Communications of the Association for Information Systems

Volume 18 Article 24

11-6-2006

Wireless Evolution 2006: Cellular TV, Wearable Computing, and RFID

J.P. Shim
Mississippi State University, jshim@cobilan.msstate.edu

Upkar Varshney
Computer Information Systems, Georgia State University, uvarshney@gsu.edu

Sasha Dekleva
DePaul University, sdekleva@condor.depaul.edu

Follow this and additional works at: https://aisel.aisnet.org/cais

Recommended Citation
Shim, J.P.; Varshney, Upkar; and Dekleva, Sasha (2006) "Wireless Evolution 2006: Cellular TV, Wearable Computing, and RFID," *Communications of the Association for Information Systems*: Vol. 18 , Article 24.
DOI: 10.17705/1CAIS.01824
Available at: https://aisel.aisnet.org/cais/vol18/iss1/24

This material is brought to you by the AIS Journals at AIS Electronic Library (AISeL). It has been accepted for inclusion in Communications of the Association for Information Systems by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Communications of the Association for Information Systems

WIRELESS EVOLUTION 2006: CELLULAR TV, WEARABLE COMPUTING, AND RFID

J. P. Shim
Management and Information Systems
Mississippi State University
jshim@cobiLan.msstate.edu

Upkar Varshney
Computer Information Systems
Georgia State University

Sasha Dekleva
School of Accountancy and MIS
DePaul University

ABSTRACT

This paper summarizes the panel discussion at AMCIS 2006 on the evolution and trends in mobile wireless services and technology. The panelists included information systems faculty members from the United States and Mexico. The covered topics included wireless fundamentals, wireless technologies, applications and value chain evolution, wearable computing, wireless mobile issues including privacy and security, issues of worldwide mobile services and trends, and social implications. The panelists believe that there has been a virtual explosion in the ubiquitous and embedded computing industry over the past decade. Computing technology is moving beyond personal computers and is progressing into devices with embedded technology. The trend of mobile wireless technologies is moving to one single device rather than multiple devices. A single device could contain any or all of the following components, such as cellular phone, digital camera, video recording, MP3, mobile cellular TV services including digital multimedia broadcasting (DMB) and digital video broadcasting, handheld (DVB-H). Also, wearable computing such as watches, smart shirt and clothing, body sensors, and health monitoring devices are in the nascent stages. Wireless technology known as radio frequency identification (RFID) is used to identify objects, including living creatures. Various RFID applications including item tagging and electronic passports prompted valid loss of privacy concerns and triggered intense and sometimes irrational public discussion.

Keywords: mobile wireless, cellular TV, wireless networks, 4G networks, wearable computing, cellular, privacy protection, RFID, issues in m-commerce

I. INTRODUCTION

Starting in 2003, AMCIS included an annual panel session to bring together academicians and practitioners with expertise in wireless and mobile communications. The panels focused on cutting edge mobile and wireless issues and trends. Themes have included mobile commerce and services, wireless information systems, cellular and mobile TV phone services, WiMAX and WiBro technologies, wearable computing and devices, privacy issues of wireless network technologies and RFID, and the future of wireless services. This report consists of four sections:

Following this Introduction, Section II discusses wireless mobile services and cellular TV. Section III discusses evolution of wireless networks, as well as wearable computing and devices. Section IV discusses the privacy issues of RFID. Appendix I lists the panelists.

II. WIRELESS MOBILE SERVICES AND CELLULAR TV

We observed rapid development of wireless network technologies with great interest and expect their continued expansion. While 3G and 3.5G mobile networks in 2006 offer broadband transmission with speeds of up to 2 Mbps (or even 10 Mbps) in most developed areas of the world, other countries lag behind with only "kbps" speed for their users. The 3G and 3.5G wireless access systems provide data services along with voice and messaging capabilities. Some features of 3G services (using CDMA 2000 and WCDMA standards) and 3.5G (using HSDPA upgrade) include 3D games, video-conferencing, full motion videos, and high-speed Internet access on roaming mobile phones. At this time, telecommunication vendors and service providers are collaborating to develop a true broadband wireless cellular system, also known as 4G, using orthogonal frequency division multiplexing (OFDM) (a transmission modulation technique), multiple input multiple output (MIMO) technology (which refers to the communication using dual-array multiple-antenna systems), and other emerging and advanced wireless transmission technologies. Figure 1 presents the evolution of broadcasting technologies, focusing on the use of such technologies rather than the technological development itself. The evolution of broadcasting technologies over the years illustrates the progress of digitization and platform convergence in the communications sector (DVB, 2005).

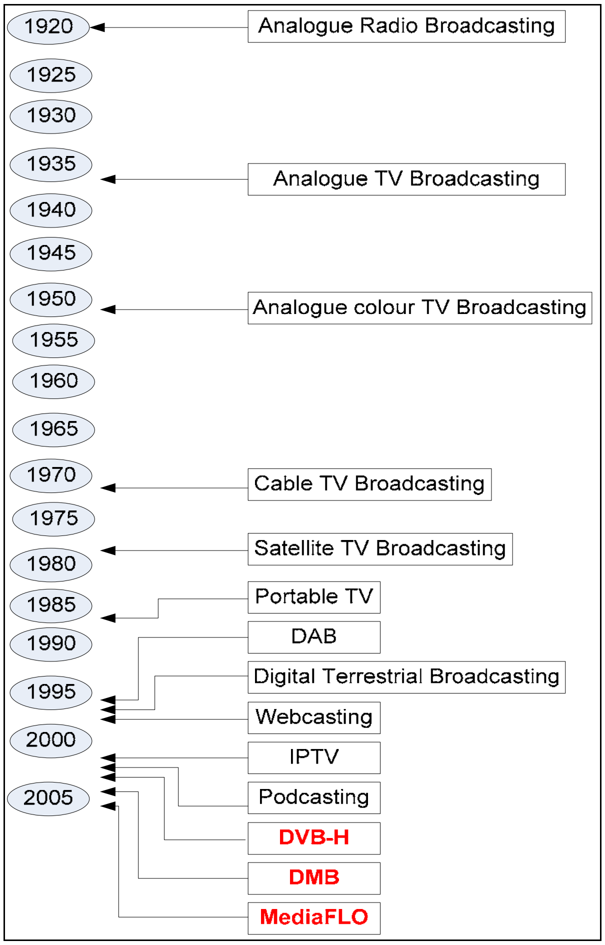


Figure 1. Evolution of Broadcasting Technologies (Source: Shim et al., 2006b)

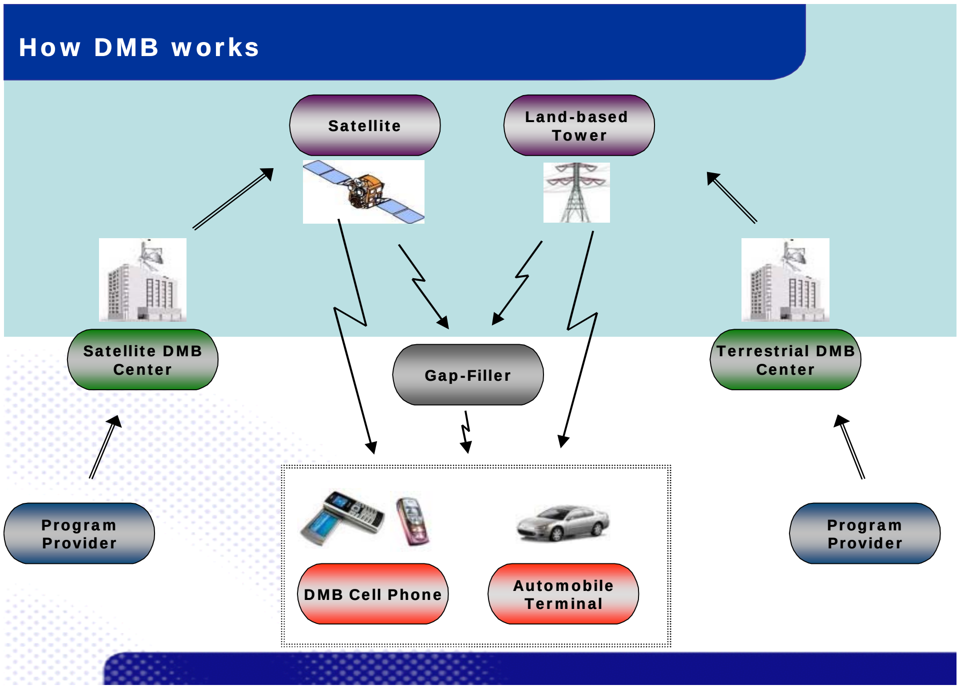


Figure 2. Satellite and Terrestrial DMB

Based on Figure 1 in (Shim, 2005a; Shim et al., 2006)

Asian countries, such as Japan and Korea, once lagged behind the West in information technology (Budde, 2002). Despite their late entry into the wireless market, Asian wireless operators, with supportive government policies, propelled themselves forward to become global leaders with the implementation of the 3G or 3.5G technologies. NTT DoCoMo, a primary Japanese 3G carrier, rolled out 3G services in Japan on October 1, 2001. However, three South Korean operators implemented 3G networks even earlier. Both KTF and LG Telecom implemented CDMA 2000 1X on May 1, 2001, while SK Telecom implemented CDMA 2000 1X even earlier, on October 1, 2000 (3gToday, 2006). Mobile handsets have since evolved into a universal remote control that has been integrated into daily lifestyles. Mobile phone applications vary from accessing educational tutors to controlling residential appliances to leisure and entertainment (Lewis, 2004). Currently, Korea is the leading digital mobile TV market, especially with its own standard, digital multimedia broadcasting (DMB). As of July 2005, DMB has been approved by WorldDAB as a standard. Driven by user demand and the changes in the culture of technological usage, Korean DMB market will be important for validation of new DMB technologies.

Satellite and terrestrial DMB systems provide content such as video, CD-quality audio and data through hand-held devices and vehicle-mounted terminals to the users-on-the-move (RoK MIC, 2005). A schematic depiction of digital television transmission standards in Figure 2 provides a basic explanation of satellite and terrestrial DMB. Competing technologies include digital video broadcasting handheld (DVB-H) and QUALCOMM’s technology called MediaFLO. MediaFLO USA Inc., a wholly owned subsidiary of QUALCOMM, has announced its plans to rollout commercial operation at the end of 2006. Table 1 lists digital TV transmission standards, characteristics/features, and modulation.

Table 1. Digital Television Transmission Standards

Standards	Region	CHARACTERISTICS/FEATURES	Modulation
DMB: Based on Eureka 147 DAB	Korea	• European broadcasters can add video at little extra cost • Rapid implementation • Frees up telecom pipelines for higher-margin data services (video phone calls) • Consumes too much power	COFDM
DVB-H: Based on DVB-T	Europe	• "Time slicing" technology: short high-bandwidth bursts rather than constant low bit rate streaming • Reduces power consumption and saves battery life • Requires allocation of new frequencies • More expensive investment • Dependence on separate networks: over-the-air and 3G	COFDM
ISDB-T	Japan	• Lower power consumption • Operates on unused TV channels • Provides SFN (single frequency network) and on-channel repeater technology	OFDM
MediaFLO	USA	• Power efficiency, superior mobility, maximum spectral efficiency • Channel change delays are unacceptable	OFDM

Source: (Shim, 2005b; Shim et al., 2006)

Cellular TV services, such as DMB or DVB-H, will be attractive to users, since the service costs will be much lower than the cost for high data rates of 3G cellular services. The telephone industry players started to push a broad range of multimedia services to their customers. This technology provides audio, video, messaging, and high graphical content for customers. Table 2 lists the strengths and weaknesses for the three standards: DVB-H, DMB, and MediaFLO (QUALCOMM Inc., 2005).

As mentioned earlier, Korea's introduction of DMB has marked a milestone in the world of mobile TV technology. On December 1, 2005, terrestrial DMB (T-DMB) service was launched in Korea. Satellite DMB (S-DMB), T-DMB's rival technology, began its service seven months earlier, on May 2005 (Shim et al., 2006a). Figure 2 above shows the operation of both S-DMB and T-DMB. As of August 2006, Korea had about 2 million DMB subscribers, which demonstrates its popularity and potential to attract more users in a short period of time and expand further (Cho, 2006). Rising popularity of cellular TV among users in Korea suggests that the trend of combining multiple devices into one will likely expand to other countries. Cellular TV, such as DMB, has a potential to greatly impact us as our personalized digital tool.

Table 2. Strengths and Weaknesses of Mobile TV Standard

Standard	Strengths	Weaknesses
DVB-H	• The market is not highly fragmented; • Pilot projects in Australia, UK, Finland, and many other countries have been successful; • The battery consumption by DVB-H is much less than DVB-T.	• New market and more competitors • financial loss or slowing of revenues; • In UK, the frequency is occupied and will not be released for some time and it leads to a lesser reception for customers.
DMB	• Based on the Eureka 147 DAB standard; • Due to T-DMB's basis through DAB, much of T-DMB's infrastructure and required spectrum is in place; • Both satellite (S-DMB) and terrestrial service (T-DMB); • Service is already provided to customers via various portable devices, while the other two competitive technologies each have only one type of terminal.	• It is not quite as established or widely deployed as DVB-H.
MediaFLO	• Power efficiency (less power consumption); • Faster access programming (channel switching time); • Low network deployment costs (less towers); • Superior mobile reception; • High capacity = More channels.	• No support outside USA; • QUALCOMM's spectrum is not available; • No permission to deploy MediaFLO in USA.

Actual DMB usage statistics released by TU-Media (an S-DMB service provider) show that users in their late 20s through 50s represent a large percentage of DMB service viewers. They favor soap operas on TV, sports, and music program contents (Suh, 2005). Several reasons explain why most of the younger consumers in Korea are not currently subscribed to S-DMB and have lower inclination to subscribe (Shim, 2006):

1. S-DMB handsets, with a retail price range of $600-$800, are expensive;
2. The teens in Korea lack the extra out-of-pocket money to pay for the S-DMB $13 service monthly fee (and $20 activation fee);
3. To the parents, purchasing a DMB handset for their children's TV watching and gaming does not seem justified.

Additionally, most school-age children have no time to watch DMB programs due to an overloaded academic schedule or time conflicts. However, the actual usage results among various demographic groups for T-DMB services, once released, are expected to differ from those of S-DMB because T-DMB services are offered for free.

The cellular mobile service industry has many complex issues, which span across logistical, social, cultural, and technical issues. These challenges call for cooperation among the cellular and network service providers, service developers, and handset makers. These stakeholders also need to collaborate with the government and consumers. If successful, their efforts will foster growth in the wireless mobile telecommunications industry.

III. EVOLUTION OF WIRELESS NETWORKS & WEARABLE COMPUTING AND DEVICES

The current limitations of wireless and mobile networks are:

- spotty coverage,
- low and variable bit-rate,
- unpredictable quality of service,
- lack of inter-operability and inter-working,
- limited battery power,
- lack of personalization, and
- a lack of universal location management across multiple networks and carriers.

Different vendors, who sell mobile and wireless networks, are addressing many of these challenges. However, both technical as well as business-related obstacles exist, as many carriers shy away from investing heavily in the existing infrastructure. The carriers are concerned about the risks involved in the changing nature of business and technology and provide additional services on top of the basic voice-oriented wireless service.

The emerging Fourth Generation (4G) wireless networks could address some of these problems. The 4G networks will likely enable roaming across heterogeneous and packet-switched wireless networks. These networks will provide IP interoperability and higher speeds. The 4G networks are scheduled for deployment between 2008 and 2010. Other functionalities of 4G networks are listed below and discussed in the following paragraphs.

- Multi-network access & roaming
- User-centric and highly personalized services (Varshney and Vetter, 2002)
- Support for group-oriented services (Varshney, 2002)
- Higher bit-rates (Varshney, 2003a)
- More advanced physical layer definition
- Highly energy-efficient transmission
- Context and location awareness (Varshney, 2003b)
- Pervasive and ubiquitous coverage (Lyytinen et al., 2004)
- Fully integrated access
- End-to-end security
- New ways of charging batteries
- Support for transactions
- Programmable, intelligent and human-aware devices

The 4G networks will offer user-centric and highly personalized services by utilizing user preferences and history (Figure 3). This feature will require storing and updating user preferences, interests, and history of actions (Varshney and Vetter, 2002). The 4G networks will likely offer considerably higher bit rates than most users need. This requirement could result in even over-provisioning where more than enough resources are allocated for guaranteed quality even when traffic and user requirements go up significantly in a short-period of time. It may also be possible to have one wireless network for every family where the network moves with the user by means of infrastructure in vehicles, watches, and entertainment devices.

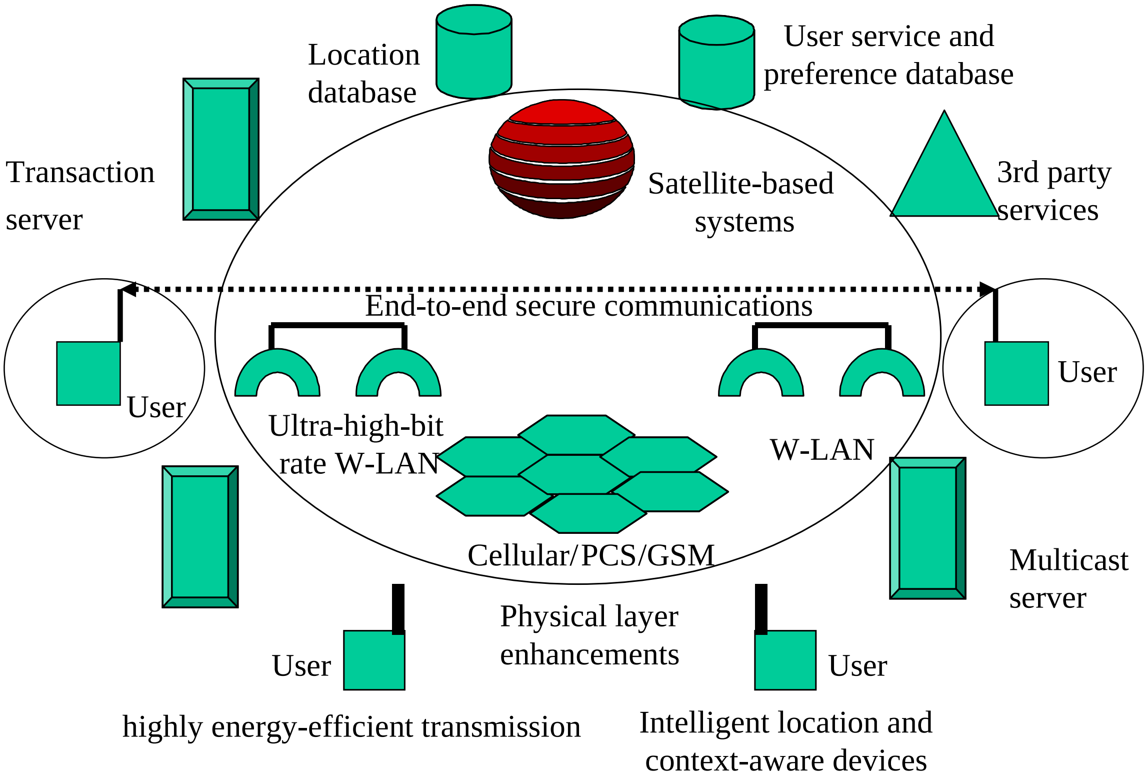


Figure 3. Multiple Functionalities of 4G Environment

Dynamic spectrum management, tunable devices, and many newer and more advanced physical layer transmissions (OFDM and MIMO) and technologies such as Ultra Wide Band (UWB) will likely help to overcome the bandwidth and resources limitations.

Very highly energy-efficient transmission will likely become possible, so that most users will not need to worry all the time about battery power and charging. Analysts anticipate many new ways of transmitting wireless information and new ways of charging batteries (e.g., solar, human, and transmission from other users). The devices will find ways and avenues of charging without user intervention.

We expect that the 4G networks will offer context-aware and location-based wireless services. These improvements can facilitate higher productivity and highly sophisticated location-related services. People will not be interrupted unless the context level of incoming events exceeds the context level of existing events.

Hand-held devices will probably become increasingly sophisticated, programmable, intelligent, and human-aware. A large amount of user information including healthcare and financial information will be stored and updated in hand-held devices. For many mobile services, the support for transactions would be provided by the 4G networks. The end-to-end security needed for many transactions and business applications will also be seamlessly provided in the 4G environment.

WEARABLE COMPUTING

Wearable computers are one part of the big vision of “Pervasive Computing”, where people will have access to computing anywhere anytime. Wearable computing can support this by embedding computers in many daily-life components such as clothing, glasses, caps, headwear, shoes, and other wearable objects. In future, a new generation of computers will become available that are designed as clothing items.

Wearable computers will be designed to provide portability during operation, where people will access computing and communications functionality without being burdened by the weight and shape of computing devices. These devices will provide hands-free or virtually hands-free use, where people will be able to perform other tasks without being burdened by the need to hold or carry computers in their hands. The wearable computers will run continuously allowing the users to access them as and when necessary without a significant access delay. The wearable computers will attempt to sense the user’s current context and will thus help him/her in performing the task effectively.

The goal of wearable computing is an interface ideal for a continuously worn, intelligent assistant that augments memory, intellect, communication, and abilities (Starner, 2001). The style of interface is the focus of wearable computing, as opposed to the manifestation in hardware as shown in media and other outlets (Starner, 2001). A general figure of wearable computing future is shown in Figure 4. The major challenges in wearable computers relate to:

- power requirements,
- network resources,
- privacy concerns, and
- the design of innovative interfaces.

A wearable computer can be a single worn device or a group of devices spread over the human body. This potential distribution of subsystems over the body could lead to very complicated power use and distribution. This distribution involves both how power is generated and dissipated by wearable computers. The wearable computers can have their batteries charged when a user is sleeping, eating, or driving. Alternatively, the human body could act as both a charger (source) for these devices as well as an end medium for heat absorption (sink).

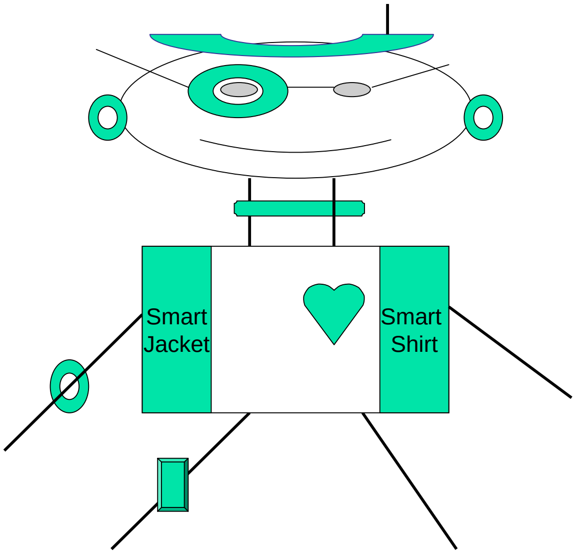


Figure 4. A Wearable Computing Future

The networking challenges in wearable computers are very complex as both intra-body and inter-body communications may be supported in addition to communications to other networks. The intra-body communications can be supported by creating Body Area Networks (BANs) where individual subsystems on the human body can act as networking devices (such as routers). Depending on the frequency used, line of sight issues may have to be addressed. From a topology point of view, a wearable computing device in the center of the human body can act as a switch or router, and thus can minimize the power requirement for BANs. The inter-body communications to another similarly equipped human (with wearable devices) can be direct point-to-point or assisted by other humans (ad hoc networking) or could go through another wireless network covering both the source and destination humans.

Wearable computing generates a significant level of privacy concerns. Wearable computers could store a large amount of “intimate” information on users, thus creating privacy challenges. Hackers may find it very attractive to collect private information about everyone who passes by certain places in a city. In some cases, privacy may also be compromised by employers or co-workers. With wearable computers, a user should be informed what personal information is collected while passing by or accessing a certain network service. This would allow a user to make a benefit-loss tradeoff before allowing a location- or service-based function. In some cases, especially medical or emergency situations, privacy violations could be considered desirable (and thus even be encouraged).

Interface refers to the numerous fields that address human and computer interaction (Starner, 2001). These fields include human-computer interfaces, human factors, ergonomics, industrial design, and fashion. In the future, wearable computing can be implemented as a cross-section of multiple domains of engineering, design, and fashion. Also, the peripheral interfaces should be designed to make simple things simple and complex things possible (Starner, 2001).

THE FUTURE IMPACT OF WEARABLE COMPUTING

Wearable computing will impact personalization, healthcare applications, military applications, and the fashion industry.

Personalization

The use of multiple wearable computers on humans will lead to an unprecedented level of personalization. Both the physical closeness of computing devices and their abilities to sense the current context and user’s intent can lead to highly effective user-centric applications and service. This will also help users complete many tasks more effectively while avoiding many unnecessary, previously attempted, and unsuccessful tasks. The near-integration of significant computing and storage functions of wearable computers with high levels of human cognitive abilities can create wonders.

Healthcare Applications

Another major impact area of wearable computing will be in healthcare areas such as assisted living, patient monitoring, and telemedicine. Some of these applications are already in clinical trials of LifeShirt (http://www.vivometrics.com). It is a lightweight shirt weighting only 8 ounces, designed for human use, and it is machine washable. The sensors embedded in the shirt are arranged around the chest and abdomen. The sensors allow for a single channel electrocardiogram for heart rate and a three-axis accelerometer for patient posture and activity. Several additional peripheral devices can also be added for blood pressure, blood oxygen saturation, electroencephalography, periodic leg movement, body temperature, skin temperature, and cough. LifeShirt Recorder in a PDA continuously encrypts and stores the patient's physiologic data. Digital Patient Diary allows patients to record time and date-stamped symptom, mood, and activity information in the recorder's digital diary.

Military Communications

Another major area of impact of wearable computing will be in military communications, and more specifically in deriving survival status and location tracking. Smart-Shirt (http://www.gtwm.gatech.edu/gtwm.html) is designed with multiple fibers and the continuity of these fibers is a sign that a soldier wearing the Smart-Shirt is doing fine. In case of a gunshot wound, one or more fibers would be broken, and the interruption of light traveling through the broken fiber will be used to detect the status of the soldier.

Fashion Industry

The use of wearable computing in clothing could spawn another fashion industry of “Smart&Cute” clothing. Just like NTT DoCoMo’s iMode phones became a major social statement for many teenagers in Japan, such clothing may become a mainstream fashion and not just a passing fad. These (tailor-made) clothes can be designed to fit humans better than existing mass-produced clothes where one size supposedly fits all. Imagine a future where you don’t throw old clothes away, but just upgrade or “re-fiberize” them as needed.

Wearable computing will be a major component in the implementation of ubiquitous and pervasive computing. Eventually, human brains and computing machines will be coupled together very tightly, and the resulting partnership will be able to think better than humans alone, as well as process the amount of data at a speed not approached by computing machines today. Multiple devices on user’s body can form BAN using short range wireless networks. Wearable computers will provide augmented reality systems where information will be overlaid on the physical world, such as x-ray results on an actual patient during surgery.

IV. RFID AND PRIVACY

This section will briefly introduce Radio Frequency Identification (RFID) technology and a selection of typical early applications. An explanation of reasons for privacy protection concerns and a few hypothetical ways for compromising it are presented next. Such valid concerns have, however, been misunderstood, over-hyped, and resulted in paranoia and public protests and outcry. Finally, two of the more controversial applications of RFID – the Electronic Product Code (EPC) for item tagging to optimize supply chain and retail management and electronic passports – are discussed in more detail.

STRUCTURE OF AN RFID SYSTEM

As noted in Figure 5, the elements of a complete RFID system are a tag with its antenna and a reader with its own antenna. A reader is typically connected to a computer, which is normally further connected to a network. A reader communicates with tags through radio waves used not just to transfer data, but may also transfer energy and synchronization and other control signals. Tags may be passive, active, or semi-passive. Passive tags do not have their own energy source and are powered by the radio signals emitted by the reader. This mode of operation limits the communication range to several feet, but their operational life may extend into decades. Active tags contain batteries and may continuously broadcast their messages or wait for the signal from the reader before they start transmitting.

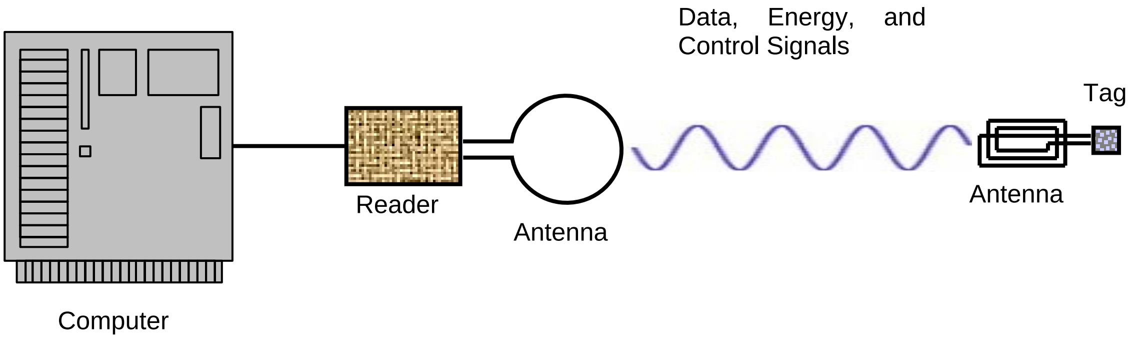


Figure 5. Structure of an RFID System

Semi-passive tags have their own energy source but use it just to maintain the sensor-generated data in their internal memory while they still depend on energy emitted by the reader to communicate with the reader. Other important physical characteristics of RFID systems are operational frequencies and tag capabilities. Radio frequencies, normally within a wide scope from 135 kHz to 5.8 GHz, influence range, penetration, and other qualities of radio signals. Finally, tags can be simple and inexpensive with limited processing capabilities and memory, which can only be written in once; or, they can be sophisticated micro-controllers with mesh networking and processing capabilities, various built-in sensors and larger memory, which can be written to and updated.

A PLETHORA OF RFID APPLICATIONS

Some of the most widely discussed RFID applications are those in transportation and distribution, aviation, healthcare, security and access control, and retail. With appropriate placement of tags and readers, containers and pallets can be tracked as they progress through the supply chain. Also in transportation, many passenger tickets all over the world contain imbedded RFID tags as do millions of car keys. In the aviation industry, numerous expensive replacement parts are tagged to improve the maintenance parts inventory management. Airport administrators also consider RFID tags as luggage tags to improve baggage handling, and even for boarding passes which would enable airlines to locate late passengers at the airports. In healthcare, administrators consider RFID tags for various applications from tagging the surgical equipment to avoid leaving something inside the patient after surgery, to tagging patients using bracelets or even implants to prevent treatment errors, to the supervision of movements of Alzheimer patients, and the quick retrieval of medical records in emergencies. The pharmaceutical industry is promoting the use of tags to prevent the distribution of counterfeit drugs.

Many employee identification cards contain RFID tags used for access control to restricted areas, such as those for the World Summit on Information Society and for a congress of the Chinese communist party. The security program of the Canadian Air Transport Security Authority (CATSA) uses smart cards equipped with RFID first deployed in March 2004. Similarly, the Rikkyo Primary School in Tokyo carried out a trial of active RFID tags in September 2004 in order to monitor the movements of its students in real-time (WSIS, 2005). The U.S. and other governments are just starting to issue e-Passports containing RFID tags. Some privacy groups and general public deem this controversial, and so have triggered vivid discussions. The same kind of public reaction accompanied the introduction of RFID technology in retail environments. Widely reported accounts of Wal-Mart’s request that its 100 largest suppliers start tagging pallets and boxes by the beginning of 2005, for example, set off public protests. Both RFID applications in passports and retail environments will be discussed in more detail below following a general discussion of privacy implications.

PRIVACY IMPLICATIONS

The general ability to read an RFID tag inconspicuously from a distance causes a lot of valid concerns. According to one report (EPCglobal, 2004), three of the main data protection implications are collection of personal information, storing personal data on tags, and tracking of individuals. In the following scenarios, these three implications appear in combination.

Even when an RFID tag does not contain any personal information, its unique number can, in some cases, be linked to personal data. One example would be loyalty cards with imbedded tags distributed by a chain of grocery stores. Signing up for such a program may require consumers to be identified by name, address, and so on. Even if that were not the case, executing a payment with a credit or debit card would identify the consumer, enabling the grocer to forever associate a unique tag number with a particular individual. With appropriate placement of readers throughout the store, individual buying patterns and shopping behavior could be tracked, analyzed, and possibly sold to third parties. The store could make inferred assumptions about shopper’s income, health, lifestyle, and buying habits. Many shoppers would likely consider this an unacceptable invasion of privacy.

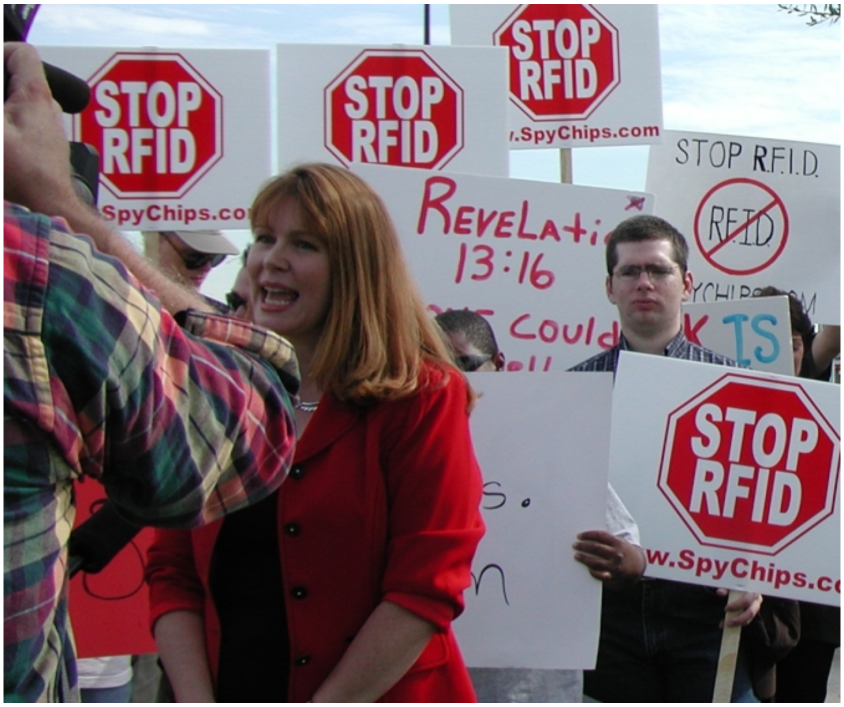
A scenario involving more than one store becomes even more interesting. Assume that an individual walks into a second store carrying a shopping bag with tagged items bought in a first store. Those tags could be read and recorded in the second store’s database. The same consumer walks into the second store a few days later, a tag with the same tag number may be recognized because it is attached to, say, a purse, enabling the second store to associate the unique RFID tag number with a particular individual and use it as a personal identification number.

The assumption that various objects would be tagged and would contain information revealing the nature of these objects does not seem stretched too far. For example, researchers considered embedding RFID tags in banknotes. A hidden RFID reader would be able to detect such banknotes as well as books, medicines, or valuable objects carried by a passerby. The knowledge of this information by unrecognized and unauthorized parties invades the privacy of the person carrying the tagged objects. An even more striking intrusion would appear when personal information is stored in the tags, as is the case in electronic passports. In general, however, privacy could be compromised not only by an individual being identified by an RFID reading, but by being identifiable by association of such reading with other information, such as information from loyalty or credit cards.

HYPE AND MISINFORMATION

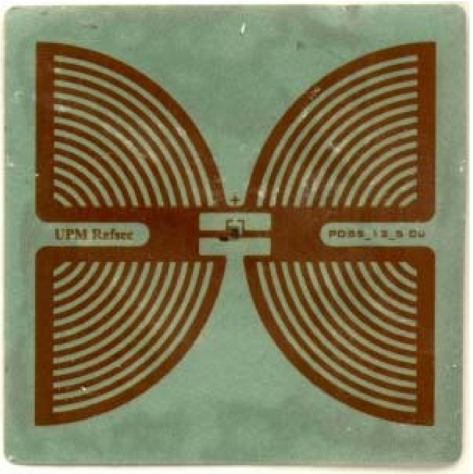
Although the concerns about the loss of privacy are generally valid, many are overstated and clearly unrealistic, such as beliefs that Big Brother would be able to read RFID tags and recognize belongings and track individuals’ every move using satellites. This led Mike Liard, principal RFID analyst for ABI Research, to state at the U.S. Senate RFID Caucus (Trebilcock, 2006a): “The key takeaway is there’s been a lot of hype and misinformation around RFID technology, especially when it comes to privacy issues.” Senator Byron Dorgan (D-N.D.) agrees (Trebilcock, 2006b): “The first priority is education. You have to understand it.”

Misinformation is abundant. For example, one Web page proclaims (Szymanski, 2006): “Plans to Microchip every Newborn in U.S. and Europe Underway,” and further clarifies: “Technology exists to create a totalitarian New World Order and sinister plans to use it on innocent public being covered up by U.S. policy makers.” This particular news was posted all over the Web. The publication of the infamous book *Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID* (Albrecht and McIntyre, 2005) and its follow-up *The Spychips Threat: Why Christians Should Resist RFID and Electronic Surveillance* (Albrecht and McIntyre, 2006), helped to steer public concerns about this technology. Albrecht holds a Doctorate in Education from Harvard University and is the director of Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), an organization she founded in 1999. A charismatic speaker and privacy advocate, Albrecht was featured on mainstream TV (Figure 6), radio and print media including CNN, NPR, the CBS Evening News, *Business Week*, and the *London Times*. Yet, the CASPIAN's Web site (CASPIAN, 2006) prominently presents misinformation such as the following: "RFID chips, tiny tracking devices the size of a grain of dust, can be used to secretly identify you and the things you're carrying – right through your clothes, wallet, backpack, or purse." Albrecht organized public protests in Europe and the United States. Figure 7 shows the RFID tag affixed to a Hewlett-Packard printer purchased at a Texas Wal-Mart store that sparked the protest. An objective observer would likely say, "So what?" to this find.



Copyright CASPIAN, used by permission

Figure 6. Ms. Albrecht Being Interviewed



Copyright Liz McIntyre, used by permission

Figure 7. RFID Tag That Sparked the Protests

For better or for worse, the general public and many technology analysts are deeply concerned. For example, during an open comment period initiated by the U.S. State Department, the public overwhelmingly rejected the notion of RFID in passports. Of 2,335 comments received on the plan to introduce the electronic passports, 2,019 residents listed security and privacy as their top concern (DoS, 2005). We will discuss the electronic passports in some detail below.

In general, many of the privacy concerns are exaggerated. Data stored on the passive tags can be legally accessed by a reader positioned only a few inches or at most a few feet away, depending on the design. However, the perpetrators may not care to conform to the government-imposed restrictions on radio power limits and be thus able to read the tags from longer distances. Laboratory experiments proved that unencrypted data stored in passive RFID tags can be read from far longer than nominal ranges. There are multiple reports of such experiments. In one case, using a rogue device built from widely available components costing about $100 in total, powered by a 12V battery, and conforming to a popular ISO-14443 standard, the reading range was extended to five times the nominal range, allowing the perpetrator to skim a tag from a distance that does not require the attacker to touch the victim (Kirschenbaum and Wool, 2006). Similarly, as a proof of concept, data from an RFID tag were successfully retrieved by passing a legitimate key owner in a parking lot and then used for unauthorized building access (Newitz, 2006). A group of hackers at the 2005 DefCon technology convention in Las Vegas, Nevada, used an antenna attached to an RFID reader to scan the information on a tag nearly 70 feet away (Sieberg, 2006). RFID proponents downplayed the demonstration, saying the apparatus was impractical and wouldn't work if the information on the RFID tag were encrypted. However, the government testers found that some readers were able to read the information on RFID chips considered for electronic passports from a distance of up to 30 feet (Calabrese, 2004). All of these and many other reports suggest that we need to pay attention to the ways this technology is being implemented. To make sure that privacy will not be compromised, we need to implement security technologies such as encryption, authentication, metallic protectors, tag disabling, and so on. Fortunately, privacy concerns were very much on the minds of pioneering EPC designers from the beginning (Sarma, 2006). In addition, passive tags today have poor communications performance for an antagonist seeking to invade one's privacy. The cell phone in a pocket and the toll pass in a car offer better opportunities to invade privacy (Sarma, 2006).

Yet, as Ashton writes (2005): "Once … dramatic exaggerations are excluded, we are left with some important, serious, and reasonable questions. How can we know when and how RFID is being used? How can we make sure it is not misused? How can we exercise choice over how it affects us personally? How do we ensure that it is safe?"

Besides implanting RFID tags in humans, tagging individual products and imbedding them into passports spur the most controversy. We will next focus on the electronic product code technology and finally on electronic passports.

ELECTRONIC PRODUCT CODE

Based on the idea of creating "an Internet of things," perhaps including living beings, a more modest goal of tracking objects along the supply chain drove several individuals and teams at MIT in the 1990s (Sarma, 2006). In 1999, these efforts led to the launch of the Auto-ID Center at MIT under the sponsorship of the Uniform Code Council, Gillette, and Procter and Gamble (Sarma, 2006). This effort eventually led to the definition of international standards for object tagging. In early 2002, MIT generously donated all intellectual property rights in the interest of society and the world to a not-for-profit entity named EPCglobal, a joint venture of the Uniform Code Council (UCC), which administered the Universal Product Code (UPC) bar code in the U.S., and EAN International, which did the same for the rest of the world. A global organization dedicated to the design and implementation of global standards and solutions to improve the efficiency of supply chains named GS1 was formed later as the UCC and the Canadian ECCC joined EAN International.

One of the major drivers in the standard development at Auto-ID Center was to minimize the cost of product tags, which required simplification of communication protocols and limited the processing capabilities and memory capacity. The other driver from the very outset of the project was the concern about privacy protection. The result of the first driver and in support of the second, the standard defines tags as passive with short reading range and being able to store only a unique number for each object. This means that the tag carries no information about the item's owner and not even about the item itself. To simplify the processing, this unique identification number is not encrypted. The structure of the number named Electronic Product Code (EPC) has four fields:

- Version number (a.k.a. Header)
- Manufacturer number (EPC Manager)
- Product number (Object Class)
- Serial number

So far, a number of variants of this structure have been defined, but they are all either 64 bits or 96 bits in length. Figure 7 shows the EPCglobal UHF 96 bit data format with a sample data presented in hexadecimal notation for brevity. Manufacturer number is assigned by the EPCglobal and the Product number and Serial number are assigned by the manufacturer.

No descriptive information, such as object name, production and expiration date, weight, size, and so on, is stored on the EPC tags. An effective supply chain management application would certainly need such information. In fact, the EPC is only one element of a comprehensive system known as EPCglobal Network. Beside EPC numbers, the network consists of EPC tags and EPC readers, EPC middleware, Discovery Services, and EPC Information Services (EPC IS). The middleware is used to manage real-time events, such as a tag being recognized by a certain reader, and to communicate read information to EPC IS and a company's other information systems. The designers of Discovery Services used the Internet and its Domain Name System as a model. The Discovery Services enable users to find data about a specific EPC and to request access to the particular database storing that data. Typically, each manufacturer will maintain a database with information about its tagged products, and each such database will be a component of the global distributed EPC database. The Object Naming Service, another component of Discovery Services, is a mechanism that leverages a Domain Name System-like facility to discover information about a product and related services from the EPC. Finally, the EPC IS enables users to exchange EPC-related data with authorized trading partners through the EPCglobal Network.

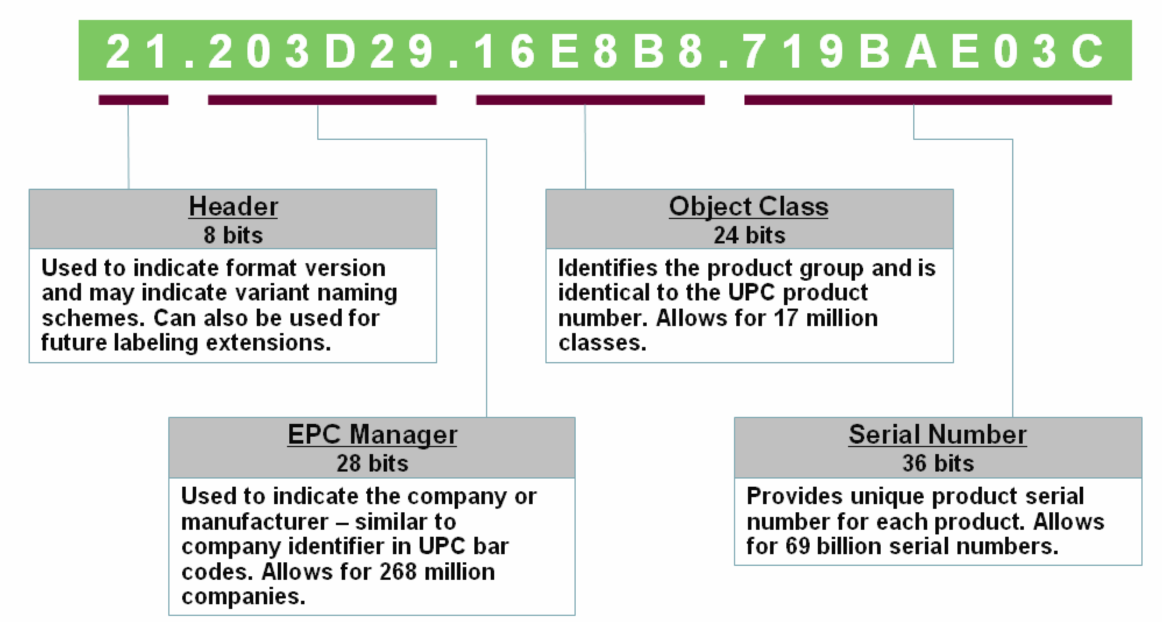

21.203D29.16E8B8.719BAE03C
Header
8 bits
Used to indicate format version and may indicate variant naming schemes. Can also be used for future labeling extensions.
Object Class
24 bits
Identifies the product group and is identical to the UPC product number. Allows for 17 million classes.
EPC Manager
28 bits
Used to indicate the company or manufacturer – similar to company identifier in UPC bar codes. Allows for 268 million companies.
Serial Number
36 bits
Provides unique product serial number for each product. Allows for 69 billion serial numbers.

Figure 7. EPCglobal UHF 96 bit data format

Adapted from [RFID Edge, 2006]

Privacy concerns related to EPC tags are somewhat mitigated because the tags do not contain any other data, but a unique item number and because of the rather short reading range. In addition, the RFID standards developers have designed a function known as the kill switch or the kill command, which permanently disables the EPC tag and could be used, for example, at the point of sale. It has been endorsed by EPCglobal. Its specification states that a password will be used to prevent unauthorized tag disabling. However, in some cases permanent tag disabling is not desired, such as for “receipt-less” item returns, “smart” RFID-enabled appliances, in rental and borrowing applications, and so on. Several proposed alternatives are considered, such as blocker tags, which, when present, would “spam” any reader attempting to scan tags without the right authorization. Another alternative is recoding, in which case a tag is overwritten with a new ID number when it changes hands. Researchers have also noticed that using the signal-to-noise ratio of the transmissions they receive, RFID tags would be able to estimate their distance from the reader. Since short distance implies trust, this may serve as a privacy protection improvement. IBM researchers proposed a design with perforated tag where partially destructible RFID antenna can be removed by a consumer after purchase (Datamonitor, 2005). This would limit the scanning range from a few meters to just centimeters.

In conclusion, consumer privacy is protected by a number of measures integrated into the ERP standards for item tagging. The privacy concern has been recognized as a hot button issue from the very beginning and continues to be studied. We must pay attention to the way the technology will be implemented, but we should not overreact and panic. It is comfortable to realize that technology vendors can use a number of measures to protect consumer privacy. We need to make sure that such measures will be implemented.

ELECTRONIC PASSPORTS

Passports have to be globally interoperable, and it is interesting to observe how in cases of different technologies particular bodies and associations emerge and assume the role of standard bearers. In case of the so-called Machine Readable Travel Documents (MRTD), the International Civil Aviation Organization (ICAO), an agency of the United Nations, developed the standard, which also applies to electronic passports. It was accepted on July 11, 2005 (ICAO, 2005). The ICAO decided on RFID technology conforming to ISO standard 14443 to improve the security of travel documents and to promote border crossing efficiency. In compliance to this standard, the so-called ePassports are being currently implemented in 30 countries including the United States. After the U.S. Department of State issued its Final Rule on October 25, 2005, the pilot program was rolled out for U.S. diplomats in December 2005, and the distribution to the general public started in Denver in August 2006. The rollout of this project covered the whole country by the end of October 2006.

The ICAO standard defines the reading range (of up to 10 cm) and the structure of data stored on the passive RFID chip. The standard does not prescribe the chip’s memory capacity, but recommends that the adopting countries implement as high a capacity as they possibly can that is operationally feasible and practical, with an absolute minimum of 32 kilobytes (KB), or, even better, 64 KB (ICAO TAG, 2004). This would enable the storage of not only a compressed facial image, but optionally also fingerprints and iris scans. The U.S. Department of State is implementing chips with memory capacity of 72 KB and is initially storing only the data visually presented on the data page of the passport, including the name, nationality, sex, date of birth, place of birth, and digitized photograph of the passport holder; as well as, data about the passport itself such as the passport number, issue date, expiration date, and type of passport. The chip will not contain home address, social security number, or other information that might facilitate identity theft. Unused space could be used in the future for additional biometric information.

After publishing the proposed rule on February 18, 2005, the Department of State received 2,335 comments on the introduction of the ePassport (DoS, 2005). Comments opposing the proposed rule mostly focused on privacy protection and security. Based on feedback, additional security and privacy features were integrated into the final rule. They include anti-skimming material in the front cover and spine of the passport, so that passive RFID tag content can only be accessed when the passport is open. In addition, the Basic Access Control (BAC) protocol will further mitigate any potential threat of skimming. The BAC utilizes a form of Personal Identification Number (PIN), which is automatically derived from the printed characters in the second line of data on the Machine-Readable Zone, visible on the passport data page. The PIN must be physically read to unlock the data on the chip and is used to encrypt the data communicated between the chip and the reader to make eavesdropping ineffective. The measures also include the use of a form of Public Key Infrastructure (PKI), so the issuing states and their offices will be able to use digital signatures to protect the data stored on the chip from tampering and passports from being falsified.

The Department of State believes that the measures described in the rule adequately address the concerns raised by comments regarding security and privacy, but not everybody agrees. Kevin Ashton, the co-founder of MIT's Auto ID-Labs, said (Ferguson, 2006): “The idea of storing all this sensitive data (in passports) is horrible. You can take the chip off one passport and stick it on another. No one will know the difference." He added: “My big issue is it is truly a stupid idea to store any information on an RFID tag other than a unique number. Otherwise there is always the risk of data change." Bruce Schneier, a well-known security technologist and author, said during a May 26 interview with *eWeek* that eavesdropping will only get easier. Although he acknowledged: “Shielding is good. Basic Access Control is good. Putting a switch would be great," his opinion nevertheless is that (Ferguson, 2006): “… if you don't have RFID you don't need any of this. I haven't seen any compelling reasons why we are doing this. If we (the government) did it out in the open then everyone would scream." The controversy thus continues, but there are compelling reasons for using RFID technology in passports as the U.S., and essentially all other governments from 180 countries participating in the ICAO see them.

V. CONCLUSION

Although this paper focuses on three specific new developments in the domain of wireless communications, it exemplifies the breath of applications and the speed of technological evolution. One gets an impression that this breathtaking progress is driven by engineering and scientific progress rather than proven market demand. In other words, we seem to observe technology in search for applications. For example, the premise that people – at least in the U.S. – are eager to watch TV programming on their cell phones has not been proven. The ESPN just recently discontinued such service (AP, 2006). Similarly, wearable computing can implement the vision of Pervasive Computing by embedding computers in wearable clothing or computers designed as wearable items. Many identified applications of wearable computing in healthcare, military, and fashion industries make sense, but we may be surprised as anticipated drivers fail and unforeseen employments become great successes. We also seem to be only at the pioneering stage in the evolution of wireless machine-to-machine communications including the RFID technologies, in which case the fear of privacy loss is real. However, legal, technical, industry agreements, and other measures can and should be introduced to mitigate concerns. We have embarked on an interesting, largely unpredictable, technology driven, and most exciting journey.

REFERENCES

EDITOR’S NOTE: The following reference list contains the address of World Wide webpages. Readers, who have the ability to access the web directly from their computer or are reading the paper on the web, can gain direct access to these references. Readers are warned, however, that

1. these links existed as of the date of publication but are not guaranteed to be working thereafter.

2. the contents of webpages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.

3. the authors of the webpages, not CAIS, are responsible for the accuracy of their content.

4. the author of this article, not CAIS, is responsible for the accuracy of the URL and version information.

3gToday (2006) “3G Operators”, http://www.3gtoday.com (current Sep. 10, 2006).

Albrecht, K. and L. McIntyre (2005) Spychips: *How Major Corporations and Government Plan to Track Your Every Move with RFID*, Nashville, TN: Nelson Current.

Albrecht, K. and L. McIntyre (2006) *The Spychips Threat: Why Christians Should Resist RFID and Electronic Surveillance,* Nashville, TN: Nelson Current.

AP (2006) “ESPN pulls plug on cell phone operation,” *Associated Press*, Oct. 1, http://www.msnbc.msn.com/id/15045069/ (current Nov. 15, 2006).

Ashton, K. (2005) “Foreword,” in *RFID: applications, security, and privacy*, Garfinkel, S. and B. Rosenberg (ed.), Upper Saddle River, NJ: Pearson Education, p. xxii.

Budde, P. (2002) “Asia and Australia Telecommunications Industry Overview”, in *Annual Review of Communications*, Vol. 55, pp. 243-250.

Calabrese, C. (2004) “ACLU Testimony On Computer Chips In Virginia Drivers Licenses,” American Civil Liberties Union, Oct. 6, http://www.aclu.org/privacy/gen/15770leg20041006.html (current Sep. 1, 2006).

CASPIAN (2006) “Is Big Brother in your grocery cart?” htpp://www.nocards.org (current Aug. 28, 2006).

Cho, J. (2006) “DMB Users Need Upgrade or No Reception,” *The Korea Times*, Aug. 13.

Datamonitor (2005) “IBM promises privacy with retail RFID tag,” *Datamonitor NewsWire*, Nov. 7.

DoS (2005) “Electronic Passport,” Department of State, Federal Register, 70(205), pp. 61553-61555, October 5, http://docket.access.gpo.gov/2005/05-21284.htm (current Aug. 30, 2006).

DVB (2005) Digital Video Broadcasting, http://www.dvb.org/ (current Oct 20, 2005).

EPCglobal (2004) “The EPCglobal Network,” Sep. 24, http://www.epcglobalinc.org/news/EPCglobal_Network_Overview_10072004.pdf (current Aug. 18, 2006).

Ferguson (2006) “Report: DHS Should Soothe RFID Passport Fears,” *eWeek.com*, July 25, http://ww.eweek.com/article2/0,1759,1994188,00.asp (current Sep. 9, 2006).

ICAO (2005) Machine Readable Travel Documents home page, http://www.icao.int/mrtd/Home/Index.cfm (current Aug. 18, 2006).

ICAO TAG (2004) “Biometrics Deployment of Machine Readable Travel Documents,” ICAO Technical Advisory Group, May 21, http://www.icao.int/mrtd/download/documents/Biometrics deployment of Machine Readable Travel Documents 2004.pdf (current Sep. 9, 2006).

Kirschenbaum, I. and A. Wool (2006) “How to Build a Low-Cost, Extended-Range RFID Skimmer,” May 8, http://www.eng.tau.ac.il/~yash/kw-usenix06/index.html (current Sep. 1, 2006).

Lewis, P. (2004) “Broadband Wonderland,” *Fortune*, Sep. 20, pp. 191-198.

Lyytinen, K., Y. Yoo, U. Varshney, M. Ackerman, G. Davis, M. Avital, D. Robey, S. Sawyer, and C. Sorensen (2004) "Surfing the Next Wave: Design and Implementation Challenges of Ubiquitous Computing", *Communications of the AIS*, 13, pp. 697-716.

Newitz, A. (2006) "The RFID Hacking Underground," *Wired*, 14(05), May, http://www.wired.com/wired/archive/14.05/rfid.html (current Aug. 31, 2006).

QUALCOMM Incorporated (2005), *MediaFLO: FLO Technology Brief*, www.qualcomm.com/mediaflo

Republic of Korea MIC (2005) "U-Korea: Humanism in the Digital World IT 839 Strategy," book-let released by the Republic of Korea, Ministry of Information and Communication, http://www.mic.go.kr/board/etc/spam_count/it839_down.jsp (current Sep. 17, 2006).

RFID Edge (2006) "RFID Mandates and Standards," PowerPoint presentation, http://www.scansource.com/rfidedge/files/Mandates_Standards_Update.pps (current Oct. 15, 2006).

Sarma, S. (2006) "A History of the EPC," in *RFID: applications, security, and privacy*, Garfinkel, S. and B. Rosenberg (ed.), Upper Saddle River, NJ: Pearson Education,.

Shim, J.P. (2005a) "Korea's Lead in Mobile Cellular and DMB Phone Services," *Communications of the AIS*, 15, pp. 555-566.

Shim J.P. (2005b) "Empirical Findings on Perceived Use of Digital Multimedia Broadcasting Cellular Phone Services," *Proceedings of EXPO Comm Wireless Conference*, Seoul, May 18, pp.113-131.

Shim, J.P. (2006) "Empirical Findings on the Usage of Digital Multimedia Broadcasting (DMB) Cellular Phone: Revisited," *Proceedings of IEEE Broadcast Technology Society (BTS)*, Las Vegas, April 6.

Shim, J.P., K. Ahn, and J. Shim (2006) "Empirical Findings on the Perceived Use of Digital Multimedia Broadcasting Mobile Phone Services," *Industrial Management & Data Systems*, 106(2), pp. 155-171.

Shim, J. P., K. Ahn, J. Shim, and S. Park (2006) "Perceived Use of DMB Cellular Phone," *IEEE Broadcast Technology Society Newsletter*, (14)1, pp. 13-14.

Sieberg, D. (2006) "Is RFID tracking you?" *CNN.com*, Aug. 25, http://www.cnn.com/2006/TECH/07/10/rfid/index.html (current Sep. 1, 2006).

Starner, T. (2001) "The Challenges of Wearable Computing," *IEEE Micro*, 21(4), pp. 54-67.

Suh, Y. (2005) "Mobile Broadcasting Market and S-DMB," TU Media President's Report, TU Media Corp, Korea.

Szymanski, G. (2006) "Plans To Microchip Every Newborn In U.S. And Europe Underway, According To Former Chief Medical Officer of Finland," *Arctic Beacon*, May 11, http://www.arcticbeacon.com/11-May-2006.html (current Aug. 20, 2006).

Trebilcock, B. (2006a) "RFID goes to Washington," *Modern Materials Handling,* July 25, http://www.mmh.com/article/CA6355944.html (current Aug. 19, 2006).

Trebilcock, B. (2006b) "Q&A with Byron Dorgan, RFID's proponent in the Senate," *Modern Materials Handling*, July 25, http://www.mmh.com/article/CA6355948.html (current Aug. 19, 2006).

Varshney, U. and R. Vetter (2002) “Framework, Applications, and Networking Support for M-commerce”, *ACM/Kluwer Journal on Mobile Networks and Applications (MONET)*, 7(3), pp. 185-198.

Varshney, U. (2002), “Multicast over Wireless Networks”, *Communications of the ACM*, 45(12), pp. 31-37.

Varshney, U. (2003a) “The Status and Future of 802.11-based WLANs,” *Computer*, 36(6), pp.102-105.

Varshney, U. (2003b) "Location Management for Mobile Commerce Applications in Wireless Internet”, *ACM Transactions on Internet Technologies*, 3(3), pp. 236-255.

WSIS (2005) “The Brave New World of Smart Technologies,” Newsroom: World Summit on the Information Society, http://www.itu.int/wsis/tunis/newsroom/background/smart-technologies.html (current Sep. 16, 2006).

LIST OF ACRONYMS

3G	Third Generation
3.5G	Third-and-a-Half Generation
4G	Fourth Generation
BAC	Basic Access Control
BAN	Body Area Network
CASPIAN	Consumers Against Supermarket Privacy Invasion and Numbering
CATSA	Canadian Air Transport Security Authority
CDMA	Code Division Multiple Access
COFDM	Coded Orthogonal Frequency Division Multiplexing
DMB	Digital Multimedia Broadcasting
DVB-H	Digital Video Broadcasting – Handheld
EPC	Electronic Product Code
HSDPA	High-Speed Downlink Packet Access
ICAO	International Civil Aviation Organization
IP	Internet Protocol
IS	Information Services
ISO	International Organization for Standardization
MIMO	Multiple Input Multiple Output
MIT	Massachusetts Institute of Technology
MRTD	Machine Readable Travel Documents
OFDM	Orthogonal Frequency Division Multiplexing
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RFID	Radio Frequency Identification
S-DMB	Satellite Digital Multimedia Broadcasting
T-DMB	Terrestrial Digital Multimedia Broadcasting
TV	Television
UCC	Uniform Code Council
UHF	Ultra High Frequency
UPC	Universal Product Code
UWB	Ultra Wide Band
WCDMA	Wideband Code Division Multiple Access
WiBro	Wireless Broadband
WiMAX	Worldwide Interoperability for Microwave Access

APPENDIX I. PANELISTS AND TOPICS

Topic: Mobile Wireless Services and Technologies in Ubiquitous and Embedded Computing: Trends[1]

Panelists:	J. P. Shim, Professor at Mississippi State University
	Upkar Varshney, Associate Professor at Georgia State University
	Sasha Dekleva, Associate Professor at DePaul University
	Ante Salcedo, Professor at ITAM, Mexico
	Robert Nickerson, Professor at San Francisco State University

ABOUT THE AUTHORS

J. P. Shim is Professor of BIS at Mississippi State University. He received a PhD from University of Nebraska and completed Harvard Business School's Executive Education Program. He has taught IS at Georgia State University, New York University, and, while on sabbatical, at the Chinese University of Hong Kong. He serves on SE, AE, and editorial boards for IS journals. He is serving on Wireless Telecommunication Symposium as program chair and fellow. Professor Shim has received various awards, grants, and distinctions, including NSF, Microsoft, and Mississippi IHL. He is an eight time recipient of outstanding faculty award, John Grisham Excellence award, and Ralph E. Powe Research award. He has written over 150 research papers. Recently, he has served as a program chair for US-Japan e-business conference sponsored by NSF, and as a keynote speaker at international ubiquitous and embedded conference. He has lectured in the USA, UK, France, Greece, Korea, Kuwait, Hong Kong, Taiwan, Japan, Jamaica, and China.

Upkar Varshney is Associate Professor of CIS at Georgia State University. He received a B.E. in Electrical Engineering with Honors from University of Roorkee, MS in Computer Science, and Ph.D. in Telecommunications and Networking from the University of Missouri-Kansas City. He has written over 100 journal and conference papers on m-commerce, pervasive healthcare, and wireless networking. Several of his papers are among the most cited in mobile commerce, including Mobile Networks and Applications (MONET)'s most viewed paper (2005) and the most downloaded ACM transactions paper (2004). He has delivered several keynote speeches, tutorials and workshops. Dr. Upkar received the Myrone T. Greene Outstanding Teaching Award (2000 and 2004), and RCB College Distinguished Teaching Award (2002). He is or has been an editor/member of editorial board for *IEEE Computer, Decision Support Systems, International Journal of Network Management, IJWMC, CAIS, and IJMC,* and has guest edited major journals including *ACM/Kluwer Mobile Networks and Applications*.

Sasha Dekleva is an Associate Professor at the College of Commerce, DePaul University in Chicago. He has over ten years of industrial experience in engineering, systems analysis, and management at IBM and other companies in Slovenia. Besides being on faculty at DePaul University since 1985, he has taught at the Universities of Iowa, Maribor, and Ljubljana. His papers appeared in journals such as *MIS Quarterly, Information Systems Research, Communications of the ACM, Data Base, Information & Management, Journal of Software Maintenance, Journal of Systems and Software* and many others. His current research interests include wireless communication technologies and applications, IT management, and valuation of IT investments.

[1] The authors gratefully acknowledge Professors Robert Nickerson and Ante Salcedo, and the panel audience for their helpful comments at the panel session. The authors also acknowledge CAIS Editor-in-Chief for his constructive and helpful comments on an earlier draft of this paper.

Copyright © 2006 by the Association for Information Systems. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and full citation on the first page. Copyright for components of this work owned by others than the Association for Information Systems must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, or to redistribute to lists requires prior specific permission and/or fee. Request permission to publish from: AIS Administrative Office, P.O. Box 2712 Atlanta, GA, 30301-2712 Attn: Reprints or via e-mail from ais@aisnet.org

.

Communications of the Association for Information Systems

ISSN: 1529-3181

EDITOR-IN-CHIEF
Joey F. George
Florida State University

AIS SENIOR EDITORIAL BOARD

Jane Webster Vice President Publications Queen's University	Joey F. George Editor, CAIS Florida State University	Kalle Lyytinen Editor, JAIS Case Western Reserve University
Edward A. Stohr Editor-at-Large Stevens Inst. of Technology	Blake Ives Editor, Electronic Publications University of Houston	Paul Gray Founding Editor, CAIS Claremont Graduate University

CAIS ADVISORY BOARD

Gordon Davis University of Minnesota	Ken Kraemer Univ. of Calif. at Irvine	M. Lynne Markus Bentley College	Richard Mason Southern Methodist Univ.
Jay Nunamaker University of Arizona	Henk Sol Delft University	Ralph Sprague University of Hawaii	Hugh J. Watson University of Georgia

CAIS SENIOR EDITORS

Steve Alter U. of San Francisco	Jane Fedorowicz Bentley College	Chris Holland Manchester Bus. School	Jerry Luftman Stevens Inst. of Tech.

CAIS EDITORIAL BOARD

Erran Carmel American University	Fred Davis Uof Arkansas, Fayetteville	Gurpreet Dhillon Virginia Commonwealth U	Evan Duggan U of Alabama
Ali Farhoomand University of Hong Kong	Robert L. Glass Computing Trends	Sy Goodman Ga. Inst. of Technology	Ake Gronlund University of Umea
Ruth Guthrie California State Univ.	Alan Hevner Univ. of South Florida	Juhani Iivari Univ. of Oulu	K.D. Joshi Washington St Univ.
Michel Kalika U. of Paris Dauphine	Jae-Nam Lee Korea University	Claudia Loebbecke University of Cologne	Sal March Vanderbilt University
Don McCubbrey University of Denver	Michael Myers University of Auckland	Fred Niederman St. Louis University	Shan Ling Pan Natl. U. of Singapore
Dan Power University of No. Iowa	Kelley Rainer Auburn University	Paul Tallon Boston College	Thompson Teo Natl. U. of Singapore
Craig Tyran W Washington Univ.	Upkar Varshney Georgia State Univ.	Chelley Vician Michigan Tech Univ.	Doug Vogel City Univ. of Hong Kong
Rolf Wigand U. Arkansas, Little Rock	Vance Wilson U. Wisconsin, Milwaukee	Peter Wolcott U. of Nebraska-Omaha	Ping Zhang Syracuse University

DEPARTMENTS

Global Diffusion of the Internet. Editors: Peter Wolcott and Sy Goodman	Information Technology and Systems. Editors: Alan Hevner and Sal March
Papers in French Editor: Michel Kalika	Information Systems and Healthcare Editor: Vance Wilson

ADMINISTRATIVE PERSONNEL

Eph McLean AIS, Executive Director Georgia State University	Reagan Ramsower Publisher, CAIS Baylor University	Chris Furner CAIS Managing Editor Florida State Univ.	Cheri Paradice CAIS Copyeditor Tallahassee, FL