22 .According to the Supreme Court of India in the case of R. Rajagopal v/s. State of Tamil Nadu reported in AIR 1995 SC 264, the right to privacy is implicit in the right to life and liberty guaranteed to the citizens of India by Article 21 of the Constitution.

According to Rohan Samarajiva, in UNESCO Courier, there is little, if any, evidence on the level of public concern about privacy in poor and developing countries. But it is a fact that the issue does not figure large in the policy agendas of these countries. For example in Sri Lanka, the civil war and its attendant problems of security, the cost of living and unemployment are likely to be listed as priority issues, not privacy. Even if the focus were to be narrowed to Internet and telecom, it is likely that access to voice telephones would be given more weight.

Attitudes toward telephone numbers can indicate the intensity of privacy concerns. In parts of the United States such as Nevada well over 50 per cent of residential telephone numbers are unpublished. Home telephone numbers are usually not printed on U.S. and European business cards. By contrast, it is a rare Sri Lankan or Indian business card that does not flaunt one.

Academic research suggests otherwise. Irwin Altman of the U.S. has shown that the essence of privacy--the ability, explicitly or implicitly, to negotiate boundary conditions of social relations--is transcultural. **What differs among cultures is the concrete form of privacy concern.** It is natural to see a heightened awareness of Internet privacy in the U.S. The same form will not be found in developing countries, where there are less than two telephones or Internet connections per one hundred people (Appendix 6).

According to one school of thought, the developing countries exhibit different approaches to privacy vis-à-vis United States, EU and other developed countries; a condition of limited access to identifiable information about individuals--from sociological, regulatory and managerial perspectives. This hypothesis is supported by two widely debated cases of privacy intrusions in India.

The first one being, DPS MMS scandal case in which Baazee.com CEO and Indian-born US citizen Avnish Bajaj was sent to jail for six days by a Delhi court. The focus of this case was not intrusion of privacy but illegal distribution of the clip on net. The Police claimed that Baazee.com listed the DPS MMS clip on its site for sale on November 24 and that the CEO did not make any effort to remove it until prodded (Appendix 7).

The second being a stealth video footage of an actor, by a media agency, invading privacy in the process. Legal experts believe that actor may find little recourse in the law apart from being able to file a defamation suit. While the US has expansive laws dealing with the invasion of privacy, India does not have any such legislation.

Concern over intrusion of privacy by the electronic media has hastened the setting up of a government-appointed regulator, but there is precious little an aggrieved individual can do about it currently in India.

Government policies and legislations for privacy in developing countries – A Comparative Study

Policy discourses in digitally deprived countries have emphasized external forces as drivers of privacy policies. The developing elements of the legal information-communications infrastructure for the developing countries, the most persuasive the claim that their privacy policies must meet U.S. and European Union standards for the sake of trading relationships.

Also, offshoring of services has increased rapidly in the recent years, leading to the export of critical data to offshore destinations. This has brought the issue of data security to the fore, with companies and individuals in the West raising concerns around the security of proprietary information and the confidentiality of personal data being off shored to developing countries like India and China. US and European organizations insist on legal agreement from BPO (Business Process Outsourcing) companies to protect sensitive data and information.

A recent evaluation of the information security environment (regulatory environment and security practices) in India vis-à-vis that in the US and the UK, compared Indian IT and ITeS (IT enables Services) companies with their counterparts in the US and the UK, with regard to the practices followed to ensure data security and confidentiality.

Security Environment: Country Comparison

Laws	India	China	Philippines	Ireland	US	EU
IPR						
Copyright	✓	✓	✓	✓	✓	✓
Patent	Product Patents - 2005	X	X	X	✓	X
DATA PROTECTION						
Data Protection Laws	Comprehensive framework - 2004	X	X	✓	✓ *	✓
Vertical Specific Laws	X	X	X	✓	✓	✓
CYBER						
Digital Signatures	✓	✓	✓	✓	✓	✓
Hacking	✓	✓	✓	✓	✓	✓
Privacy	✓	✓ **	✓	✓	✓	✓

Source: Evalueserve Analysis

* Though the US does not have comprehensive data protection laws, US companies with Safe Harbor certification are eligible to receive data from the EU.

** Though privacy laws exist in China, they are not comprehensive.

Source: Evalueserve Analysis at www.Nasscom.org

Given the disparate nature of economies and cultures in Asia and the Pacific islands it is unsurprising that there's wide range of legislation (or lack of legislation) and practice compared to Europe, US and other developed countries.

Debate about policy questions, community expectations, industry codes and legislation has primarily concerned data collection/handling by government agencies rather than the private sector. In particular it has centered on political surveillance and on questions of censorship, reflecting public attitudes about civil society and individual rights, past data collection practices in the private sectors of emerging economies (e.g. few comprehensive databases about consumption) and the priorities of national governments.

At a regional level there have been a number of statements by bodies such as APEC (Asia-Pacific Economic Cooperation), in particular the 1995 Seoul Declaration and 1998 Singapore Declaration. *[For detailed privacy laws and legislations in developing countries viz. China, Taiwan, Korea Malaysia and Thailand, please refer appendix 8.]*

The 1998 Singapore Declaration on privacy and E-commerce called for the APEC Telecommunications Working Group (APECTEL) to consider privacy as a key issue "that will affect consumer confidence and ability to use electronic commerce within the APEC region". The list for that consideration was to embrace:

a. Reviewing and contributing to international approaches for protecting the privacy of personal data
b. Identification of the essential elements of a legal and regulatory framework for electronic commerce

c. Encouraging all APEC member economies to remove existing and avoid the introduction of new legal, regulatory and other barriers to conducting electronic commerce in the region
d. Promoting the use of best practices on electronic commerce, i.e. the development of self-regulation measures by industry.

9. Existing Laws in Developing Countries

a. India - Information Technology Act 2000

India's first cyber law makes punishable cyber crimes like hacking, damage to computer source code, publishing of information which is obscene in the electronic form, breach of confidentiality and privacy, and publication of digital signature certificate ….

The Indian Parliament had passed the IT Act, 2000 on May 17, 2000 and this legislation received the assent of the President of India on 9th June 2000.

The IT Act aims to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information and to facilitate electronic filing of documents with the government agencies.

The Information Technology (Certifying Authorities) Rules, 2000 detail various aspects and issues concerning to Certification Authorities for digital signatures. These rules specify the manner in which information has to be authenticated by means of digital signatures, the creation and verification of digital signatures, licensing of certification authorities and the terms of the proposed licenses to issue digital signatures. The said rules also stipulate security guidelines for certification authorities and maintenance of mandatory databases by the said certification authorities and the generation, issue, term and revocation of digital signature certificates.

The overall net effect of all these notifications is that the information in the electronic format has been granted legal validity and sanction; digital signatures have been defined and made legal. It is now possible to retain information in an electronic format. Electronic contract has been recognized to be legal and binding.

Some types of cyber crimes have been defined and made punishable offences like hacking, damage to computer source code, publishing of information which is obscene in the electronic form, breach of confidentiality and privacy and publishing digital signature certificate false in certain particulars and for fraudulent purpose.

In Section 72, of the act, the clause for penalty for breach of confidentiality and Privacy is given as follows:

b. Penalty for breach of confidentiality and privacy (Section 72)

Any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record book register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh (0.1 Million) Indian Rupees , or with both.

c. Communications Convergence Bill 2000

The bill has addressed the issue of interception of communications. The principles laid down by the Supreme Court in the Telephone Tapping Case of People's Union of Civil Liberties v/s Union of India reported in AIR 1997 SC 568 find an echo in the Convergence Bill. The Bill lays down a detailed procedure to be followed by agencies desirous of intercepting messages or communication. The interception of communications is to safeguard against misuse in the interests of sovereignty and integrity of India, the Security of the State, friendly relation with foreign States or public order or for preventing incitement to the commission of an offence.

10. Framework for developing legislations (developing countries)

Governments in developing countries, after involving all the parties in RFID implementation and usage viz. manufacturers, 3PL, retailers and consumers, must rollout comprehensive legislations that ensure privacy safeguards such as notice, choice and data access by consumers. Framing of comprehensive regulations/legislation, as currently being done in EU, would impact, private sector and Government's RFID deployment, favorably the objective of bringing balance between commercial gains vs. alleviating privacy concern over usage of RFID.

Following are the suggested legislations, to be framed by Government bodies, for developing countries:

a. Regulating entities such as businesses and individuals

Developing countries like India and China can take direction from two pieces of important legislations in USA, viz. **The Gramm-Leach-Bliley Act;** also referred to as the **Financial Modernization Act of 1999**, and the **Health Insurance Portability and Accountability Act (HIPAA)** of 1996.

These laws tend to focus on:

i. Regulating electronic collection (especially via the Internet) and warehousing of personal information and
ii. Sharing or unauthorized distribution of personal information with other entities and individuals, particularly among business partners and affiliates.

The proposed regulations/legislations must also satisfy various principles falling into the following categories:

a. Transparency and Access
b. Consumer Consent and Choice
c. Appropriate Use
d. Safeguarding Information
e. Redress
f. Notify the affected parties

Following is the brief summary of each category:

i. Transparency and Access

No system that gathers personal information through RFID should ever in and of itself be kept a secret. Individuals have a right to know why personal information is being collected, and information should be used only for the originally intended purpose. Individuals must have access to the information being collected, through RFID, about them and they must be told how that information is to be used. As much as possible, personal information should be gathered directly from the explicit individual's informed consent.

ii. Consumer Consent and Choice

Individuals must be given a way of preventing information gathered for one purpose from being used for some other purpose without prior consent. People must be able to correct, amend, or add to the information gathered about them. Individuals should have the opportunity and method for "opting out" of programs using their personal information for commercial reasons.

i. Appropriate Use

An information-gathering system, such as RFID, must have socially desirable purpose and only data relevant to that purpose should be collected. Those entities that gather personally identifiable information must make sure that the data are used as intended and must take steps to prevent misuse.

ii. Safeguard the Information

Those entities that collect information should act as trustees. They do not "own" private information. They must safeguard the information they collect, and they must use it in the best interests of the individual. Whenever data systems are designed, privacy protections should be included in the specification and implementation of the system. The definitions and standards for privacy may change as new technologies, social concerns, and markets emerge. Personal information may be

transferred between parties only when the privacy protections of the recipient trustee are at least equal to the protections provided by the original trustee.

iii. Redress

Individuals whose privacy has been violated have the right to seek relief of some kind. Privacy violations can be resolved by negotiation, complaint resolution, or civil and criminal procedures.

iv. Notify the affected parties

The suggested legislation requires that the organizations storing sensitive personal information -- including government agencies, businesses, and persons engaged in business activities -- to notify the affected parties (customers, clients etc.) when that information data has been, or may have been, accessed without authorization. The purpose of the new law is to give affected parties adequate time to take steps to check their credit ratings and protect against identity theft.

11. Conclusion

Currently, the focus of introducing RFID and ubiquitous technologies is on increasing the efficiency for retailers or manufacturers in both developing and developed countries. The main obstacle for wider adoption of ubiquitous technologies is expected to be the issue of the invasion of customers' privacy and inter-operable RF standards.

The Governments in developing countries must realize that there can never be either purely technological or legislative solution to privacy, and that social-economic issues unique to their countries must be considered in their own right before developing a comprehensive framework for alleviating concern on privacy arising due to usage of ubiquitous technologies.

For Governments in both developing and developed countries there is clearly a need to balance the security concerns as against invasion of individual privacy. Experience of various privacy policies and regulations show that a self-regulatory approach by and large needs to be followed although in areas such as consumer financial and personal and information privacy, there is need for special legislation.

Effective legislations and policies need public support. Privacy advocates within and outside government must rethink their missions as including a strong component of public education. There is a need to translate abstract privacy concerns into concrete definition of scope and limitations of the information-handling and dissemination

practices to be followed by the organizations adopting and using ubiquitous technologies. This is the key to bridging the privacy divide in developing world.

For Organizations operating in developed countries and branches in developing countries and vice-versa, earning customer's trust and confidence through better privacy practices on RFID and other ubiquitous technologies is a necessary prerequisite to achieve a long-term and profitable customer relationship. Given rising high consumer expectations, investing in good privacy and data protection practices could be the sustainable strategy for survival and value creation for the organizations dealing with ubiquitous technologies.

Appendix 1:

Automatic Identification Technology (AIT) is a suite of enabling tools and devices that are used to automate the capture, recording, reporting, aggregation, or collection of data directly at the source of the data and feed it into an automation information system (AIS). The suite of tools consists of such media as linear and 2 dimensional barcodes, contact memory buttons (CMB), common access cards (CAC), biometrics, optical memory cards (OMC), satellite tags and tracking systems, and passive and active Radio Frequency Identification (RFID) tags and readers.
Source: United States Marine Corps

Appendix 2:

Xerox's Palo Alto Research Center (PARC), has been working on pervasive computing applications since the 1980s. Although new technologies are emerging, the most crucial objective is not, necessarily, to develop new technologies. IBM's project Planet Blue, for example, is largely focused on finding ways to integrate existing technologies with a wireless infrastructure. Carnegie Mellon University's Human Computer Interaction Institute (HCII) is working on similar research in their *Project Aura*, whose stated goal is "to provide each user with an invisible halo of computing and information services that persists regardless of location." The Massachusetts Institute of Technology (MIT) has a project called *Oxygen*. MIT named their project after that substance because they envision a future of ubiquitous computing devices as freely available and easily accessible as oxygen is today.

Appendix 3

In human-centered, ubiquitous technologies, speech and vision technologies will let humans communicate naturally with computers, just as they would with other people. Decentralized networks and robust software/hardware architectures would adapt to mobile users, currently available resources, or varying operating conditions.
A person living in this future will be able to tell the computer -- tell it, not type instructions -- to book a flight to London on a certain date, and the computer will take care of it, knowing already about preferences in seat assignments and meal choices, and working within personal preferences as to the price, number of stopovers and landing times.
While people on the move and outdoors would still use cell phones and PDAs to interact with increasingly intelligent and adaptable technology, The scientists envisions fully integrated smart environments in which the user requires no device in hand to interact.
Source: Sci-Tech Today, available at:
http://www.sci techtoday.com/perl/story/18363.html

Appendix 4

NASSCOM's requirement was to track delegate participation and identify attendance trends at the annual conference. RFID technology was selected to track delegate participation in real time at different sessions over three days of the conference. Cognizant Technology Solutions, an IT solution provider based out of India, was responsible for developing and deploying an appropriate RFID solution at the conference for this purpose.
The details for each conference hall were visible on the display screen and were refreshed at regular intervals. For each conference hall the details like name of the hall, the session name, attendance at different times and the last refresh time were displayed.

The Reporting Module consisted of:

- Hall wise attendance summary
- Attendee Details for individual conference halls
- Delegates registered and attended
- Delegates registered and not attended

Delegate Tracking at NASSCOM 2005: India Leadership Forum in Mumbai, India
Photo Courtsey: Cognizant Technology Solutions

Appendix 5

The Rs 1500 million (41 miilion Swiss Francs) Chitale Dairy Farm, located at Bhilawadi, around 240 km from Pune, handles about 60 million litres of milk per annum.

The enterprise has achieved considerable success with the use of RFID tags. Each buffalo is tagged with a card that takes care of the feeding data (a buffalo can eat only a certain programmed portion of daily ration at one time), breeding data (contains information on the genetic stock of the animal and all aspects related to animal rearing, pregnancies, vaccinations, diseases) as well as milking record (indicates if the buffalo is not milked or if the milk is not directed to the tank or if the buffalo has not produced as much milk as expected).

- The orange tag is a simple numbering of the buffalo for keeping track of the number of buffaloes. Plus the number is electronically associated with the electronic ID, which is stored in the computer.
- The blue tag is the metallic cover under which the smart card has been locked for safety purposes. Since buffaloes cannot be expected to maintain any kind of discipline, the blue metallic cover ensures that there is no damage to the card inside.
- At the time of allocating the electronic ID, a link is created with the physical ID.
- The card stores a host of information on the buffalo mainly on three counts—

Feeding: The farm has a unique feeding system that feeds the buffaloes correctly. The buffalo can never eat more than a certain programmed portion of daily ration at one time. The total ration is fed over 24 hours in small amounts from half a kg to two kg.

Milking: Every time the buffalo enters the parlor, the transponders in the strap (blue tag) is identified. On the milking point controller (MPC), a warning lamp lights up at the appointed symbol if the buffalo is not milked or if the milk is not directed to the tank. If the buffalo has not produced as much as expected, the warning lights will glow.

Breeding: This contains information on the genetic stock of the animal and all aspects related to animal rearing related to pregnancies, vaccinations, any diseases. This has resulted in 15 to 20% improvement in total milk yield. The national average of buffalo milk yield in the country is 800-1000 litres in 300 days. At the Chitale dairy farm, they are able to achieve 2500 litres in 300 days.

Source: Dataquest India

Appendix 6:

A close examination of the law in question — Information Technology Act 2000 — shows that the police did not do anything out of the ordinary in arresting Bajaj. On the face of it, the case falls squarely under Section 67 of the IT Act which imposes a stiff penalty of imprisonment up to five years on anybody who transmits any pornographic material in electronic form. Though there is already a general provision against pornography in the Indian Penal Code, the IT Act contains this special provision as a part of the legal framework created by it for the emerging e-commerce. It was a signal to all Internet operators that they would have to take special care to ensure that their sites do not peddle pornography.

At the same time, the lawmakers made allowance for the fact that not all operators can exercise the same degree of control over their sites. The IT Act recognises the reality that the extent to which an operator can exercise control depends on the nature of his site. Somebody who is purely a service provider, such as Baazee.com, would have little control over what is sold. Given this inherent constraint, Baazee.com does little beyond making the sellers undertake that they would not use the site for peddling any illegal stuff, including smut. A content provider, on the other hand, would be able to take greater responsibility as it is feasible for him to vet any article before it is put on the website. A news portal is a common example of a content provider.

So, making a clear distinction between the two kinds of providers, the IT Act exempts service providers from liability for "any third party information or data" in certain cases. Section 79 stipulates that no service provider shall be liable if he "proves" either of these conditions: that the offence was committed without his knowledge or that it happened even after he had exercised all due diligence. To be sure, any service provider booked under the Act will try to take refuge in either or both these conditions. But he can get off the hook only if he succeeds in proving his claim. And, in the normal course, he will get his turn to prove his innocence only in the course of the trial.

The implication of all this is that the police were very much authorised to arrest Bajaj as the head of the service provider that offered to sell copies of the CD containing the offending MMS. At the current stage of investigation, they are entitled to disbelieve Bajaj's protestations of innocence. When he sought bail before the Delhi High Court, the police made much of the 38-hour delay on the part of Baazee.com in removing the CD from the site even after it had been informed that the CD displayed child pornography.

In the event, the High Court granted bail to Bajaj holding that the evidence "indicates only that the obscene material may have been unwittingly offered for sale on the website." This prima facie observation or oblique reference to Section 79 does not, however, mean that the High Court has pre-judged the case in favour of Bajaj. It only means that, given the nature of the case, the High Court is convinced that there was no need to detain Bajaj beyond the four days he had already spent in custody. He has been released subject to the condition that he would continue to

cooperate with the investigation and not leave the country without the trial court's permission.

At the end of their investigation, the police may come round to the view that Baazee.com's role was entirely innocent and decide not to press any charges against Bajaj or any of its employees. If the police decides otherwise, the courts may, depending on the evidence adduced against him, discharge him before the trial or acquit him at the end of it. In none of those scenarios, nothing can really compensate Bajaj for the detention already inflicted on him. And whatever the ultimate outcome of the case, it will not detract from the legality of his recent detention.

His arrest was also based on the general principle, embodied in Section 85 of the IT Act, that when an offence is committed by a company, the persons in charge of it are liable to be proceeded against. There may well be scope to make the Act kinder than it already is to service providers as opposed to content providers. But any objection to the very arrest of Bajaj amounts to undermining the rule of law, which includes the principle of equality.

Source: The Indian Express, December 23, 2004 ; An article by Manoj Mitta. Available online at: http://iecolumnists.expressindia.com/print.php?content_id=61351

Appendix 7:

a. Less than 5 percent of computers connected to the Internet are in developing countries.
b. Eighty-eight percent of all Internet users are in industrialized nations, yet those countries only have 15 percent of the world's population.
c. The United States has more computers than the rest of the world combined.
d. Internet users in Africa and West Asia together account for just 1 percent of people connected online.
e. While poor countries have about 1.4 lines telephones per 100 people, the industrialized world has nearly 50 telephone lines for every 100 people.
f. Tokyo has more telephone lines than all of Africa, while more than half of the world's population has yet to make a telephone call.
g. Eight of 10 Web sites are in English, a language understood by only one in 10 people on the planet.

Sources: CIA Worldfactbook; World Bank Country Report: India; Census of India 2001; United Nations World Employment Report 2001; United Nations Human Development Report; Population Resource Center; U.S. Internet Council; India Ministry of Commerce and Industry; Marshall School of Business at University of Southern California; International Telecommunications Union; BBC Online

Appendix 8:

China and the Hong Kong SAR

The Chinese Constitution - like that of the former USSR - provides limited rights to privacy, notably the declaration that "the freedom of the person of citizens of the People's Republic of China is inviolable" (Article 37) and that

> *Freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law. No organization or individual may, on any ground, infringe on citizens' freedom of privacy of correspondence, except in cases where to meet the needs of state security or of criminal investigation, public security or prosecutorial organs are permitted to censor correspondence in accordance with procedures prescribed by law (Article 40)*

Government agencies have taken a broad view of "the needs of state security" and investigation. There's no general data protection legislation, few enactments that limit interference by government agencies and problematical application of legislation or statements of principle.

Hong Kong was the first part of the region to enact legislation based on the EU Directive, with a Personal Data (Privacy) Ordinance covering the public and public sectors and a Code on Access to Information.

The statutory Privacy Commissioner (PCO) is currently engaged in work of particular importance regarding privacy aspects of identity cards and health databases.

Taiwan

Across the straits the 1994 Taiwanese Constitution articulates a restricted right of privacy, i.e. that "The people shall have freedom of privacy of correspondence".

That has been extended through legislation such as the 1995 *Computer-Processed Personal Data Protection Law* concerning the collection and use by government agencies and some private sector bodies of personally identifiable information. The 1995 law requires that "collection or utilization of personal data shall respect the rights and interests of the principal and such personal data shall be handled in accordance with the principles of honesty and credibility so as not to exceed the scope of the specific purpose", with an in principle right of data access, correction and deletion. Data flows to countries without privacy legislation can be prohibited.

Malaysia

Malaysia's federal Constitution does not specifically recognize a right to privacy and there's been little progress in the development of a comprehensive regime for the protection of personal data collected/handled by the private and public sectors, despite proposals for a *Personal Data Protection Act* as part of the ambitious *National Electronic Commerce Master Plan.*

Statements by government spokespeople characterize privacy safeguards as a cost of

doing business rather than a public good and as an impediment to the proper policing of society. In practice provisions in the *Communications & Multimedia Act* 1998 restricting telecommunications interception appear to be ignored or overridden by the Internal Security Act and the Computer Crime Act of 1997.

Thailand

Thailand's 1997 Constitution seeks to protect a "person's family rights, dignity, reputation or the right of privacy", indicating that "the assertion or circulation of a statement or picture in any manner whatsoever to the public, which violates or affects a person's family rights, dignity, reputation or the right of privacy, shall not be made except for the case which is beneficial to the public" and that "Persons have the freedom to communication with one another by lawful means".

Legislation and administrative directions under the Constitution have primarily concerned data handled by government agencies, rather than the private sector, for example the 1997 *Official Information Act* establishing a code of practice for personal information systems maintained by agencies.

13. References:

1. Tang, Beth Archibald. Pervasive Computing (2004, July 12). [Online]. Available: http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci759337,00.html (January 24, 2005).

2. Redriksson, Vendela. Smart Home or Building (2001, July 31). [Online]. Available:http://searchsmb.techtarget.com/sDefinition/0,,sid44_gci540859,00.html (January 27, 2005).

3. Mitta, Manoj. Baazee.com's run-in with the law (2004, December 23), *The Indian Express*. [Online]. Available: http://www.indianexpress.com/full_story.php?content_id=61351 (January 27, 2005)

4. Harper, Jim. (2004, June 21): " RFID Tags and Privacy: How Bar-Codes-On-Steroids Are Really a 98-Lb. Weakling", Competitive Enterprise Institute. [Online]. Available: http://www.cei.org/pdf/4080.pdf (January 27, 2005).

5. Stochniol, Dr Andre. (2001, Oct 31- 04 Nov): "How Technology moves Society: Today and in the future". [Online]. Available: http://icec.net/icec2001/down/keynote-speaker.pdf (January 24, 2005)

6. "Remote Monitoring System". [Online]. Available: http://www.iap-online.com/technologyupdates.php (January 17, 2005)

7. "What is privacy?" (31 May, 2004) Lawlink. [Online]. Available: http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_04_faqprivacy (January 26, 2005)

8. Lerner-Wright, Steven (December 3, 2003): "Creating a new privacy principle". [Online]. Available: http://www.securius.com/archive/407.txt

9. Campbell, Doug (Mar. 28, 2005): "RFID policy may not wait" , RFID Journal. [Online]. Available: http://www.rfidjournal.com/article/articleview/1461/1/128 (March 31, 2005)

10. http://www.findarticles.com/p/articles/mi_m1310/is_2001_March/ai_72299750

11. http://www.indianexpress.com/full_story.php?content_id=66709

12. http://www.electronicgov.net/pubs/research_papers/guest/Roadmap2eGov.pdf

13. http://www.pbs.org/frontlineworld/stories/india/didyouknow.html

14. http://timesofindia.indiatimes.com/articleshow/1052965.cms

15. http://architecture.mit.edu/house_n/web/resources/articles/homeautomation/Appliances%20to%20Be%20Linked%20to%20Internet.htm

16. http://www.caslon.com.au/privacyguide6.htm

17. http://www.outlookindia.com/full.asp?fodname=20050307&fname=Kamal+Nath+(F)&sid=1

18. http://www.dqchannelsindia.com/content/channeltech/104090201.asp

19. http://www.dqindia.com/content/top_stories/104033103.asp

20.

21. THE COMING AGE OF CALM TECHNOLOGY, *Mark Weiser and John Seely Brown Xerox PARC*
http://www.ubiq.com/hypertext/weiser/acmfuture2endnote.htm
22. **www.ubiq.com/hypertext/ weiser/UbiHome.html**
23. http://canada.justice.gc.ca/en/news/nr/1998/attback2.html

1. Gilster, Paul (2003, July 2003). RFID threatens privacy. [Online]. Available: http://newsobserver.com/business/story/2717267p-2519499c.html [October 27, 2003].

2. Awerdick, John H. (1996): "On-Line Privacy" The Internet and Business: A Lawyer's Guide to the Emerging Legal Issues, *Computer Law Association.* [Online]. Available: http://cla.org/RuhBook/chp4.htm [October 28, 2003].

3. Vance, Cathy (2002): "The Broad Reach of Privacy Regulations", Commercial Law Bulletin, Mar/Apr2002, Vol. 17 Issue 2, p16, 3p, 1bw

4. Milne, George R. and Culnan, Mary J. (Oct2002) : "Using the Content of Online Privacy Notices to Inform Public Policy: A Longitudinal Analysis of the 1998–2001 U.S. Web Surveys", Information Society Vol. 18 Issue 5, p345, 15p

5. Jones, Mary Gardiner (Spring 91) : "PRIVACY: A SIGNIFICANT MARKETING ISSUE FOR THE 1990S", Journal of Public Policy & Marketing, Vol. 10, Issue 1
6. Culnan, Mary J(Spring 2000) : "Protecting Privacy Online: Is Self-Regulation Working?", Journal of Public Policy & Marketing, Vol. 19 Issue 1, p20, 7p