INTERNATIONAL TELECOMMUNICATION UNION

ITU WORKSHOP ON
UBIQUITOUS NETWORK SOCIETIES

Document: UNS/04
April 2005

Original: English

ITU NEW INITIATIVES PROGRAMME — 6-8 APRIL 2005

UBIQUITOUS NETWORK SOCIETIES:

THE CASE OF RADIO FREQUENCY IDENTIFICATION

BACKGROUND PAPER

Acknowledgements

This paper was prepared by Lara Srivastava <lara.srivastava@itu.int>, Telecom Policy Analyst, International Telecommunication Union (ITU). 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 briefing papers can be found at http://www.itu.int/ubiquitous. The opinions expressed in this study are those of the author and do not necessarily reflect the views of the International Telecommunication Union or its membership.

TABLE OF CONTENTS

1 INTRODUCTION 3

2 THE TECHNOLOGY BEHIND RFID 4

2.1 ORIGINS OF RFID 4
2.2 HOW RFID WORKS 5
2.3 TYPES OF RFID 7
2.4 INTERNATIONAL RFID 7
2.4.1 RFID and the Radio Spectrum 7
2.4.2 Key international organizations for RFID development 9

3 RFID IN APPLICATION 12

3.1 NASCENT MARKETS 12
3.2 BUSINESS APPLICATIONS 13
3.2.1 Transport and logistics 13
3.2.2 Security and access control 14
3.2.3 Supply-chain management 14
3.2.4 Medical and pharmaceutical Applications 16
3.2.5 Manufacturing and processing 17
3.2.6 Agriculture 17
3.3 GOVERNMENT APPLICATIONS 18
3.3.1 E-government 19
3.3.2 Defence and security 19
3.3.3 Library systems 20
3.4 CONSUMER APPLICATIONS 20
3.4.1 Personal welfare and safety 20
3.4.2 Sports and Leisure 21
3.4.3 Shopping and dining out 22
3.4.4 Smarter homes, smarter people? 23

4 RFID IN THE LAB 24

4.1 RFID AND WIRELESS SENSOR TECHNOLOGY 24
4.2 RFID AND THE MOBILE PHONE 24
4.3 FROM SMART CHIPS TO SMART DUST 25

5 IMPLICATIONS OF RFID 27

5.1 PUBLIC POLICY CHALLENGES 27
5.1.1 Interoperability and standards-setting 27
5.1.2 Governance of resources 27
5.1.3 Data protection and consumer privacy 27
5.2 SOCIAL AND HUMAN IMPACTS 29
5.2.1 Society under surveillance? 30
5.2.2 Individuality, self-fulfilment and self-expression 31
5.2.3 Human relationships and intimacy 32
5.2.4 New technologies, new divides 32

6 CONCLUSION 33

List of Figures

Figure 2.1: The Look of RFID 5

Figure 2.2: Getting underneath RFID 6

Figure 2.3: ETSI’s New Frequency Allocation for European RFID 11

Figure 3.1: Worldwide RFID Sales 12

List of Boxes

Box 3.1: Radio that cab fare 14

Box 3.2: RFID – The student’s new hall monitor? 15

Box 3.3: RFID in the closet 15

Box 3.4: RFID to combat counterfeit drugs 16

Box 3.5: Sink your teeth into RFID 17

Box 3.6: RFID eases production of golf cars 18

Box 3.7: Tag that soap 18

Box 3.8: Tag farming 19

Box 3.9: Tagging the ancient 20

Box 3.10: LEGO of my RFID! 21

Box 3.11: High-speed RFID 22

Box 3.12: Racing forward with RFID 22

Box 3.13: McDonald’s and RFID: Lovin’ it 23

Box 3.14: Watch this RFID: an important step towards smart technological ubiquity 24

Box 4.1: RFID tags and Shopping in Tokyo’s trendy Roppongi Hills 25

Box 4.2: More than microscopic 26

Box 5.1: Implantable chips make for better bar hopping 30

List of Tables

Table 2.1: RFID Development 4

Table 2.2: RFID in the Ultra High Frequency (UHF) Bands 8

Table 2.3: ISO Standards 9

Table 2.4: ETSI Regulations for RFID: Then and Now 10

1 INTRODUCTION

It was over a decade ago that the late Mark Weiser outlined his vision of a world in which technologies "weave themselves into the fabric of everyday life until they are indistinguishable from it"[1]. Declaring that the most profound technologies are those that disappear, he heralded the dawn of the era of "ubiquitous computing".

There are examples of ubiquitous information and communication technologies (ICTs) on the market, the mobile phone being an early but important one. Technology today is becoming an afterthought in our daily activities, an integral part of them, rather than a tool that must be actively "used". Communication via email or short message service (SMS) is now taken for granted in many parts of the world. At the same time, the power of microprocessors has doubled about every eighteen months over the last three decades. The trend continues as devices with computing power become smaller, faster, and more pervasive, and communication tools more personalized and indispensable (e.g. the mobile phone or the personal digital assistant).

For information and communication access to be truly and seamlessly embedded in the environment surrounding us, however, the exponential growth of networked devices is required together with a paradigm shift in computing. This paradigm shift will mean that smart computers will become as common as the written word. Already, human beings are more often connected to a network than not, through personal computers and handheld devices, at work and at home.

But what if not only people, but also things were connected and contactable? Far from science fiction, the day is fast approaching when every consumer product (from cars to toothbrushes) will be tracked using tiny radio transmitters, or tagged with embedded hyperlinks. Such labels will ultimately transform the way that products are distributed, sold and purchased, and perhaps eventually how people are identified and how they communicate. That is the vision of technological ubiquity that technology developers, service providers, futurologists, and economists alike are positing on today. Building on "anytime and anywhere" information and communication technology, developers are now looking to enhance access in space and time, providing access for all persons and all things. Ubiquitous ICTs may thus promise ICTs "anytime, anywhere, for anyone and anything".

Delivering on this promise is currently limited by the ability to collect raw data about where things (or people) are located and about ongoing changes in their status. Radio-frequency identification (RFID) provides just such a capacity. RFID is at the core of the aptly-named "Internet of things" and is a key enabler of the ubiquitous network society. RFID refers to those technologies that use radio waves to automatically identify and track individual items. It may be seen to fall into the family of short-range wireless technologies, such as ZigBee and Bluetooth[2], but with a higher capacity for tracking and computing. The present paper examines this important development. It includes a discussion of the underlying technology, its current applications, human implications, and future directions. It is one of three thematic papers presented at the New Initiatives Workshop on "Ubiquitous Network Societies" from 6-8 April 2005[3] hosted by the International Telecommunication Union in Geneva, Switzerland. Papers on "The impact of ubiquitous networks and computing on the traditional telecommunication industry" and "Privacy and ubiquitous network societies" were also commissioned. Country-specific case studies on Italy, Singapore, Japan, and Korea were also prepared for the Workshop. All documents are available for downloading at http://www.itu.int/ubiquitous.

2 THE TECHNOLOGY BEHIND RFID

This chapter provides a technical overview of radio frequency identification (RFID), including a discussion of standards behind the technology.

2.1 Origins of RFID

Radio frequency identification is not based upon a new idea. One can trace the origins of radio back to the discovery of electromagnetic energy, and its early understanding by Michael Faraday in the 1840s.[4] During the same century, James Clerk Maxwell formulated a theory for the propagation of electromagnetic radiation. In the early 20th century, human beings were first able to use radio waves. Soon thereafter, the 1920s saw the birth of radar. This technology detects and locates objects (position and speed) through the reflection of radio waves.

RFID is the combination of radio technology and radar. An early application of RFID emerged during World War II: the “identification of friend or foe” (IFF) programme saw the first generation of identification tags into military aircraft. But perhaps one of the first studies exploring RFID is the landmark work by Harry Stockman entitled “ Communication by Means of Reflected Power”[5] in 1948.

Following the development of radio and radar, RFID techniques were explored further in the 1950s. In the late 1960s, radio frequency began to be used for the identification and monitoring of nuclear and other hazardous materials.

Work on RFID began to blossom in the 1970s and 80s when developers, inventors, companies, universities, and governments actively developed RFID applications in their laboratories. The technology underwent enhancements aimed at reducing cost and size, as well as power requirements and communication range. This set the stage for mass market RFID. In the 1999s, millions of RFID tags made their way into applications including toll roads, entry access cards and container tracking. The first mass-market deployment of RFID was in electronic toll collection (e.g. Oklahoma, United States, 1991). Since then, technical standards have emerged, together with new applications (such as RFID in athletics), and the technology is slowly becoming part of everyday life. RFID is being used as a generic term that can be used to designate the identification at a distance by radio frequencies. It has the key advantage of suffering very little from obstruction or interference[6]. Table 2.1 sets out some of the key events in RFID development.

Table 2.1: RFID development
RFID through the decades

Time period	Event
1940-1950	Radar defined and used. Major World War II development efforts. RFID invented in about 1948.
1950-1960	Early explorations of RFID technology. Laboratory experiments.
1960-1970	Development of the theory of RFID. Early field trials.
197-1980	Explosion of RFID development. Tests of RFID accelerate. Early adopter implementation of RFID.
1980-1990	Commercial RFID applications enter the mainstream
1990-2000	Emergence of standards RFID more widely deployed.
2000-2010	Innovative applications emerge. Combination of RFID with personal mobile services. Subcutaneous RFID emerges for animals, humans. RFID becomes part of daily life.

Source: Adapted from *Shrouds of Time: History of RFID,* AIM Publications, 2001

2.2 How RFID works

Simply put, RFID technology may be seen as a means of identifying a person or object using electromagnetic radiation. Frequencies currently used are typically 125 kHz (low frequency), 13.56 MHz (high frequency), or 800-960 MHz (ultra high frequency). RFID enables the automated collection of product, time, place, and transaction information.

An RFID system consist of two main components:

1. A transponder to carry data (e.g. a tag), which is located on the object to be identified. This normally consists of a coupling element (such as a coil, or microwave antenna) and an electronic microchip;
2. An interrogator (or reader) to read the transmitted data (e.g. on a device that is handheld or embedded in a wall). Regardless of whether this interrogator is a read only or read/write device, it is always referred to as a "reader".

Many readers are fitted with an additional interface (i.e. middleware[7]) to enable them to forward the data received to another system, such as a personal computer or robot control system[8]. Most tags are no bigger than a grain of sand (i.e. less than 1/3 mm wide), and are typically encapsulated inside a glass or plastic module (Figure 2.1). Compared with tags, readers are larger, more expensive and power-hungry. In the most common type of system, the reader transmits a low-power radio signal to power the tag (which, like the reader, has its own antenna). The tag then selectively reflects energy/data back to the reader (which now acts are a receiver), communicating its identity and any other relevant information (Figure 2.2). Most tags are only activated when they are within the interrogation zone of the interrogator. When outside that zone, they are dormant. Information on the tag can be received and read by readers. These latter can be attached to a computer containing the relevant database. This database can in turn be connected to a company's Intranet, and/or the global Internet.

Figure 2.1: The Look of RFID
An RFID tag in the palm of your hand

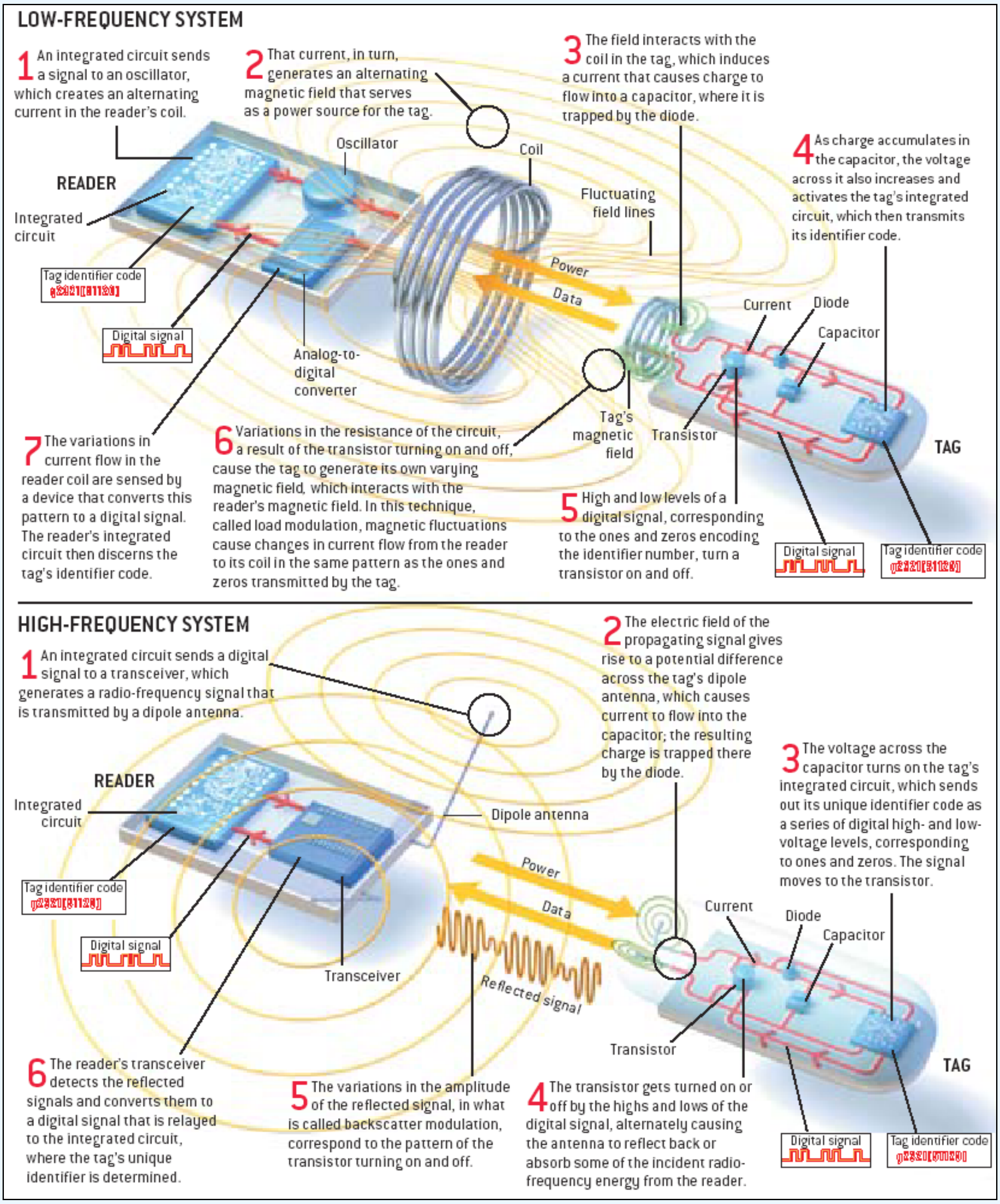
Source: ITU

Much of the recent media attention surrounding RFID use refers to the use of smart tags in consumer sales, i.e. automatic identification and data capture. This type of RFID tag has been considered by many to be the next generation of the Universal Product Code (UPC) or the traditional bar code.

RFID and the traditional bar code have some very important and fundamental differences. Firstly, traditional bar codes identify only a category of products. For instance, all Gillette Mach 3 razor blades have the same bar code. However, with RFID tags, each packet of these blades would have its own unique identifier that can be transmitted to suitably located readers for monitoring. At the moment, the Electronic Product Code (EPC) is the dominant standard for the data contained RFID tags for item-level tracking. The EPC can hold more data than a bar code, and becomes in some sense a mini database embedded in the item. Secondly, RFID allows data capture without the need for a line of sight, another significant advance over the bar code[9]. This means that the need for physical manipulation or access to individual items (often stacked or piled) is virtually eliminated for purposes of identification and tracking. This is not the case with the bar code, which must be "seen" at close range by scanners in order to be identified. Some applications limit the read range of RFID tags to between 0.15 – 0.20 metres, but the majority have a range of around a metre. Newer tags in the UHF frequency bands could even have a range of 6 - 7.5 metres.[10]

Figure 2.2: Getting underneath RFID

Schematic representation of RFID at low–frequency (LF) and high frequency (HF)



Source: "RFID : A key to automating everything", Scientific American, January 2004.

RFID is indeed more than the next generation of bar codes. It creates a variety of interfaces that can connect computers directly to individual physical items, and even to people. One of the larger RFID networks in the world is the Joint Total Asset Visibility (JTAV) network built by the US military over the last ten years: the network uses active RFID tags and GPS locators to globally track military supplies.[11] RFID tags have the potential of containing anything from item location and pricing information to washing instructions, banking details and medical records.[12] RFID is also being embedded under the human skin for purposes of authentication, location and transaction[13], and is under consideration as a mechanism for tracking bank notes[14] and passports[15]. These and other RFID applications are discussed in more detail in Chapter 3.

2.3 Types of RFID

RFID systems are typically classified according to the functionality of their data carrier (transponder or tag). For the most part, transponders are either active or passive. As such, they are categorized according to the power source used by the tag[16]:

1. *Passive tags*: Such tags require no power source or battery within the tag. The tag uses the energy of the radio wave to power its operation. This is the least expensive tag. Passive tag RFID systems are the prevalent types.
2. *Semi-passive tags*: Such tags rely on a battery built into the tag to achieve better performance, notably in terms of communication range. These batteries power the internal circuits of tags during communication. They are not used to generate radio waves.
3. *Active tags:* These systems use batteries for the entire operation, and can therefore generate radio waves even in the absence of an RFID reader.

Active and passive tags can be further classified according to how their data is encoded[17]. Tags can possess read-only, read/write or read/write/re-write capabilities. Tags that have read/write capability can contain additional data such as time of receipt, associated sales order (in the case of retail applications), quality control data etc… On the other hand, read-only tags are only meant to transmit the unique identification data initially written to the tag, like a product code or serial number. Read-only tags are naturally less costly than write-able tags.

2.4 International RFID

The widespread use of any technology requires technical harmonization at the international level, notably in the form of standards. The setting of standards facilitates compatibility and interoperability between technological features, data structures and specific applications.

The tremendous global potential of RFID-based applications is being hindered by the lack of established international standards. With the exception of electronic product codes, there has been a fragmented approach to the setting of standards. Eventually, the lack of standards means that organizations will be forced to incur high costs to ensure compatibility with multiple readers and tags.

There are two main types of RFID standards being developed. The first is RFID frequency and protocols for the communication of readers as well as tags and labels, which is typically being dealt with by international standard-setting bodies, such as the European Telecommunication Standards Institute. The second is the standardization of data formats placed on these tags and labels (e.g. electronic product codes).

In North America, currently the biggest regional player in RFID, there are standards such as Global Tag (GTAG), American National Standard Institute's NCITS-T6 256-1999 and some ISO standards. In the Asia-Pacific region, China has announced that it will develop its own national standard for RFID, in the 900 MHz band. If it works in collaboration with international organizations, this bodes well for the take-up of RFID in the country[18]. The European case is rather more complex, because there is less uniform use of frequencies.

In addition, as mentioned above, RFID data carriers (tags or transponders) and other associated components share spectrum with other short-range systems such as telemetry and alarms. Given this radio component, RFID needs to be in line with any applicable spectrum regulation, such as the use of licensed or unlicensed spectrum, electromagnetic compatibility, interference immunity and safety.

2.4.1 RFID and the Radio Spectrum

RFID systems can be classified on the basis of the spectrum they operate in. Although spectrum use varies depending on national regulation, governments around the world have been trying to harmonize frequency allocation for RFID. In most regions of the world, RFID systems can be used in the low frequency (LF), high frequency (HF) and ultra high frequency (UHF) parts of the spectrum.

Typical LF applications include access control, animal tracking, vehicle immobilization, healthcare applications, authentication, and point-of-sale applications. Typical HF applications include smart cards and shelves for item-level tracking, library tracking, patient monitoring, product authentication, and the tracking of airline baggage. UHF is the recommended frequency range for RFID applications related to distribution and logistics, such as the Electronic Product Code (EPC) standard mentioned earlier in this chapter. UHF bands are highly suited to supply chain RFID applications due to the greater range for transmission of data. The range bands is also widely used for toll collection systems on highways, manufacturing applications, and parking lot access control[19].

The use of RFID in the LF (125-134 MHz) and HF (13.56 MHz) bands is harmonized across regions, whereas RFID operation in the UHF band is not. The differences in UHF operations stem from the allowance of power levels, communication speed, and shared frequency bands. The United States and Canada typically use 915 MHz, whereas Europe uses 868 MHz. Fortunately, though, most UHF RFID tags can function in both bands, with a slight hit on performance.

In the United States, RFID devices operating in the UHF bands are allowed to operate in the ISM bands (Industrial, Scientific and Medical) under conditions defined in Federal Communications Commission Part 15 rules (section 15.247). These rules define operation within the bands 902-928 MHz, 2.4-2.48 GHz, and 5.72-5.85 GHz (Super High Frequency Band). The 902-928 MHz band offers optimum range of operation and is usually preferred for supply chain applications. Part 15 compliant RFID systems typically utilize a frequency-hopping spread spectrum modulation technique in order to maximize power allowances. Part 15 compliant UHF readers can operate at a maximum transmitted power of 1 watt. This maximum can be further raised to 4 watts using a directional antenna, when the system hops across a minimum of 50 channels[20].

Table 2.2: RFID in the Ultra High Frequency (UHF) bands
Main UHF bands used for RFID

Frequency band	Details
433.5 – 434.5 MHz	ISM (Industrial, Scientific and Medical) band implemented in Europe, and under consideration, by Japan and Korea. In April 2004, FCC released rules increasing the maximum signal level permitted for RFID systems operating in the 433.5-434.5 MHz band, following pressure from shipping companies.
865 – 868 MHz	ETSI 302-208 regulations provides additional frequency range, increasing spectrum bank from 250 kHz to 3MHz. Under old regulations, the readers were restricted to half a watt of effective radiated power (ERP), but the new regulations allow them to emit up to 2 watts ERP between 865.6 and 867.6 MHz.
869.4 – 869.65 MHz	There is a very small 250 kHz unlicensed spectrum allocation in Europe that could be used for RFID and other applications, at up to 0.5 watts ERP. This has been used, but performance is limited.
902 – 928 MHz	This is an unlicensed band available for use in North America by systems deploying spread spectrum transmission. This band would be shared with other non-RFID applications, such as some wireless LAN systems.
918 – 926 MHz	This is the Australian spectrum allocation for RFID, up to 1 watt ERP.
950 – 956 MHz	Japan has set aside this band for RFID applications (regulations not yet finalised).
2.4 GHz (Microwave)	Unlicensed ISM band that is available in most regions in the world, by systems deploying spread spectrum transmission. This band is also used by Bluetooth systems and Wireless LAN systems (e.g. IEEE 8092.11b and 802.11g)

Source: Adapted from Auto-ID Centre, 2004. RFID Journal (9 November 2004).

In Japan, RFID tracking using UHF tags was resisted for a number of years, as relevant parts of the spectrum had been allocated for mobile phones, taxi and truck communications systems, and a public wireless network for disaster prevention. Since then, however, the MIC (Ministry of Information and Communications) has opened up the 950 – 956 MHz band for RFID trials. The Standardization Administration of China (SAC) announced in 2004 that it has set up an RFID Tag Standards Working Group to develop China's national standards.

UHF is critical to the widespread adoption of RFID because it is in this frequency band that the extended read range needed to track goods in a supply chain setting is possible. The current status of UHF bands is set out in Table 2.2. With the growing importance of RFID, governments and international organizations are aiming to minimize differences between regions, and to ensure that sufficient spectrum is available for RFID applications.

2.4.2 Key international organizations for RFID development

Some of the key international organizations involved in RFID standardization and spectrum allocation are briefly presented below

EAN.UCC

In 2000, the Global Tag (GTAG) initiative was launched by EAN International and the Uniform Code Council (UCC). GTAG is mostly deployed in the United States, and covers both UHF RFID technology (including air interface) and data formats. The air interface aspects of GTAG have now been merged with ISO 18000 Part 6.

International Standards Organization (ISO)

Standards for RFID have typically been adopted for specific applications, e.g. animal tracking. In May 2000, the International Standards Organization (ISO)[21] ratified the "Smart Label" standard. The new ISO/IEC 15693-2 specifies how data is to be passed between tags and readers and covers only the 13.56 MHz frequency. More recently, the organization is working on standards for tracking goods in the supply chain using high-frequency tags (ISO 18000-3) and ultra high-frequency tags (ISO 18000-6). For animal tracking, the ISO has adopted international standards ISO 11784 and 11785.

The three main ISO standardization areas relative to RFID are the following: identification cards and related devices, automatic identification and data capture techniques, and conformance.

Table 2.3 provides an overview of the various ISO standards in these three areas.

Table 2.3: ISO Standards
Overview of ISO standards related to RFID

Identification Cards and Related Devices (JTC1/SC17)

Standard	Area	Details
ISO/IEC 10536	Identification Cards: Contactless Integrated Circuit(s) Cards	Typical range of 7-15 cm. RFID at 13.56 MHz
ISO/IEC 14443	Identification cards: Proximity Integrated Circuit(s) Cards	Typical range of 7-15 cm. RFID at 13.56 MHz
ISO/IEC 15693	Contactless Integrated Circuit(s) Cards: Vicinity Cards	Typical range of up to 1 metre. RFID at 13.56 MHz

Table 2.3: ISO Standards (cont'd)

Automatic Identification and Data Capture Technologies

Standard	Area	Details
ISO/IEC 15961	RFID for Item Management - Data Protocol: Application Interface	Defines Common functional commands and syntax features (RFID tag types, data storage formats, compression schemes), independent of transmission media and air interface protocols. Companion standard to ISO/IEC/15962
ISO/IEC 15962	RFID for Item Management - Protocol: Data encoding rules and logical memory functions	Specifies interface procedures used to exchange information in an RFID system for item management. Protocols ensure correct data formatting, structure of commands, and processing of errors in the system.
ISO/IEC 15963	RFID for Item Management – Unique Identification of RF Tag	Specifies numbering system, registration procedure and the use of uniquely identifiable RFID tags.
ISO/IEC 18000	RFID Air Interface Standards	This series of standards provides a framework to define common communications protocols for international use of RFID, and where possible, to determine use of same protocols for different frequencies. This series deals with only air interface protocol and not concerned with data content of physical implementation of tags or readers.
ISO/IEC 18001	RFID for Item Management – Application Requirements Profiles	

Conformance

Standard	Area
ISO/IEC 18046	RF Tag and Interrogator Performance Test Methods
ISO/IEC 18047	RFID Device Conformance Test Methods

Source: Auto-ID Centre, January 2004

European Telecommunication Standards Institute (ETSI)

The European Telecommunication Standards Institute (ETSI) produces consensus-based telecommunications standards with 55 member countries. ETSI standards relevant to RFID operation in the UHF bands are defined in ETSI EN 300-220[22]. Until 2004, compared with the United States, UHF bands in Europe were limited in power, bandwidth and duty cycle. In September of that year, the ETSI Technical Committee - Electromagnetic Compatibility and Radio Spectrum Matters (ERM), delivered a two part Standard (EN 302 208) giving the industry new tools to make the best use of the available frequencies for RFID. As indicated above, the new standard expands bandwidth available for RFID applications and extends power limits[23] (Table 2.3). This will allow European RFID readers in the UHF band to perform nearly as well as UHF readers operating under the Federal Communication Commission (FCC). The data rate between the reader and the tag, however, has been reduced in the new standard. This is due to the fact that only 3 MHz of spectrum is available in Europe for RFID (compared with 26 MHz available in the United States). In order to maximize efficient spectrum use, the regulation divides this relatively narrow bandwidth into 15 channels of 200 KHz each (Figure 2.4).

The new standard was written by Task Group 34 within ETSI. In November 2004, the Group will begin its work on a code of practice for RFID applications in the UHF bands. In so doing, it will also assess the extent to which this lower data rate will pose a problem for users, and whether modifications to the standard are necessary.

Table 2.4: ETSI Regulations for RFID: Then and Now
ETSI 200-220 vs. ETSI 302-208

	ETSI 300-220	ETSI 302-208
Frequency	869.4 – 869.65 MHz	865 – 868 MHz
Bandwidth	0.25 MHz	3.0 MHz
Maximum Power	0.5 watts ERP	2.0 Watts ERP
Channels	1	15
Duty Cycle	10% (6 mins/hour)	97.5% or more
Data Rate	Similar to data rate in United States	30% the data rate in the United States

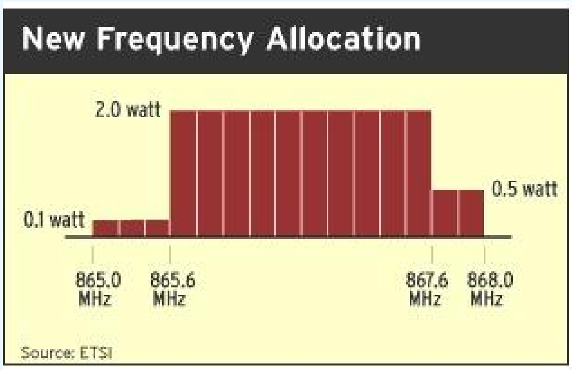
Source: RFID Journal, ETSI.

The European Radiocommunication Office (ERO)

The European Radiocommunication Office (ERO) is the permanent office that supports the Electronic Communications Committee (ECC)[24]. The ECC is the telecommunications regulation committee for the European Conference of Postal and Telecommunications Administrations (CEPT), and represents 46 countries across Europe.

The main tasks of the ECC are to develop radio-communications policies and coordinate frequency allocation, in particular the 9 kHz to 275 GHz frequency range. Recommendations related to the use of short range devices (SRDs) are found in ERC Recommendation 70-03. The ERC Decision ERC/DEC(01)04 on March 12, 2001 addresses non-specific Short Range Devices, such as RFID, operating in 868.0-868.6 MHz, 868.7-869.2 MHz, 869.4-869.65 MHz, and 869.7 - 870.0 MHz.

Figure 2.3: ETSI's New Frequency Allocation for European RFID
ETSI Rules under 302-208



Source: RFID Journal, ETSI.

EPCglobal

A joint venture between the EAN International in Europe and the Uniform Code Council in the US resulted in the creation of EPCGlobal, formerly known as the Auto-ID Centre. The Auto-ID Centre was founded in

1999 and was headquartered at the Massachusetts Institute of Technology (MIT). Its original mandate was to define standards for UHF RFID. On 26 October 2003, the Centre was closed and its technology transferred to EPCglobal. This organization's main focus is the standardization of the data format embedded in the RFID tag or label.

EPC, or electronic product code, is simply a number, typically from 64 to 256 bits long, for the identification (and tracking) of individual items. This is now an internationally accepted item-level code, and replaces the traditional bar code. RFID is the favoured medium to transmit and read that number remotely, and thus EPC and RFID are complementary. The Auto-ID Centre chose not to select a specific type of RFID system to be used for EPCs in order the allow maximum flexibility in the choice of frequencies. EPC has helped to significantly increase the adoption of RFID products across Europe and North America.

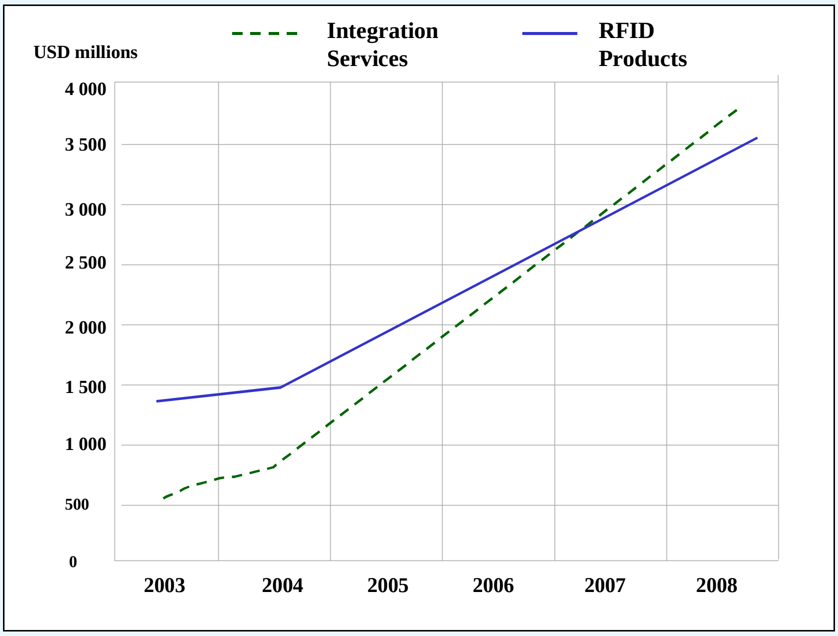
3 RFID IN APPLICATION

This chapter begins with a brief look at the market for RFID, before exploring different areas for RFID deployment, from government services to business and lifestyle applications.

3.1 Nascent markets

According to Venture Development Corporation (VDC), global shipments of RFID systems (hardware, software, and services) reached nearly USD 965 million in 2002. VDC expects the shipment market to reach USD 2.7 billion by 2007. In terms of the market as a whole, RFID systems reached $1.3 billion in 2003, and VDC expects the market to experience a compound annual growth rate (CAGR) of 43% through 2007. The firm Frost and Sullivan is slightly more optimistic with an estimated total of USD 1.7 billion for RFID systems in 2003, with predictions of USD 11.7 billion by 2010[25]. Frost and Sullivan predicts that the total RFID-based applications market will experience a compound annual growth rate of 32.2[26]. Worldwide sales of RFID integration services are expected to reach USD 2 billion in 2006 and surpass sales of RFID products in 2007 at approximately USD 2.8 billion (Figure 3.1).

Figure 3.1: Worldwide RFID sales
Sales of RFID products and integration services from 2003 to 2008



Source: OECD Information Technology Outlook 2004, citing Allied Business Intelligence.

Most analysts agree, however, that much of the growth thus far has come from traditional and established applications such as security/access control, automobile immobilization, animal tracking, and toll collection. Supply chain management applications will most likely drive the growth of RFID technology in the short term. However, emerging application segments, such as electronic product codes and item-level tracking will provide the catalyst for widespread RFID adoption across numerous vertical markets in the medium term.

The Yankee Group predicts that consumer goods manufacturers, in particular, spent an average of USD 6.9 million each on RFID in 2004[27]. Currently, RFID tags for item-level tagging cost from 40 cents to USD 10.0 each, and active tags cost between four US dollars to hundreds of dollars There are a number of different predictions with respect to the declining costs of these tags. Some analysts predict that tags will cost as little as five cents in the near future. The timeline for this is uncertain. Analysts at Gartner predict that by 2009, the most competitive RFID tags will still cost about 20 cents. Some of the big players pushing for RFID development are Texas Instruments[28], Alien Technology[29], Philips Semiconductors[30], Hitachi[31] and Matrics (now Symbol Technologies)[32].

3.2 Business applications

This section describes some of the key business applications that use RFID, such as transport, logistics, access control, supply-chain management, manufacturing, agriculture and health care.

3.2.1 Transport and logistics

One of the most promising areas for the application of RFID is public transport. RFID was first deployed for collecting fares on toll highways. Public transport companies are continuing to suffer losses due to the time-consuming and expensive sale of travel passes and tickets through automatic dispensers or in vehicles. Electronic fare management systems using RFID have been fairly successful in reducing overhead for transport companies and in facilitating travel for commuters. Typically, such systems use contactless smart cards, which last for about 10 years and are not easily damaged by liquid, dust or temperature fluctuations. In Europe, the Parisian mass transit authority, RATP, one of the most advanced networks in the world, uses RFID-based automated fare collection technology. The mass transit system in Seattle (United States) uses an Philips RFID contactless smart card for fare collection. In 2004, Transport for London (TfL) announced plans to spend up USD 65.3 million on new digital enforcement technologies for the Congestion Charging Scheme (CCS) for vehicles, which will most likely include radio frequency identification (RFID) tags for the identification of number plates[33]. But the Asia-Pacific region remains a leader in this field. The Korea "bus card" based on RFID has been around since 1997. Thailand's Bangkok subway uses RFID contactless round token system for individual trips as well as a contactless card system (i.e. one which does not require the contact with a reading machine) for regular travellers. In Tokyo, even taxi drivers have begun using RFID to facilitate their operations. A trial of the payment system was launched in October 2004, and consists of a mobile phone with an embedded chip that stores an allocated amount of funds already charged to the phone owner's credit card from JCB International (Box 3.1).

In addition to the transport of people, RFID is being used increasingly in the transport and delivery of parcels and postal items. RFID enables improved item tracking during the sorting of mail and delivery processes. More importantly, the technology does not require line of sight to assess an item and to track its location, or to transfer information. This will allow a great number of individual letters or parcels to be routed without physical manipulation.

Airlines are actively exploring the possibility of integrating RFID in baggage tags, in order to enhance the efficiency of systems employed to track customer baggage. One of the busiest airports in the world, Hong Kong International Airport (where passengers number some 35 million annually) announced in May 2004 that it would deploy RFID reader infrastructure across its extensive baggage handling facilities. At various nodes within the airport, including baggage carousels, unit load devices (ULDs) and conveyors, reader systems will have the capabilities to read and write to RFID tags that will be applied to passenger luggage. RFID-enabled handheld readers will also be used for handling luggage "on the move"[34].

Box 3.1: Radio that cab fare
Taxis, mobile phones and RFID in Tokyo

Tokyo-area taxi drivers are exploring the possibility of being paid via RFID and mobile phones. Japan-based credit card company JCB International started a trial of the payment system (QUICPay or "Quick and Useful IC Payment") in November 2004.

Selected taxi drivers were given RFID readers, which can read a passenger's mobile phone chip, determine the fund balance remaining, and deduct the requisite amount. All mobile phones used in the trail will be compatible with NTT DoCoMo's mobile wallet handsets. These are equipped with the FeliCa chip from Sony, which uses Near Field Communication (NFC) passive RFID technology.

Source: Japan Corporate News and RFID Journal, October 2004

3.2.2 Security and access control

RFID technology is increasingly being deployed to control access to restricted areas, and to enhance security in areas such as laboratories, schools, and airports. Many employee identification cards already use RFID technology to allow staff to enter and exit office buildings. The security programme of the Canadian Air Transport Authority (CATSA), for instance, uses smart cards equipped with RFID first deployed in March 2004. These contactless cards and readers offer physical access control enhanced by biometric authentication to restricted areas.

Educational institutions are also exploring the advantages of RFID for monitoring student populations. In China, in November 2003, RFID deployment began in an attempt to prevent fraud. China's Ministry of Railways and Ministry of Education were facing problems in authenticating genuine student cards, in particular for the purpose of checking eligibility for travel discounts. 10 million smart labels and microchips were delivered to China's Ministry of Education in 2003. Each chip can hold up to 2 kilobytes of data, and can be read at a distance of 1.5 metres. The chip presently stores the student's identification data and in the future will include all diplomas and degree information. Libraries are also using the chip to facilitate check out and to control the lending of books. Information on the tag is kept secure through the use of cryptography and includes tamper safeguards[35].

The Rikkyo Primary School in Tokyo (Japan) has taken RFID a step further. In September 2004, the school carried out a trial of active RFID tags in order to monitor the comings and goings of its students in real-time. The system records the exact time a student enters or leaves the campus, and restricts entry to school grounds. Since the tags can be read by scanners from a distance of up to 10 meters, they don't require students to stop at designated checkpoints (Box 3.2). The Asia-Pacific region is a leader in this field, but now schools in North America have begun following suit. One example is the Enterprise Charter School in Buffalo (New York), which deployed an RFID smart label system from Texas Instruments in 2003. This system, in addition to exercising control over access to the school campus, is also being used to identify and secure assets such as library books and laptop computers. The ID cards enable students and staff to make selected purchases at the cafeteria[36].

3.2.3 Supply-chain management

RFID represents one of the most significant advances in supply-chain management since the first bar code was scanned in 1974. Coupled with wireless systems and intelligent software, RFID has the potential to further revolutionize the supply chain[37]. Already, supermarkets are tagging pallets, cases, and other returnable transit containers such as plastic crates used for fresh foods. Tagging these items permits transparent and total visibility of assets and inventory. The ability to write to the RFID tag also allows the entry and management of information such as contents, expiry date, manufacturer and country of origin. In this manner, RFID enhances the accuracy of shipments and deliveries. In addition, it can address what is known as "product shrinkage" or product theft. The majority of this loss occurs between the manufacturer's front door and the retailer's back office. Electronic product codes transmitted through RFID can determine product arrival and departure at all points of the supply chain, thereby pinpointing the location where a given product was last reported seen. RFID can be used in the tourism and hospitality industries, for instance, to manage uniforms for their staff (Box 3.3).

Box 3.2: RFID - The student's new hall monitor?
Real-time tracking of students at Tokyo's Rikkyo Primary School

At Rikkyo Primary School in Tokyo, full roll-out of an RFID tracking system is set for April 2005. All students and authorized staff are given active RFID tags, which can be attached to book bags or other personal items. This allows for the real-time monitoring of students, thereby ensuring their safety and thwarting truancy.

The main features of the system are as follows:

1. Individual Recognition via active RFID tags: The system automatically and instantaneously records the comings and goings of multiple individuals passing by the many scanners, at a distance of up to 10 meters.
2. Unobtrusive Monitoring of School Entry or Exit: Due to the 10-meter read range, students and teachers need not stop at security checkpoints or specialized gateways.
3. Detection of unauthorized entry: Unauthorized entry is detected by this system through RFID tags and infrared sensors.
4. Privacy and Data Security: The active RFID tags carry no individually identifying information, but only a number code. Thus, no personal information can be obtained from the tags should they be lost or stolen.
5. E-mail notification: The RFID system can send an e-mail notification to parents or guardians when their child enters and leaves the campus.
6. Dedicate Website for Confirmation of School Arrival/Departure: Teachers and staff can verify the arrival and departure of all the children at the school via a dedicated and secure web site, which shows both active RFID tag timestamps and security camera imagery. Parents and guardians also have secure access to this site to check information about their own children.
7. Urgent E-mail Network: The system supports an e-mail based urgent contact network feature, for providing important informaiotn to the school community on a timely basis. This can be used, for example, in the case of a public safety warning due to accidents or weather-related incidents.

Source: Fujitsu, September 2004

Box 3.3: RFID in the closet
Tracking uniforms

Open 24 hours a day, Star City Casino in Sydney (Australia) manages a wardrobe inventory of 80'000 uniforms valued at some 1.8 million USD. Its guest rooms, health clubs, gaming floor, nightclub, sports facilities, etc., each require staff to dress in themed garments. A solution for managing the complex laundry procedures in such an establishment was needed.

RFID provided just such a solution. As early as 1997, RFID tags were embedded in each uniform (e.g. in the waistband, shirttail or collar), enabling their tracking from the point of issue to the laundry chute, from the laundry cart to the laundry machines, using strategically-placed RFID readers. Unlike the traditional barcode, which typically has to be replaced every one or two years, RFID chips usually outlast the associated garment itself (i.e. chips can endure over five years).

RFID readers and tags render inventory management more accurate. Tracking through RFID ensures that the right uniforms are ready to wear every time there is a change in shifts. All of the above has meant significant cost savings for the Casino.

Source: Accenture, Technology Labs

RFID is seen by many businesses as a key method to streamline business processes and cut costs. Procter and Gamble, one of the earliest adopters of this technology, expects to increase after-tax profits by USD 150 million and to realize a working capital increase of USD 1 billion through the adoption of RFID[38].

3.2.4 Medical and pharmaceutical Applications

An important application of RFID is in the medical and pharmaceutical fields. In hospitals, RFID enables a fully automated solution for information delivery at the patient bedside, thus reducing the potential for human error and increasing efficiency. When used in combination with secure wireless networks, such as Wireless LANs, tags embedded in medication or on patient bracelets can provide fast electronic access to patient records and other information. Key examples of RFID use in health care include:

- *Point-of-care data delivery*: Staff badges, medication packaging and patients' identity bracelets contain RFID technology. This facilitates identification of a patient by caregivers, who are thus able to submit orders in real-time at the very point of care, instead of being handwritten and sent off for future input. This system saves time, and reduces the chances of human error. Any changes in medication can be updated immediately, and any contra-indications automatically cross-checked. In addition, diagnostic codes can be verified upon admission, thereby ensuring timely and accurate patient billing.
- *Patient location*: Tracking the location of patients is particularly important in cases of long-term care, mentally challenged patients, and newborns. But its benefits are even more widespread. The ability to determine the location of a patient within a hospital can facilitate and expedite the delivery of health care. For instance, when a patient arrives in a lab for a radiology exam, medical staff is instantly alerted via the RFID tag, and the transfer of records can be effected immediately. The development of RFID technology for tracking patients received a boost in October 2004, when the United States' Food and Drug Administration (FDA) approved subcutaneous RFID implants for patients[39].
- *Asset tracking and locating*: Tracking medical staff as well as medical equipment can ensure an efficient response to medical problems and emergencies. This also optimises inventory management, saving unnecessary purchasing costs[40].

Box 3.4: RFID to combat counterfeit drugs
Pilot Project "Jumpstart" at pharmaceutical distribution centres in the United States

By using RFID tags on bottles of medication destined for pharmacies and drug stores, the pharmaceutical industry hopes to better detect counterfeit drugs, as these do not typically travel through the usual supply chains. In July 2004, a group of manufacturers, including Abbott Laboratories, Johnson & Johnson, Pfizer, and Procter & Gamble, began shipping bottles of pills with RFID labels. McKesson Corp. and Cardinal Health are the participating distributors.

In addition to tracking fake drugs, tagged bottles can serve to prevent theft, as well as to manage recalled and outdated medication.

As pharmacies receive medication through specific distribution centres, bottles would be tagged reflecting their point of origin. Alarms could thus be raised when an incomplete or inaccurate set of locations were found on a tag.

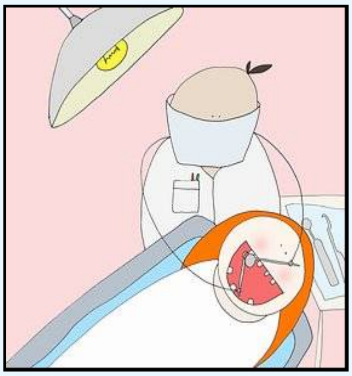
In early 2004, the USA's Food and Drug Administration issued a report recommending that pharmaceutical companies use RFID on bottles of the most commonly counterfeited drugs starting in 2006 and on bottles of most drugs by 2007.

Source: Information Week, 26 July 2004, at http://www.informationweek.com/showArticle.jhtml?articleID=25600213

For instance, a number of pilot studies are under way to determine how RFID can improve the accuracy of the delivery of blood supplies of the appropriate blood group to patients, compared to the current bar-code method. RFID offers the distinct advantage of enabling the accurate matching of blood samples/transfusions to the correct patient, through non line-of-sight data transmission, which can be effected through and around the human body, clothing, bed coverings and non-metallic materials[41].

Box 3.5: Sink your teeth into RFID
Using RFID to manufacture dental prosthetics

The French company Dentalax has launched an RFID-based system for the manufacturing of crowns and bridges for the dental industry.



A dentist typically makes an initial cast of a patient's teeth, which is sent to a dental laboratory. The lab uses the initial cast to make a second cast, which is then used to manufacture the bridge or crown. In the Dentalax system, an RFID tag or chip is embedded into the second cast before it hardens. The tag is thus locked into the dental prosthesis, recording every action or procedure on the prosthesis. The identity of the cast can also easily be checked using an RFID reader, ensuring that it reaches the correct recipient. Before the prosthesis is delivered to the dentist, the lab retrieves the data on the RFID tag, and saves it on a smart card that can be delivered to the patient. Such cards may be made available to succeeding practitioners as required. T

The Dentalax RFID package is currently priced at 380 Euros, and is made up of 100 PicPass chips, the requisite software and one reader. Individual readers are priced at 290 Euros, and a pack of 100 chips costs 100 Euros.

Source: RFID Journal, 25 October 2004.

In sum, the advantages of RFID deployment in-patient care lie in enhancing patient safety and optimising hospital workflow. Its use is equally pivotal in the pharmaceutical industry, where electronic product tags on medication can curtail counterfeiting (Box 3.4), streamline revenue distribution, reduce prescription errors, and decrease returns. RFID can also assist in the manufacture of medical prosthetics, such as dentures or crowns (Box 3.5). Finally, tracking medical waste materials as they are moved for disposal may also prove to be an important application of RFID: IBM and Japan's Kureha Environmental Engineering are currently testing waste containers equipped with RFID tags[42]. The University of California is even considering embedding RFID in cadavers to thwart the sale of body parts on the black market, and to ensure that bodies donated to science are treated with respect[43]. The use of RFID would allow authorized individuals walking past the body with a handheld device to readily identify the cadavers, or locate individual body parts that had become separated from the corpse.

3.2.5 Manufacturing and processing

Manufacturing and processing is increasingly relying on computer-controlled mechanisms and information technology. RFID tags, coupled in some cases with sensors and actuators, can enhance accuracy and overall efficiency in factories and labs. For instance, the use of RFID can speed up the assembly line for the manufacture of golf cars (Box 3.6). For products that are sensitive to time or external conditions, RFID enables tracking and monitoring: for instance, in the case of selected health and beauty products (Box 3.7).

3.2.6 Agriculture

Agricultural applications for RFID, from wineries to meat packers, have been emerging over the last couple of years. A good example is the RFID trial launched in November 2004 to track containers of frozen beef from Namibia to the United Kingdom. The goal of such a system is to track shipments, for the purpose of ensuring the quality of the meat[44]. RFID tags included with the shipments will be able to detect and record where a container's seal has been tampered or broken during its journey, and when a particular shipment has been static in excess of a pre-determined length of time.

Box 3.6: RFID eases production of golf cars
Assembly Line RFID

Golf car manufacturer Club Car streamlined its assembly process through the use of RFID. Introduced in 1999, RFID has since cut the time required to assemble each vehicle from 88 minutes to about 46 minutes.

Under the old system, workers used a handheld reader to scan the bar code label on the vehicles for tracking purposes. These were manually pushed between workstations. The new system uses a single production line that moves vehicles automatically, and uses RFID to define and verify the assembly process at each stage.

When a new vehicle is complete, the RFID tag is read and all accessories and specifications are checked automatically against a list of production requirements.

Source: RFID Journal

Box 3.7: Tag that soap
Canadian soap maker looks to RFID

Canada's Canus manufactures skin care products manufactured from goat's milk. In April 2004, the company began a pilot scheme to deploy RFID in its three distribution centres and two manufacturing plants. The main objective was to streamline operations and reduce waste. RFID is meant to save the company resources, as the tags can check the status of shipments and deliveries and determine the exact location of a shipment while in transit.

In the future, Canus plans to extend the RFID system to enable real-time monitoring of its products and their associated processes. The bulk of its fragrances, which are made from goat's milk, must be maintained at temperatures ranging from 4 and 40 degrees fahrenheit. RFID tracking coupled with monitoring can determine the point at which the products transgressed pre-set limits (e.g. temperature, expiry date etc.).

Source: Canus

The use of RFID tags in greenhouses can offer a great improvement over traditional bar codes. The latter need to be clean and dry to be read by a scanner. RFID tags, on the other hand, are protected from water or dirt and can be read at a faster rate. RFID sensors with antennae mounted upon benches and located within greenhouses can be used by plant-growers for purposes of tracking production and developing accurate inventory[45].

Farming is an area fipe for RFID implementation (Box 3.8), and a number of farms in the United States have begun using RFID to help track their produce. For instance, "Global Berry Farms" in the state of Michigan has started a trial of RFID tags on its crates of blueberries, and is working with other interested companies, from pharmaceuticals to educational institutions, to further test its systems[46].

3.3 Government applications

It is not only private industry that is using RFID to streamline business processes. National governments , too, have begun exploring the potential benefits of this technology, particularly in the current climate of political uncertainty and international terrorism. This section describes a few pioneering governmental applications for RFID.

Box 3.8: Tag farming
RFID for efficient farming

Paramount farms processes about 60 percent of the US (United States) crop of pistachios, and it exports to more than 20 countries. It now uses an RFID system to automate and streamline a core business operation - processing the incoming shipments of pistachios from its many partners (50 per cent of the pistachios it processes come from approximately 400 partners). Only a narrow period of time can be allocated to processing,, e.g. six weeks, given the perishable nature of the produce. And in order that the company's partners are paid for their shipments fairly, the company must be able to accurately calculate and account for those nuts that are acceptable for consumption.

The farms' automated processing capabilities are based on a new GRS, or grower receiving system, which uses Microsoft technology and RFID. Upon receipt of a shipment, this receiving system weighs the trailers that are filled with nuts, and then each full trailer is tagged. Inside the "scale house", there are a number of RFID readers. The tags used are 915 MHz and passive. The unique ID number of each trailer records such information as weight, license plate number, and owner information for later retrieval from the GRS database. This has, *inter alia*, reduced potential disagreements between Paramount and its partners.

Before the introduction of RFID, a Paramount employee would have had to manually check a stencilled number on the side of each trailer as it entered the scale house, and then write down the trailer number. This left the system open to human error and inaccuracies. Information about product delivery and status is also more readily available to managers through the GRS database (as well as handheld scanners), thereby allowing more informed decision-making.

Source: RFID Journal

3.3.1 E-government

Many public sector authorities are considering RFID to make e-government services more flexible, efficient and secure. In the United States, for instance, the inclusion of RFID tags on driver's licenses is under debate. The main objective of such tags would be to help thwart fraud: the downside, as, many privacy advocates argue, is that such remotely readable tags will make it easier for government agencies to spy on citizens and increase the possibility of "identity theft". Virginia, in the United States, is one of the first states to consider the use of RFID in drivers' licenses. These may in the future employ a combination of RFID and biometric data (e.g. fingerprints)[47]. In February 2005, the United States House of Representatives approved a measure that would compel states to design their driver's licenses by 2008 to comply with federal antiterrorist standards[48].

RFID enables the so-called "Internet of things", which may be further exxtended to the tracking of human beings. The United States' Food and Drug Administration has already approved implantable RIFD chips for people (See Section 5.1). The concern among ordinary citizens and privacy advocates vis-à-vis this development is undeniable, as hoax stories such as a U.S government plan to implant all homeless people with RFID tags have been widely circulated over the Internet.[49]

In Europe, there has been increasing press coverage since 2001 on the possibility of embedding RFID on Euro bank notes, in order to thwart counterfeit, fraud, and money laundering. The European Central Bank has been in discussion with various technology partners such as Philips Semiconductors, Infineon, and Hitachi on projects to tag European currency[50].

3.3.2 Defence and security

RFID offers significant potential for governments wishing to fortify their national defence and security systems, particularly in a climate plagued with increased international terrorism. Border crossings offer a good example. The border between the special administrative region of Hong Kong and Schenzhen (China) is highly regulated and is a case in point: since 2002, China's Schenzen authorities have installed an RFID system to facilitate the flow of low-risk traffic and goods across that border, and to thwart smuggling.

As already observed, the use of RFID can go further still, affecting the lives of individual citizens. Following the events of 11 September 2001, the United States has already mandated that all American passports contain biometric data, such as fingerprints. This requirement has been extended to apply to nationals from those countries not requiring a visa for travel to the United States. More recently, the government has advocated the use of RFID in combination with biometric data on passports. This measure has raised concerns among some technologists and civil libertarians. They fear that information on such chips can be read remotely, thus enabling a person's biographical information and photo to fall into the wrong hands[51].

3.3.3 Library systems

RFID is increasingly being deployed in libraries to automate the loan and return of library materials through real-time visibility of inventory. These were traditionally identified using bar code labels that had to be read individually with bar code readers. With RFID, libraries can check in and out materials using scanners (placed on shelves or in hand-held devices), thereby resulting in the reduction of personnel, a higher degree of accuracy in inventory management, and fewer losses. The Vatican City Library has opted for RFID to manage its collection (See Box 3.9).

Box 3.9: Tagging the Ancient
Vatican Library deploys RFID

The Vatican Library, containing a 40-million piece collection of books and manuscripts, began deploying RFID in 2003. About 30'000 books were tagged as of October 2004. It is likely that an additional two million pieces will be tagged.

RFID was chosen due to its low cost and for the fact that it did not damage the collection, which includes ancient manuscripts and the oldest known complete version of the Bible.

Source: CNN.Com, 14 October 2004

In the Netherlands, publishing companies are getting into the business: NBD Biblion, which sells 2.7 million books to Dutch libraries annually (i.e. 80% of the national market), began tagging all of its books in September 2004[52]. In Tokyo, the Roppongi Hills Library has been tagging its books since 2003[53].

3.4 Consumer applications

Though they may not always be aware of it, individual consumers have been exposed to RFID in action: on toll roads, in offices, and in libraries (as discussed above). Over the next few years, these small tags will be increasingly used to add further convenience to day-to-day living, from sports events to retail shopping. This section describes some interesting current applications of RFID and their future potential.

3.4.1 Personal welfare and safety

RFID applications for the medical industry (e.g. hospitals) mentioned in Section 3.2.4 above are set to address current lacunae in patient treatment and welfare. But as tags are location-sensitive, they can also be used to enhance personal safety in general. In this context, not only have schools begun deploying RFID to keep track of pupils, but public leisure parks such as Legoland in Denmark (Box 3.10) are using the technology to attract families concerned for the personal safety of their children and elderly relatives. Large shopping malls and department stores may not be far behind, particularly as many have begun using RFID readers and tags for tracking inventory.

Box 3.10: LEGO of my RFID!
RFID helps parents keep a tab on their kids

When it opened in March 2004, the Legoland amusement park in Billund, Denmark launched a child-tracking system based on RFID and wireless LAN.

Parents can choose to rent RFID-enabled wristbands from the park's administration for the purpose of keeping a check on their children's whereabouts.

Parents and guardians wishing to locate separated or missing children can use their mobile phone to send a text message to an application known as "kidspotter". The application rapidly returns a text message stating the details of the child's last location, such as coordinates, name of park area, etc…

Source: Network World, 3 May 2004, Vol. 21, Issue 18.

See also http://www.lego.com/legoland/billund/Default.asp?locale=2057&bhcp=1 .

3.4.2 Sports and Leisure

In the sporting world, RFID tags have been used in marathons to track runners, allowing both participants and spectators to benefit from the combination of mobile SMS and RFID (Box 3.11). RFID technology has been used to determine with remarkable accuracy the winner in an Indy 500 car race (Box 3.12) by tracking cars as they pass the finish line.

Hands-free access systems using RFID for ski lifts have been introduced since the last 1990s. For instance, in 1999, Texas Instruments together with the Austrian company TeamAxess deployed an RFID system for access to ski lifts and slopes in Europe. Remote-operated gates equipped with readers can detect a valid ski pass and open automatically, thus leading to shorter line-ups and more efficient customer processing. The credit-card sized RFID-enabled ski pass can easily fit into a jacket pocket, and is scanned in place, thus obviating the need for manipulation[54]. The passes can also be used to locate skiers (e.g. in cases of injury, or for the location of children).

RFID can also assist in preventing theft of property, particularly in relation to travel or leisure activities. In Germany, for example, Philips Semiconductors introduced an RFID labelling system to protect recreational boats (of which there are 660'000 in the country) from theft by providing secure electronic identification. In the past, boats were simply identified by painting numbers on them. This system of identification suffered the considerable disadvantage of fraudulent removal or modification. Since RFID tags allow the identity of a boat to be determined remotely, German authorities can check the status of a boat against their databases of stolen and registered boats, without the need for a search warrant. The RFID labels are thin and waterproof, and can be read at a distance of up to 60 centimetres, even through materials such as wood or fibreglass. Plans to extend the current system to other forms of high value property such as trailers, caravans and bicycles are being actively considered[55].

In the travel and hospitality industries, RFID tags are enhancing and facilitating customer service. Manchester City Football Club in the United Kingdom was the first football club in Europe to adopt RFID, thereby giving fans ticket-less access to football grounds and significantly reducing the time it takes spectators to enter the grounds[56].

Box 3.11: High-speed RFID

RFID tracks runners in marathons

Marathon organizers in such cities as Boston, London, New York, Berlin, Los Angeles, and Capetown are bringing high-tech communications to participants as they run the course.

For example, all of the official entrants in the 2004 Boston Marathon were issued with the “ChampionChip”, a small token that is either tied onto the runner's shoe or attached to a wheelchair. These chips time the runners at various points throughout the race, including the starting line. As a runner crosses stationary mats located throughout the race, his/her time is recorded.

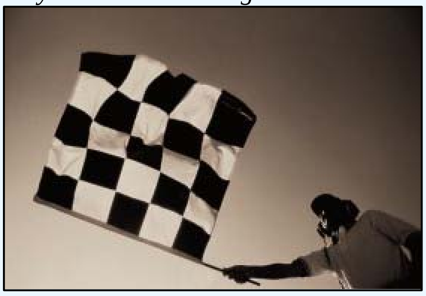
The chips contain RFID tags that transmit the runner's time at the checkpoints to databases operated by the Boston Athletic Association and its technology partners (Hewlett-Packard and Verizon Wireless).

Some 33,000 runners competed in the London marathon on 18 April. Participants could have their positions tracked and recorded by electronic tags attached their shoes. Friends and family of competitors were able to follow their progress by signing up to an SMS text message service that will send athletes' positions as they make their way around the course. Special mats were positioned every 5km along the marathon course. When an athlete ran over the mat, their time and position was sent to an Oracle database. Running over special mats with receivers would send a message to those who signed up to receive the alerts.

Source: ITU Internet Reports 2004 “The Portable Internet”, http://www.itu.int/portableinternet.

Box 3.12: Racing forward with RFID

Indy 500 and active tags



An RFID system by the name of “Tranx Pro”, developed in the Netherlands, is being used for automatic identification and tracking by a number of sports organizations across the world, from car racing to athletics. In the case of the Indy 500 in May 2004, tags embedded in the cars and in the antennas in the asphalt turn the 2.5-mile racetrack into a giant stopwatch that measures the time-gap of successive cars crossing a given point to an accuracy of 10’000th of a second. RFID provides for speeds of up to 200 miles per hour, and with 33 cars completing a lap every 40 seconds.

RFID transponders measuring approximately two square inches in area and one inch thick, are typically installed in the same location on each car, 33 inches from the front and 12 inches above the asphalt. A detection loop installed in the track’s surface at the start/finish line picks up the unique ID code of each vehicle as it crosses the line.

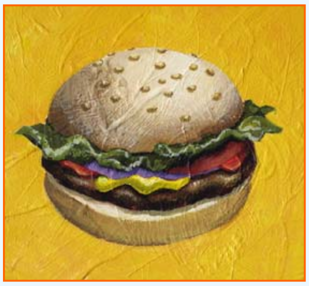
Source: RFID Journal, 31 May 2004.

3.4.3 Shopping and dining out

Wal-Mart was the first to deploy item-based tagging using RFID for the purposes of streamlining their supply chain. Other major stores such as Tesco (UK), Metro AG (Germany), Home Depot (United States), and Mitsukoshi (Japan) are among the growing list of large retailers joining this new method of tagging products. This section looks at RFID in the retail world from the consumer perspective.

Clearly, the advantage to customers of a retail store deploying RFID is a speedier checkout. If every item in a consumer’s shopping basket is tagged and the necessary reader is suitably installed, there should no longer be any need to lay the items on the belt and manually scan each one for purposes of determining the final bill. Eventually, when users will also be equipped with contactless payment cards, the onerous and dilatory checkout procedure could be eliminated. All items in the shopping cart would be automatically debited from the consumer's account upon exiting the store. Early contactless payment solutions using RFID are already being deployed around the globe, for instance for ticketing applications. Calypso is a good example of a global player in this area. And in February 2005, Visa introduced a system using RFID to enable consumers to make purchases by simply waving their cards. Meanwhile, McDonalds have introduced a Mastercard wireless system using RFID to make their fast food even faster (Box 3.13).

Box 3.13: McDonald's and RFID: Lovin' it
Was that with a tag on the side?



McDonald's has chosen to provide a wireless credit card system using RFID technology to make their fast food even faster. Customers need simply wave their "Mastercard PayPass" card near a "VeriFone" RFID card reader. The device then automatically interprets the wave, charging the amount of the order to the customer's MasterCard account.

First tests will be carried out at McDonald's restaurants in New York City and Dallas in late 2004 before nationwide deployment.

Source: San Jose Business Journal, 18 August 2004, http://sanjose.bizjournals.com/sanjose/stories/2004/08/16/daily33.html

Retail stores are not the only ones to benefit from RFID technology. Restaurants can use item-level tagging to improve the customer experience and facilitate the billing process. Pintokona, a Sushi restaurant in Tokyo, has introduced RFID tags to track and price their plates of sushi that are presented on a rotating belt. Sushi freshness is a critical requirement for Pintokona, as dishes should typically be exposed no longer than thirty minutes. RFID tags associated with individual dishes contain the precise time of their placement on the rotating belt, thus facilitating their withdrawal upon the expiry of the pre-determined period. The system also assists with the calculation of the bill, as each tag contains information such as price, sushi type, and chef[57]. Future applications of RFID for the consumer are discussed in Chapter 4.

3.4.4 Smarter homes, smarter people?

An important market segment emerging in technology-savvy environments such as Korea is the use of RFID and other wireless sensor and communication technologies (e.g. Zigbee) for consumer applications such as smart houses and smart cities. There is significant interest in introducing RFID functionality in the construction of new urban landscapes and in consumer appliances. In March 2004, the Korean government opened a museum in Seoul, "Ubiquitous Dream" that includes a mock up of a "smart home". The design includes a networked refrigerator that initiates the automatic re-ordering of food items, contactless security systems and wireless sensors (e.g. for lights), and smart laundry machines (that determine treatment required for different fabrics)[58]. RFID tags, readers and sensors can also create in-home environments that could make it possible for the elderly or physically challenged to continue to live at home. A smart home system could detect, monitors and record the daily living activities of a resident by collecting data tiny RFID tags affixed to household items, thereby ensuring their independence and reducing the burden on caregivers[59]. Data harvested from RFID tags would reassure family and caregivers, for instance that the elderly patient had taken their medication.

If homes seem to be getting smarter, so too are people, with the help of portable smart devices. A good example is RFID-enabled wearable technology such as the "smart watch system", being developed by the University of Washington in collaboration with Intel. This smart watch helps people remember to take their essential items with them when leaving the house, or leaving a public place (Box 3.14).

Like tags, readers are also being developed that are smaller in size, and friendlier to a mobile, and more invisible technological environment. For example, the company SkyeTek developed its new RFID reader, dubbed "M1-mini", measuring 1 inch in diameter and 0.1 inch in thickness[60]. The tiny reader can be integrated in a glove, or in a mobile phone, to read tags on items such as medication to warn users of any contra-indications, or ensure secure access to homes, entertainment systems, and appliances. In the future, clothing may be equipped with sensors, readers and tags[61], for local adjustments or remote monitoring: the collected data would then be sent wirelessly to other devices such as watches, mobile phones or personal digital assistants.

Box 3.14: Watch this RFID: an important step towards smart technological ubiquity
Radio frequency tags in smart watches remind people that they may have forgotten something

A working prototype of what might be called a "smart watch system" has been developed by a University of Washington computer scientist, in collaboration with Intel. The watch is an intelligent, integrated, and responsive system, capable of prompting users who leave the house or workplace without essential items, such as keys, wallet, glasses etc…

The wristwatch acts as an interface and is driven by a small personal server, easily carried in the pocket, which could eventually be integrated with the wristwatch itself. Important items in the household are embedded with RFID tags, and readers are installed in various locations, e.g. home, car, office etc… When the wristwatch passes a reader, the information is sent to a personal server that checks whether all critical (tagged) items are present. In the future, wireless location systems may also determine the location of the user (whether they are arriving or leaving), and use this information for decision-making.

Source: EurekAlert, 6 October 2004, http://www.eurekalert.org/pub_releases/2004-10/uow-awt100604.php

4 RFID IN THE LAB

4.1 RFID and wireless sensor technology

While RFID tags are being tested and deployed in a number of industries, sensor technology is in its early stages of development. The traditional function of sensors is to measure specific phenomena or determine the status of the environment through the collection of physical values, e.g. temperature, humidity, pressure, noise levels, presence of absence of objects, speed etc… The addition of wireless communication capabilities to sensors significantly extends their potential, giving them more autonomy and collaborative potential (e.g. collaboration with other objects or with a remote interrogator)[62].

Not surprisingly, sensors such as temperature tags, vibration sensors, chemical sensors etc., can significantly enhance the functionality of RFID technology. Such smart sensors will provide yet another mechanism for acquiring data. Their integration with accurate time and location-sensitive RFID tags will provide records of the status of a given item and how it has been handled.

For instance, biosensors that can detect that a perishable item has expired are being developed. Such sensors would be tiny and capable of detecting the presence of any biological or chemical agents[63]. Consisting of a transducer and a computer chip, the sensor would be embedded into a single RFID tag that could function inside a water bottle or even in the liquid at the bottom of a package of meat. Although RFID biosensors are some years away, a number of companies, including one of McDonald's largest beef providers, Golden State Foods, has been testing RFID biosensors since 2002. A system made up of RFID sensors would eventually allow the tracking and monitoring of all food supplies, thereby thwarting contamination and even bio-terrorism. In some instances, insurance coverage against terrorism may become available to companies employing RFID biosensor technology.

4.2 RFID and the mobile phone

The use of information stored on RFID tags in combination with sensor capabilities can enable computations and communication with peer objects, which can eventually create an environment in which the context of users and the status of "smart objects" can be continuously determined and monitored[64]. Mobile phones can serve as an important platform for users to communicate with smart objects and open up possibilities for location-based services.

For example, in 2003, the first trial of mobile RFID shopping was run in Tokyo, opening up an entirely new location-based shopping experience (Box 4.1). RFID technology in combination with mobile phones was used to locate customers wishing to receive information about the area. Targeted promotions, entertainment options, and customized shopping information could then be delivered to the customer.

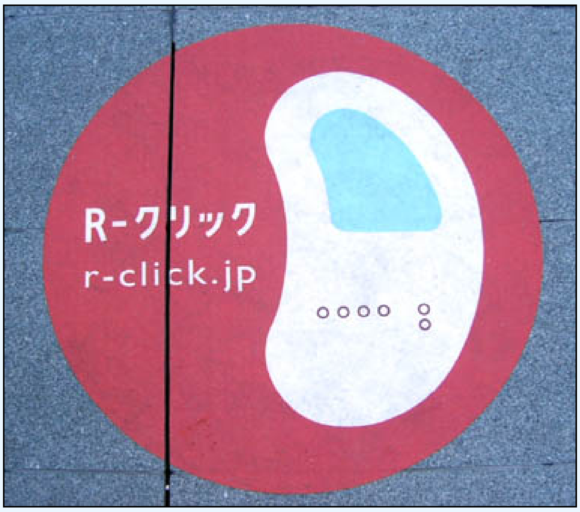
In March 2004, Nokia introduced the Nokia RFID Kit, a GSM phone with RFID reading capability for supply-chain applications[65]. Within a couple of years, the handset manufacturer intends to give consumers the ability to use their mobile phones to access data rich in information about consumer products sold in retail stores, through the use of RFID. Nokia is developing the RFID consumer phone jointly with Verisign. The potential applications of such mobile phones are manifold, including:

- One-touch warranty registration
- Allowing for quick ingredient look-up in supermarkets (of particular use those consumers with allergies)
- Customer Service and brand management (e.g. promotions)

Given the immense potential RFID holds for information and communication access and machine-to-machine communications, technology developers continue to explore its synergies with the increasingly ubiquitous mobile phone. The Near Field Communications Forum (NFC Forum) is using RFID to bridge the connectivity gap between all kinds of devices (such as the mobile phone) and electronic information transfer[66].

Box 4.1: RFID tags and Shopping in Tokyo's trendy Roppongi Hills

This use of RFID tags at Roppongi Hills in Tokyo has now been expanded to retail shopping: the trial of NTT DoCoMo's "R-click" service in 2003 and 2004 was a successful one. The R-Click service delivers information specific to a user's location using RFID tags. DoCoMo has issued about 4'500 RFID tags (embedded in small handheld terminals), which can be attached to users' mobile phones. Subscribers can inform the network of their wish to be located by pushing a button. The default setting is "off", in order not to surprise those customers not wishing to be disturbed by such information. The small handheld device then enables users to receive a wide variety of area information as they walk around the new metropolitan cultural complex of shops, restaurants, entertainment facilities, residences and hotels.



Source: Adapted from *ITU Japan case study on "Shaping the Future Mobile Information Society"* available at http://www.itu.int/futuremobile/

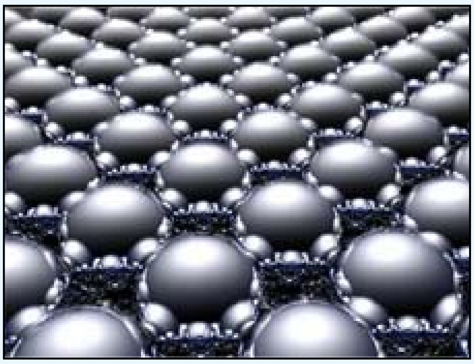
4.3 From smart chips to smart dust

At this time, radio-frequency identification tags are about the size of a grain of rice. But rapid advances in this technology herald an age of microscopic, or even "nano-scopic" computing capabilities. Looking beyond the early phases of RFID deployment, there is a silent revolution gathering momentum – one that applies the computing power in a tag or chip to a much smaller scale.

In the 1980s, personal computers running on the DOS operating system typically had 640k of memory. Over the last 20 odd years, the size of desktops has remained relatively constant, but the power of the CPU (central processing unit) and the size of real memory (e.g. RAM or random access memory) have both increased by a factor of more than 1'000. Imagine this degree of enhancement applied to the size of the machine itself, rather than its power. One could then have at least the power of the old microprocessors in the 1970's in a surface not surpassing one millimetre, i.e. "smart dust".

Technology developers are already working on such particles (known as "motes") and other similar innovations grouped under what have become known as "nanotechnology" (Box 4.2). Universities and research institutes such as the Massachusetts Institute of Technology (MIT) and the University of California at Berkeley (United States) are working on autonomous sensing and communication for devices under a cubic millimetre[67]. Research engineers at the latter institution have recently developed a wireless sensor chip, integrating sensors and transmitters in a mere five square millimetres. The dust, known as "spec" by its creators, represents a milestone in the creation of low-power, low-cost wireless sensor devices, which will eventually be able to self-organize into networks of tiny sensors that can be manipulated remotely[68].

Box 4.2: More than microscopic
Nanotechnology in a "nanoshell"



While many definitions for nanotechnology exist, three elements seem to be common:

- Research and technology development at the atomic, molecular, or macromolecular levels in the length scale of approximately 1 - 100 nanometer range.
- Devices and systems that have novel properties and functionality due to their small size.
- The ability to control or manipulate on the atomic scale.

Though the use of nanotechnology is limited today, nanoparticles are used in a number of industries. Nanoscale materials are employed in electronic, magnetic, optoelectronic, biomedical, pharmaceutical, catalytic, and materials applications. Areas reportedly producing the greatest revenue for nanoparticles are chemical-mechanical polishing, magnetic recording tapes, sunscreens, automotive catalyst supports, bio-labeling, electro-conductive coatings, and optical fibers. Applications that are already on the market include: catalytic converters on cars, burn and wound dressings, water filtration, protective and glare-reducing coatings for eyeglasses and cars, sunscreens and cosmetics, and ink.

The latest display-technology for laptops, cell phones, digital cameras, and other uses is made out of nano-structured polymer films. OLEDs, or organic light emitting diodes will provide brighter images, be of lighter weight, use less power, and secure wider viewing angles than conventional devices.

It is widely acknowledged that high-performance nanotechnology materials will facilitate the production of ever-smaller computers that store vastly greater amounts of information and process data much more rapidly than those available today. Computing elements are expected to be so inexpensive that they can be embedded in fabrics, e.g. for smoke detection.

The impact of nanotechnology on new sensor technology, and therefore on the vision of the ubiquitous network society, is significant. The company NanoMarkets LC predicts that the overall nanotechnology sensor market will generate global revenues of $2.8 billion in 2008 and will reach $17.2 billion by 2012.

Source: Adapted from ITU, "Ubiquitous network technologies and their impact on the traditional telecommunication industry", Thematic Paper, April 2005, available at http://www.itu.int/ubiquitous .

5 IMPLICATIONS OF RFID

A technology such as RFID, the core of the future "Internet of things", has the potential of becoming ubiquitous in every sense of the term, and as such is subject to a number of important public policy challenges. Apart from influencing the shaping of the ICT landscape, it also has significant implications for social constructs and behaviour.

Early signs of how such pervasive technologies might impact society can already be gleaned from the use and social dynamics of the use of mobile phones today[69]. Otherwise said, it may not be too early to draw lessons from a technology such as the mobile phone, widely celebrated for its "ubiquity" and pervasiveness, and apply them to the new and burgeoning are of RFID.

5.1 Public policy challenges

There are three main challenges that policy-makers face with the advent of RFID. From a technical standpoint, the optimal realization of an "Internet of things" hinges upon technical interoperability and the creation of effective global standards. Once this is achieved, the governance of the system must be assured in a balanced and equitable fashion. Finally, one of the most widespread concerns over RFID technology is the control over individual data and the protection of consumer privacy.

5.1.1 Interoperability and standards-setting

Because the implementation of RFID technology can be an expensive investment, issues relating to compatibility and interoperability need to be identified and addressed across sectors and on a global level. However, the industry still lacks common standards for RFID on many fronts, ranging from data formats, to interoperability between RFID readers and tags from different vendors, to interference problems between products. Also, RFID systems used by the retail industry might differ greatly from those used by office access controls. Therefore, cooperation among the various RFID manufacturers will be essential for the promotion and widespread adoption of the technology.

5.1.2 Governance of resources

There is general agreement in many circles that the governance of the global Internet should be multilateral, transparent and democratic. Both the private and public sectors are being called upon for the achievement goals such as the equitable distribution of resources, facilitated access, network stability and security. The need for such governance becomes even more acute as the global Internet expands in content and accessibility, and therefore in strategic commercial importance. Domain names (e.g. companyname.com), for instance, have become more than a simple URL. In fact, they have become powerful marketing tools due to their ability to be easily identified and located with or without search engines.

In this area, VeriSign has somewhat of a monopoly. It manages the core Domain Name Service (DNS) directory that allows users to look up addresses for Web sites that end with ".com" and ".net". This monopoly over digital content has just been expanded as EPCglobal has awarded Verisign the contract to maintain its electronic product codes for RFID item-level tagging, which, as seen above, could eventually identify billions of products (and even people). EPCglobal chose Verisign due to its vast infrastructure. It is of the utmost importance that the current monopoly over the DNS system is not transferred to the future "Internet of Things".

5.1.3 Data protection and consumer privacy[70]

Strong opposition to the widespread deployment of RFID tags has been voiced by a number of consumers and privacy advocates. The main concern is the capacity of RFID to track things and people, and to record a wide array of information. RFID critics argue that stores, corporations and governments could eventually use RFID to spy on individuals[71]. In November 2003, a coalition of advocacy groups (e.g. the Electronic Privacy Information Centre, the Electronic Frontier Foundation, the American Civil Liberties Union) led by CASPIAN (Consumers against Supermarket Privacy Invasion and Numbering) released a "Position statement on the use of RFID on consumer products". This position statement called for a "moratorium" on RFID technology in order for a full assessment of the impact of the technology to be conducted[72].

During 2003, consumer boycotts were subsequently organized against two large companies planning to deploy RFID, Benetton and Gillette. Benetton subsequently cancelled its plans to implement the technology. In 2005, CASPIAN called for yet another worldwide boycott of Tesco after the supermarket giant announced its plans to expand trials of RFID[73]. The group expressed concern that tags may continue to remain active once a product is purchased, and can therefore be scanned through clothing by third-party readers. This would also allow corporations to compile data transmitted by the tags to determine which products a consumer purchases, and when, and even where the product travels. The aggregation of this data could lead to the formulation of sophisticated consumer profiles including their income, health, lifestyle, buying habits and even location. This information could then be sold or made available to government agencies, employers, or other companies for marketing purposes and for use in the context of CRM (customer relationship management) databases [74].

The deployment of RFID tags to track and identify individuals, outlined above, only fuels these concerns. Simson Garfinkel, previously of MIT's Auto-ID Centre, has proposed an "RFID Bill of Rights" a framework for voluntary guidelines that companies deploying RFID could adopt[75]:

- The right to know whether products contain RFID tags.
- The right to have RFID tags removed or deactivated upon purchase of the associated product.
- The right to use RFID-enabled services without RFID tags.
- The right to access an RFID tag's stored data.
- The right to know when, where and why the tags are being read.

More recently, in January 2005, the European Union's Data Protection Working Party (set up under Article 29 of Directive 95/46/EC) published its first assessment report on data protection issues related to RFID[76]. This working document raises concerns about the impact of item-level tagging using RFID on the potential for direct marketing and customer tracking. Applications that link RFID tags with consumer bank accounts were also stated as problematic. The report suggests that consumers should be given adequate tools to delete any information on tags embedded in goods they purchase, or in the alternative, the ability to remove the tags after purchase. For passports and other identification mechanisms, the Working Party advises the use of standard authentication protocols (e.g. ISO) in order to ensure that the data is encrypted and unavailable to those without the requisite authorization.[77] The report identifies three main data protection areas related to the use of RFID.

The first is the use of RFID to collect information linked to personal data. This link might be direct of indirect. A supermarket, for instance, might use RFID to identify consumers by their names and record their habits in the store, including the sections they visit, and the number of times visits occur without purchases. The second is the use of RFID tags for the storage of personal data. A good example of this use is in public transport, where an organization could track the location of an identified individual carrying a contactless public transport card while he/she is within range of their readers. The third and final area is the use of RFID for tracking purposes, without "traditional" identifiers. This includes the following case: if a grocery store hands out re-usable RFID-enabled tokens for shopping carts, it can track the location of the cart as well as the content of the cart, thereby enabling the creation of a detailed database for marketing or dynamic pricing. This information could also be made available to third parties, all without the informed consent of the consumer.

After outlining these three areas of data protection, the report goes on to assess the applicability of European data protection legislation to the information collected through the use of RFID. A request for public comment to the document has been launched, with a deadline for submission of 31 March 2005.

Privacy concerns surrounding RFID deployment are only further exacerbated by the possibility of a "human bar code", or implantable RFID tags for the tracking and monitoring of individual citizens. Far from science fiction, RFID implants have already been used for medical[78] and entertainment uses. For instance, VIP patrons in clubs such as the Baja Beach Club in Barcelona receive access to exclusive lounges and facilitated payment services if they volunteer for the implants (Box 5.1)[79].

Recently, the Food and Drug Administration (FDA) of the United States has even approved and endorsed RFID implants designed by Applied Digital Solutions, and known as "VeriChips", that are injected under the skin. These would contain a unique ID number that would be used to access medical records on a remote server maintained by Applied Digital Solutions[80]. The stated objective of these chips is to provide better health care and reduce medical errors. In some hospitals, projects to tag newborn babies are being implemented[81], and RFID implants have also been used to enhance security at prisons.

The principal concern in the mind of privacy advocates and sociologists is the retention and control of identity by individuals after the implantation of an RFID chip. Some argue that "identity theft" will actually grow in importance rather than diminish. Access to an individual's unique serial numbers and information must be strictly controlled.

With the multiplying population of reading machines (unavoidable in a ubiquitous network environment), and the current rate of technological innovation (likely to increase, if anything), it will become essential to ensure that user data does not fall into the hands of unauthorized parties. Without advocating the need for legislation to curtail the use of RFID at this early stage, the Progressive Policy Institute in its 2004 Policy Report on the subject[82], does acknowledge the need for the industry to take privacy issues into account, notably customer choice and notice. It encourages retailers to take the following steps to ensure the smooth deployment of RFID:

- Label RFID-tagged items with recognizable logos;
- Indicate the location of RFID tags on tagged items;
- Conduct public information campaigns, e.g. through informative flyers or signs clearly indicating the presence of RFID tags in-store.

The Institute also recommends the use of commercial standards by both industry and government.

An RFID Privacy Workshop held at the Massachusetts Institute of Technology (MIT) in November 2003, highlighted the need for an ongoing dialogue about consumer rights and the benefits of RFID. Industry seems aware that sufficient consumer fear and outrage could slow and even thwart the development of the technology. Though some privacy concerns have been exaggerated, protecting consumers from illegitimate tracking was viewed as a legitimate issue that needs to be addressed by researchers and policy makers[83].

Technical countermeasures to block the scanning of radio-frequency ID tags are already in the making. These "jammers", like their mobile phone counterparts[84], respond to privacy concerns about tagged consumer items being tracked within and beyond a retailer's premises. The blocker tag can be placed over a regular RFID tag, and can prevent the reader from scanning information transmitted by the tag. It does this by sending the readers more data than it is capable of reading, i.e. similar to a denial-of-service attack[85].

5.2 Social and human impacts

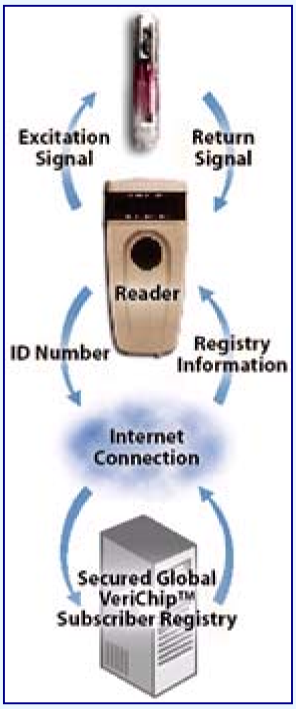
No technological development is possible without effect upon society – desired or undesired. The world as we know it will be transformed by the diversification of RFID use, and its expanded adoption across industries.

As discussed above, RFID can offer levels of convenience (e.g. in the home or in the shop) that are miles ahead of current standards. The technology can facilitate daily tasks and increase the speed of transactions. Individual items, or people, can be located and identified in wide or confined spaces. The mass deployment of RFID is likely to have a significant impact on the quality of life. Like so many other technical innovations, it is yet another extension of the human endeavour to control time and space.

For instance, applications of RFID technology in the health sector will aid in the care of children, the elderly and the infirm. This will not only go a long way towards the prolongation of life, but will make such lives more comfortable and productive. The development of ambient or ubiquitous networking environments (e.g. using RFID) will facilitate the practice of flexible working hours and reduce commuting time. This will in turn have positive spin-off effects on the quality of family life and on the environment.

Indeed, no one can deny that the expansion of these "anywhere, anytime" communication technologies, for "anyone and anything", will bring about increased convenience, greater access and a whole host of innovative applications and services. However, the capacity of these technologies to impact human lives (private and public) will grow correspondingly. This brings to mind the notion of the "Faustian Bargain"[86] in the context of technological change. In other words, while a given technological advance improves many aspects of daily life, it also risks reducing the advantages of earlier technological developments or earlier ways of life. It is only through an increasing awareness of this risk that humanity (and societal progress) can be preserved in what has become an ever-expanding sea of technology and automation.

Box 5.1: Implantable chips make for better bar hopping
RFID has its privileges for VIP patrons of Barcelona's Baja Beach Club



The Baja Beach Club in Barcelona has introduced RFID chips for their VIP patrons. An RFID implant (made by Applied Digital Solutions and known as the "VeriChip"™) injected via syringe allows club-goers to breeze past readers that instantly identify them and their VIP status. The chip contains information about access status and can open exclusive areas of the club for the "chipped" patrons. It also stores credit data, so authorized VIPs may purchase drinks and food by a simple wave of their "chipped" arm. About the size of a grain of rice, each Verichip RFID device contains a unique verification number, allowing access to a database. This database contains persona data relating to the VIP patron.

VeriChip works in the following manner. It is implanted just under the skin (typically in the upper arm) via a syringe. It can then be scanned when necessary with a Verichip™ RFID scanner. A small amount of radio frequency energy passes from the scanner, energizing the dormant chip, which then emits a radio frequency signal. The signal transmits the individual's unique personal verification ID number and provides instant access to the Global Subscriber Registry. This is done via secure, password-protected Internet access. Once data is confirmed by the registry, the appropriate benefits become available to the approved VIPs.

The United States Food and Drug Administration (FDA) recently approved the use of the VeriChip™ for use in hospitals.

Source: Adapted from ITU Internet Reports 2004: The Portable Internet, available at http://www.itu.int/portableinternet.

5.2.1 Society under surveillance?

The more complex and pervasive technological systems become, the more vulnerable they are to misuse and to malfunction. When a technological development is in its early stages, the consideration of possible abuses or undesirable effects is timely and crucial. The ubiquity of networking technologies, combined with the current political climate, raises concerns about citizen surveillance.

Even in the offline world, the monitoring of human behaviour has grown considerably, due largely to the use of credit cards, loyalty cards and cameras. Most citizens of industrialized countries now leave a sizeable trail of electronic data behind them as they go about their daily tasks. In addition, over the last several years, the location and activities of citizens are increasingly captured by the use of video surveillance cameras. According to one estimate, the average person in the United Kingdom is recorded by CCTV (closed circuit television) cameras over 300 times a day[87].

The dawn of the online world has made this type of data collection cheaper and more efficient. The fact that on-line behaviour is tracked by websites is no longer a secret: cookies, which caused uproar several years ago, are now accepted as standard practice. Mobile phone records (calls, messages etc…) are often kept by operators for years, and there is minimal legislation in this domain. Surveillance cameras have become more sophisticated and can now be connected to the World Wide Web, thereby enabling owners to operate them remotely from their personal desktops. In January 2005, it was discovered that simple searches using Google could give anyone (not only camera owners) access to data from over 1'000 unprotected surveillance cameras around the world[88]. Moreover, advances in digitization have meant easier storage and analysis of private and public data.

In this context, the growing adoption of RFID-based services has been a particular source of concern. RFID will make it much easier for companies and government investigators to establish the whereabouts of citizens, by accessing information on tags embedded in their clothing or other personal items. Today, investigators in civil and criminal cases regularly use records from E-Z Pass automatic tolls based on RFID to prove where an individual's car was located at any given time[89]. And it is, in general, possible for companies to use RFID tags to profile their own customers and share this information with governments or other agencies. This has important implications for human rights[90]. The use of such personal information needs to be carefully monitored and ideally limited in scope, as it is fundamental to the notion of human identity – its constitution and its preservation. The mechanism, purpose and extent of identification (be it RFID data, biometric data etc…) must favour the citizen and adhere to principles of transparency and individual choice, thereby thwarting the development of an Orwellian-like[91] landscape of surveillance.[92] However, at this time, attention remains focused on industrial development, rather than the consideration of such issues.

Furthermore, as information and communication technologies become increasingly ubiquitous, they will be able to learn even more about individual citizens, gathering information about their habits, preferences and behavioural patterns. Although the initial purpose of such data collection might be limited in scope, national concerns over security and terrorism (in particular since 11 September 2001), coupled with public acquiescence over time, will lead to the inadvertent surrender of more and more intimate personal information by citizens. Once surrendered, this information may be open to analysis and manipulation by an ever-increasing number of actors and agencies.

Users of today's Internet already complete forms for various services (e.g. news alerts) using false names and addresses. People are increasingly afraid of revealing personal information when online. This climate of distrust may be exacerbated in a future in which all kinds of network appliances or items prompt users for personal identification. If data is constantly exchanged between things and people (in some cases unbeknownst to those affected), who will ultimately retain control over this data? Currently, most users can still choose whether or not to reveal their identity over the Internet. But in the future, tiny devices the size of a grain of sand might give the wind a pair of eyes, or fingerprint-activated doorknobs may recognize owners by a simple touch[93]. If such a future is allowed to come about without the appropriate checks and balances, the flow of personal data will become arbitrary and uncontrolled, thereby increasing the possibility of citizen surveillance.

5.2.2 Individuality, self-fulfilment and self-expression

The impact on the human psyche of any kind of surveillance, real of imaginary, cannot be ignored. If not kept in check, it would breed distrust and fear, creating intense anxiety in the exercising of choice and the taking of decisions, no matter how small. Decision-making is essential to individual self-fulfilment and self-expression, and to societal advancement as a whole. On the other hand, suspicion and paranoia have a negative impact on the growth of healthy social intercourse, as well as creativity and overall human development. In a pervasive environment of surveillance, both the availability and exercise of individual choice may decrease and finally disappear. It is important to remember that improvement is the other name of innovation, and innovation is founded upon choice (e.g. of a technical path) and the making of decisions. With the disappearance of choice, human beings are forever locked in a fixed scenario with no escape. If we have reached where we have today, it is because preceding generations have kept open for us the freedom to choose.

Ubiquitous networks and technologies, such as RFID, are important tools for business and personal life. But tools they must remain, and not pretend to replace the essence of human life[94], such as social interaction, affiliation and the sense of belonging. Of course, the need for belonging and a sense of self are basic constituents of the human condition. In an environment of technological ubiquity, belonging and identity with place (cultural and geographic) is giving way to a sense of belonging to a network - a communications network. This is already the case with mobile phones, which enable users to be contacted regardless of the physical space in which they find themselves[95]. The advent of ubiquitous technologies will enable the construction of a home or office environment anywhere and anytime. The individual, himself or herself, then becomes in a sense the portal. As such, technical devices facilitating this portal have been increasingly seen as the embodiment of the self - pivotal to human identity. Technology is no longer limited to the function of a tool, but begins to reflect identity and inner consciousness.[96] The highly personalized nature of the mobile phone, for instance, is an indication of how the form and use of technology have become important aspects of the individuality and personality of a user[97]. The mobile phone has indeed become the most intimate aspect of a user's personal sphere of objects (e.g. keys, wallet, money etc…) and an object of emotional attachment. This phenomenon will only become more acute as networked technology is more pervasive and is even implanted under human skin (Box 5.1).

Yet, it has to be remembered that such networked devices may enhance and reflect identity, but not replace it. Though technology is playing a greater and greater role in the creation of identity, it ought not be made out to be deterministic of it, as identity stems from a number of non-technical sources, namely culture, education, community, and personality. Moreover, as networks expand and become less visible, the boundaries between real and virtual worlds, real and virtual identity, are blurring. The important distinction between these two spheres must never be lost, either at the individual or at the community level.

Moreover, the creation of a network of smart things will serve to automate daily tasks, even more than is the case today. The full and complete automation of human activity, however, is not necessarily a desirable outcome. Humans are not automats, nor should they ever become so. Each human being, whether or not implanted with an electronic code for location and tracking, is a unique individual and should be seen as such. The increase of surveillance mechanisms discussed above may encourage people to suppress their individuality, as they will prefer not to draw attention to themselves. Society may indeed become more conformist. At the same time, a techno-political environment in which individuals are seen like mere numbers - one in which their uniqueness is not only of little import, but is felt as such - must be discouraged.

5.2.3 Human relationships and intimacy

Technology does not and cannot exist in a vacuum. Neither does the individual, whose need for socialization and social intimacy is fundamental.

Information and communication technology has gone a long way in satisfying the human need for communication. Mobile phones and the Internet have brought people across the globe closer to each other, and enabled more frequent communication between friends, family members, colleagues, and even strangers. In other words, existing social networks have hence been expanded, and new ones created (e.g. through bulletin boards and chat rooms).

However, this also means that human relations are being increasingly mediated by technology. The prodigious use of SMS (short message service), instant messaging and email are important and telling examples. Many young people today prefer to text rather than to talk. Moreover, the rise of communication technologies is eroding the boundaries of private space, accelerating the pace of life and reducing the amount of time available for personal and social development.

But relationships and intimacy remain important human needs. With the growth of technophile populations, the quantity of communication may have increased (e.g. through mobile phones and the Internet) but the qualitative aspect of human relationships may not have been correspondingly improved. In many instances, like the technical devices that facilitate them, these relationships are increasingly transient and ephemeral[98]. Modern information and communication technologies are already being blamed for making users less committal - many send text messages to cancel appointments at the last minute or to avoid awkward face-to-face contact. This phenomenon will only be more apparent as technologies grow and become even more intimate (and invisible) aspects of daily life.

5.2.4 New technologies, new divides

Given the rapid pace of current technological innovation, it is important to ensure that the divide between the technology "haves" and "have-nots" does not widen. The current digital divide is not only comprised of an inequality of access to computers and the Internet; it now includes mobile phones, satellites, and cable services. Far from being a single divide, it is a patchwork of varying levels of access to ICTs, including basic usage and applications development[99].

In fact, it seems that this patchwork is becoming yet more complex. Without careful consideration of the social impact of new technologies such as RFID, we may bear witness in the future to a new kind of divide - a "privacy divide". The current widespread use of loyalty card schemes among retailers is an early and telling example. Customers typically sign up for loyalty cards in order to receive discounts and reductions on various products. For retailers, these cards enable the collection of data about the shopping preferences of their customers. Some retailers, such as Metro AG, are considering the use of RFID in loyalty cards (though this firm subsequently dropped the idea)[100]. The availability of discounted prices for loyalty card holders means that those without loyalty cards pay more at the cash register[101]. The end result is that those that cannot afford goods and services at their full (undiscounted) rate must surrender personal information and thus compromise their privacy.

Indeed, the effective cost of privacy is on the rise. While market forces and technological innovation may be threatening it, an increasing number of tools geared towards its protection are becoming available, e.g. "anonymizers" that enable users to mask their identities while they surf the Internet[102]. The possibility of "purchasing" privacy is a real one[103]. Despite the growing use of technologies that pervade all aspects of human life, privacy should not become a luxury available only to the rich. This holds true both at individual and community level. Though concerns over such issues in industrialized countries have become more frequently raised in recent years, there is little evidence of public concern over privacy in the world's poorer countries, as it rarely figures in the policy agenda of developing and emerging economies.

6 CONCLUSION

RFID technology has tremendous potential to ease life and to improve the human condition. Still, further innovation and industrial deployment of this technology should be done in parallel with a careful exploration of all related aspects. First, in order to avoid market fragmentation and needlessly costly development, there is the need of a concerted effort towards the development of an international standard. Second, the development of RFID should not be the subject of monopolistic commercial development. Third, realization must grow that a fully effective development of RFID is not possible without the consideration of issues related to data protection and consumer privacy. Finally, the ethical and sociological impacts of any innovation are important to consider alongside with economic and technological issues. It is vital to ensure that amidst continuing technological innovation, the essence of our humanity remains untouched. "The tail must not wag the dog" is perhaps a trite saying but applies well to the case of RFID technology and expresses aptly the possible dangers surrounding its use, pitfalls that should be surveyed ahead, and thus avoided.

Endnotes

[1] "The Computer for the 21st Century", Mark Weiser, *Scientific American*, Vol 265., No 3, pages 94-104, September 1991.

[2] See ITU Internet Reports 2004: The Portable Internet, http://www.itu.int/portableinternet/.

[3] See the project website at http://www.itu.int/ubiquitous/. The workshop on "Ubiquitous Network Societies" was organized by the Strategy and Policy Unit of the ITU (see http://www.itu.int/spu/).

[4] "Shrouds of Time: History of RFID", AIM, 2001.

[5] Harry Stockman, *Communication by Means of Reflected Power*, Proceedings of the IRE, pp 1196-1204, October 1948.

[6] "RFID Explained", IDTechEx White Paper, Cambridge, United Kingdom, 2004.

[7] Middleware such as RS 232, RS 485 etc…

[8] Klaus Finkenzeller, "RFID Handbook", 2nd Edition, Wiley and Sons, April 2003.

[9] "RFID: Powering the Supply Chain", Logistics Management, Vol. 43, Issue 8, August 2004.

[10] The Association for Automatic Identification and Mobility (AIM), RFID FAQ, 2004. See the AIM Global website at http://www.aimglobal.org

[11] "RFID and the Internet of Things", Digital ID World, November/December 2003.

[12] "The Internet of Things", The Guardian Unlimited, 9 October 2003.

[13] For example, see "Clubbers at Baja Beach Club in Madrid get chipped with RFID Tags", RFID Gazette, 12 May 2004.

[14] For example, see "Euro notes to get RFID tags from Hitachi?", Silicon.com, 23 May 2003.

[15] For example, see "US Tests E-Passports", RFID Journal, 2 November 2004.

[16] "Demystifying RFID: Principles and Practicalities", White Paper, Steve Hodges and Mark Harrison, Auto-ID Centre, Cambridge, October 2003.

[17] "Understanding RFID: A Practical Guide for Supply Chain Professionals", Tompkins Associates. 2003.

[18] RFID Gazette, 23 July 2004.

[19] "Understanding RFID and Associated Applications", White Paper, Psion Teklogix, May 2004.

[20] See http://www.fcc.gov/oet/info/rules/

[21] See ISO's home page at http://www.iso.org

[22] See ETSI's website at http://www.etsi.org/services_products/freestandard/home.htm

[23] "New ETSI RFID Rules Move Forward", RFID Journal, 9 November 2004.

[24] The ECC was formerly the European Radiocommunication Committee (ERC).

[25] Frost and Sullivan, June 2004.

[26] "RFID Sees All", IEE Review, April 2004, p. 22.

[27] The Yankee Group, 16 September 2004.

[28] See company website at http://www.ti.com/rfid/. Texas Instruments' TI-RFid™ technology is used in a broad range of applications worldwide including access control, automotive, document tracking, livestock, product authentication, retail, sports timing, supply chain, ticketing and wireless payment.

[29] See company website at http://www.alientechnology.com/. Alien Technology was an early member of the Auto ID Center and was involved in creating the recommended specification for Electronic Product Code (EPC) RFID tags and readers

[30] See company website at http://www.semiconductors.philips.com.

[31] See for instance http://www.hitachi.co.jp/Prod/mu-chip/, which describes their "µ-chip".

[32] See company website at http://www.symbol.com/products/rfid/rfid.html.

[33] "Car-tracking RFID tags may enforce Congestion Charge", Silicon.com, 17 August 2004.

[34] Smart Travel News.com, 26 May 2004.

[35] RFID Journal, 24 November 2003.

[36] Texas Instruments, TI-RfidTM Press Release, 15 September 2003.

[37] See *Digital 21 Strategy*, The Government of the Hong Kong Special Administrative Region, at http://www.info.gov.hk/digital21/eng/knowledge/rfid_scm.html

[38] "The EPC Network: Enhancing the Supply Chain" , A Verisign White Paper, 2004.

[39] "Feds approve human RFID implants", The Register, 14 October 2004.

[40] "Moving Beyond the Barcode with RFID", Advance Newsmagazines for Health Information Executives, 2004.

[41] See for instance "Pilot program explores RFID's role in blood transfusion safety ", 11 March 2004, *RF Design: RF and Microwave Technology for Design Engineers*, http://rfdesign.com/news/radio_pilot_program_explores/.

[42] "Japanese company to conduct first medical waste trial using radio frequency identification tags (RFID)", IBM, Pervasive Wireless, 2004.

[43] "Body ID: Barcodes for Cadavers", Wired News, 5 February 2005.

[44] RFID Journal, 10 December 2004

[45] "On Board with RFID", Greenhouse Grower, September 2004, Vol 22, Issue 10.

[46] Mlive.com, 7 October 2004.

[47] "RFID Driver's License Debated", Wired News, 6 October 2004.

[48] See "National ID cards on the way", Zdnet, 14 February 2005.

[49] "U.S. to implant homeless with RFID tags", Thunderbay Indymedia, 3 April 2004, http://thunderbay.indymedia.org/news/2004/04/13189.php

[50] "Euro notes may be radio tagged", Zdnet.co.uk, 22 May 2003. See also "Euro bank notes to embed RFID chips by 2005", EE Times, 19 December 2001.

[51] "American Passports to get Chipped", Wired News, 21 October 2004.

[52] "Publisher Tags All Library Books", RFID Journal, 22 September 2004.

[53] Srivastava, L., "Japan's ubiquitous mobile information society", *INFO*, Vol. 6 No. 4, September 2004.

[54] Texas Instruments, http://www.ti.com/tiris/docs/solutions/ticket.shtml.

[55] RFID Knowledge Base, IDTechEx, at http://www.idtechex.com/knowledgebase/en/casestudy.asp?freefromsection=9

[56] Deloitte, United Kingdom, 2004.

[57] L. Srivastava, "Japan's ubiquitous mobile information society", *INFO*, Vol. 6 No. 4, September 2004.

[58] IDTech Ex, Smart Labels Analyst, November 2004.

[59] See the Centre for Aging Services Technologies (CAST) at http://www.agingtech.org/index.aspx, and RFID Weblog, 16 March 2004, http://rfid.weblogsinc.com/entry/4193323787721756/.

[60] "SkyeTek Shrinks the RFID Reader", RFID Journal, 29 January 2004.

[61] ITU, "Ubiquitous network technologies and their impact on the traditional telecommunication industry", Thematic Paper, ITU New Initiatives Workshop on "Ubiquitous Network Societies", April 2005, available at http://www.itu.int/ubiquitous.

[62] For a discussion of sensors and actuators, see ITU, "Ubiquitous network technologies and their impact on the traditional telecommunication industry", Thematic Paper, ITU New Initiatives Workshop on "Ubiquitous Network Societies", April 2005, available at http://www.itu.int/ubiquitous.

[63] "RFID Gussied up with Biosensors", Wired News, 26 August 2003.

[64] F. Siegemund and C. Florkemeier, "Interaction in Pervasive Computing Settings using Bluetooth-Enabled Active Tags and Passive RFID Tecnology together with Mobile Phones", Proceedings of the First IEEE International Conference on Pervasive Computing and Communications, 2003.

[65] "VeriSign, Nokia Ally To Bring RFID Apps To Consumers", Information Week, 5 November 2004.

[66] See the NFC Forum website at http://www.nfc-forum.org.

[67] See for instance, http://robotics.eecs.berkeley.edu/~pister/SmartDust/.

[68] See http://www.jlhlabs.com/jhill_cs/spec/ for more information. See also "Smart dust gets smaller and more intelligent", Network World Fusion, 24 March 2003 at http://www.nwfusion.com/newsletters/techexec/2004/0607techexec1.html. See also "Researchers Create Wireless Sensor Chip the size of glitter", Space Daily, 9 June 2003.

[69] L. Srivastava, "Mobile phones and the evolution of social behaviour", *Behaviour and Information Technology*, Taylor and Francis, Volume 24, Issue 22, March-April 2005. See also the ITU Workshop on "Shaping the Future Mobile Information Society" (Seoul, Korea, March 2004) at http://www.itu.int/futuremobile.

[70] For a more detailed examination of privacy issues related to ubiquitous information and communication technologies, see one of the other papers prepared for the ITU New Initiatives Workshop on "Ubiquitous Network Societies" (April 2005): ITU, "Privacy and Ubiquitous Network Societies", available at http://www.itu.int/ubiquitous.

[71] J. Hutto and R. D. Atkinson, "Radio Frequency Identification: Little Devices Making Big Waves", Progressive Policy Institute, Policy Report, October 2004.

[72] "Position Statement on the Use of RFID on Consumer Products", CASPIAN, 14 November 2003, http://www.privacyrights.org/ar/RFIDposition.htm. See also the CASPIAN site at http://www.nocards.org.

[73] "Tesco sparks RFID protest", Vnunet.com, 3 February 2005.

[74] "Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology", Report prepared by the Information and Privacy Commissioner for Ontario (Canada), 2004.

[75] "An RFID Bill of Rights", Technology Review, October 2002, http://www.technologyreview.com/articles/garfinkel1002.asp . See also CASPIAN's "RFID Right to Know Act of 2003", available at http://www.nocards.org/rfid/rfidbill.shtml.

[76] Article 29 Data Protection Working Party, "Working Document on data protection issues related to RFID technology", WP105, 10107/05/EN, 19 January 2005. See also http://www.europa.eu.int/comm/privacy.

[77] "The European Union Works out RFID Privacy Legislation", Information Week, 6 February 2005, http://informationweek.com/story/showArticle.jhtml;jsessionid=KNF0DEZP1OAOAQSNDBGCKHSCJUMEKJVN?articleID=59301363&tid=6004

[78] See "The man with the RFID arm", CNET News, 15 February 2005, http://news.com.com/The+man+with+the+RFID+arm/2100-1029_3-5578023.html

[79] See ITU Internet Reports 2004: The Portable Internet, available at http://www.itu.int/portableinternet.

[80] "Feds approve human RFID implants", The Register, 14 October 2004.

[81] For example, Stanford University's Lucile Packard Children's Hospital (LPCH) . See "RFID delivers newborn security", RFID Journal, http://www.rfidjournal.com/article/archive/4/ .

[82] J. Hutto and R. D. Atkinson, "Radio Frequency Identification: Little Devices Making Big Waves", Progressive Policy Institute, Policy Report, October 2004.

[83] S. A. Weis, "RFID Privacy Workshop: Concerns, Consensus and Questions", IEEE Security and Privacy, March/April 2004.

[84] For an article on mobile phone jammers, see for instance "Right to Silence? ", BBC News Online, 13 October 2004, available at http://news.bbc.co.uk/1/hi/magazine/3738652.stm

[85] "Jamming Tags Block RFID Scanners", Wired News, 1 March 2004.

[86] The notion of the "Faustian bargain" of technology was raised by, among others, Neil Postman. See N. Postman, *Technopoly: The Surrender of Culture to Technology*, Vintage Books, New York, 1992.

[87] "No Hiding Place", The Economist, 23 January 2003.

[88] See "Google exposes web surveillance cams", The Register, 8 January 2005, at http://www.theregister.co.uk/2005/01/08/web_surveillance_cams_open_to_all/

[89] See "Watchdogs push for RFID Laws", Wired News, 5 April 2004, at http://www.wired.com/news/privacy/0,1848,62922,00.html?tw=wn_tophead_3

[90] See D. Hurley, "Pole Star: Human Rights in the Information Society", Rights and Democracy (Canada), September 2003, available at http://www.ichrdd.ca/english/commdoc/publications/globalization/wsis/mainWSIS.html

[91] G. Orwell, *1984,* New American Library, New York, 1949, reprinted in 1961.

[92] See "Orwellian Eyes", The Washing Times, 27 November 2003, http://www.washingtontimes.com/functions/print.php?StoryID=20031126-113641-3955r .

[93] "The Surveillance Society", Wired News, December 2001.

[94] M. Friedewald et al., "Perspectives of ambient intelligence in the home environment, *Telematics and Informatics*, Volume 22, August 2005.

[95] L. Srivastava, "Mobile phones and the evolution of social behaviour", *Behaviour and Information Technology*, Taylor and Francis, Volume 24, Issue 22, March-April 2005. See also the ITU Workshop on "Shaping the Future Mobile Information Society" (Seoul, Korea, March 2004) at http://www.itu.int/futuremobile.

[96] As Walter Ong put it, "Technologies are not mere exterior aids but also interior transformations of consciousness". See W. J. Ong, "Writing is a Technology that Restructures Thought," from The Linguistics of Literacy, eds. P. Downing, S. Lima, M. Noonan, Philadelphia, J. Benjamins, 1992.

[97] L. Srivastava, "Mobile phones and the evolution of social behaviour", *Behaviour and Information Technology*, Taylor and Francis, Volume 24, Issue 22, March-April 2005. See also the ITU Workshop on "Shaping the Future Mobile Information Society" (Seoul, Korea, March 2004) at http://www.itu.int/futuremobile.

[98] D. Hurley, "Pole Star: Human Rights in the Information Society", Rights and Democracy (Canada), September 2003, available at http://www.ichrdd.ca/english/commdoc/publications/globalization/wsis/mainWSIS.html

[99] Bridges.org, "Spanning the Digital Divide: Understanding and Tackling the Issues", available at http://www.bridges.org/spanning/summary.html

[100] "Metro store rejects RFID tags in loyalty cards", Computerweekly.com, 3 March 2004, at http://www.computerweekly.com/Article128846.htm.

[101] J. Vaderlippe, "Supermarket Cards: An Overview of the Pricing Issues", CASPIAN, http://www.nocards.org.

[102] See for example the company website of Anonymizer, at http://www.anonymizer.com/.

[103] "The coming privacy divide", CNN.com, 24 February 2000.