



## **FOCUS GROUP MEETING ON Embedded Systems & Ambient Intelligence**

### **FG ORGANIZATION**

**Infonomics & New Media Research Centre  
Zuyd University, The Netherlands**

### **DATE**

**31th Octobre 2008**

### **PLACE**

**European Journalism Centre, Maastricht, The Netherlands**

### **PARTICIPATING PROJECT PARTNERS**

**CSSC, CESAGEN, OPTEL**

## **Digital Identities in Embedded Systems and Ambient Intelligence**

Octobre 31<sup>th</sup>, 2008

11.00 – 15.00

Venue : European Journalism Centre,  
Avenue Ceramique 50  
Maastricht, The Netherlands.  
Tel +31 +43 3254030

### Directions and practical information:

Ms. Marina Beckers [marina.beckers@hszuyd.nl](mailto:marina.beckers@hszuyd.nl)

Tel +31 +45 4000540 On the meeting day: +31 +613492737

### Scientific organisation:

Ms. Irma van der Ploeg [i.vdploeg@hszuyd.nl](mailto:i.vdploeg@hszuyd.nl)

Tel +31 +45 4000522

## **Agenda**

10.45-11.15 Reception and Coffee

11.15 -11.30 Welcome and Introduction

*Dr. Irma van der Ploeg*

Focus Group on Digital Identities in Embedded Systems and Ambient Intelligence

11.30 – 11.45 Introduction to the HIDE project

*Dr. Emilio Mordini*

11.45 -12.30 Expert Presentations

11.45 -12.15: *Dr. Dimitrios Tzovaras*, Informatics and Telematics Institute,  
Thessaloniki Greece, Project coordinator ACTIBIO.

12.15 -12-45: *Dr. Ruud van Munster*, Senior Consultant Biometrics and  
Surveillance, TNO Science and Industry, Delft, The Netherlands.

12.45-13.00 : Q&A

13.00-13.45 Lunch at the EJC

13.45 – 14.00 Introduction Focal Issues

Presentation of the key questions put up for discussion in the afternoon session

14.00-15.30 Round Table Discussion

*Chair Dr. Irma van der Ploeg*

15.30 – 15.45 Preliminary Conclusions

*Dr. Emilio Mordini*

15.45 – 16.00 Further planning FGs, question round for suggestions, wrap up.

*Dr. Irma van der Ploeg*

## **1 Introduction to the topic**

One of the most influential developments in ICT in the near future is generally thought to be the shift away of computing power from PCs and desktop-configurations to the physical environment. Embedded software, ubiquitous computing, ambient technology, smart objects, and the emergence of 'the Internet of Things' are all terms denoting a particular aspect or view of this near future.

Due to developments in a.o. radio frequency identification (RFID), miniaturisation, wireless, sensor and networking technologies, people will be moving through and interacting with their physical environment in new ways. Objects themselves will interact and communicate, and send information about themselves, their users, or their environments to electronic networks and databases.

Already our daily lives are organised through a myriad of electronic passage points, negotiated through an increasing number of electronic identifiers, code words, pass words, PIN numbers, user names, access controls, electronic cards or biometric scans. Some are highly visible and negotiated willingly (e.g., a PIN credit card purchase), others are more covert (e.g., a speed camera on a motorway), others are embedded (e.g., GPS technology in mobile phones).

On the positive side, huge gains in convenience, efficiency, and safety are predicted to result from this; on a more bleak view, this could mean the ultimate track- and traceability and loss of privacy. In particular, and most relevant to the HIDE project, the information on peoples' behaviors generated by these systems, will, in all probability, prove an invaluable and highly tempting resource for law enforcement and crime prevention and security policy, which, if so used, entails a post-hoc blanket recasting of end-users, consumers, and citizens as suspects, which may render them vulnerable in unforeseen ways.

In particular, problems can be expected to surface wherever detection technologies involve the collection or processing of personal data ("any information relating to an identified or identifiable natural person"). Insofar as their use is governed by Community law, it will be regulated by the "Data Protection Directive", which states that no data collection ought to go unnoticed by the data subject (art.7 par.1) . Yet this is exactly what embedded technologies to some extent are geared to preclude. Moreover, there is an exception to this rule, where art.7 par.2 states that par. 1 does not apply in case of "processing of data relating to offences, criminal convictions or security measures". Yet is it legitimate to extend the concept of "security measures" to any technology used in any context? The growing proliferation of embedded technologies, the emergence of an "Internet of things", cannot be conceptualised as the never-ending growing of an indistinct "security area".

## **2 Relevance to HIDE**

The Hide project is concerned with the ethical and social aspects of biometrics and other ICT-based personal identification technologies, in particular their use for security and law enforcement purposes

Many, if not most, of the envisaged and currently developed or already deployed AmI systems, for example, are 'user centric' and comprise personalised functionality. This means that people's interactions with such systems require

them to be identified within the system, in order to enable it to retrieve the relevant personal profile and settings.

Moreover, for it to work effectively, ambient intelligence requires intuitive and convenient interfaces, meaning that identification and authentication are usually (half-) automated and as unobtrusive as possible, with little conscious effort needed from the user. This requirement makes identification technologies like biometrics and RFID likely options in this context, but also puts such systems on a direct collision course with the data protection principle that personal data collection must always involve an aware and informed data subject (EU Data Protection Directive, art.7 par.1)

In addition to identification/authentication to access or activate the system, continued interaction or mere contact with the system generally results in registration of personal identifiers, data on movements, behavior, location, etcetera, communicated to, and stored in central databases. These personal data may be required for the improvement of the systems performance (by updating and perfecting the personal profile) but may, obviously, be used for other purposes.

National security, law enforcement and crime prevention interests in particular are highly likely to make authorities seek access to, for example, data collected through systems for mobility and traffic management, such as payment systems for public transport, toll collection, road pricing and so on.

Thus the technological developments in this domain are highly relevant to HIDE's overall aims and subject matter, and positively requiring the project to address, analyse and assess them extensively. Main instrument in this particular task will be one of four focus groups, each of which is devoted to specific technological developments.

### **3 Aim of the Focus Group**

WP 2 of the project aims at **Critical Issue Identification** within specific areas of technological development. This task will be approached through a series of technology orientated focus groups exploring ethical and social issues in relation to particular (sets of) technologies. The four technological areas are:

- Technology Convergence
- System Interoperability
- Privacy Enhancing Technologies
- **Embedded Systems/AmI**

The focus group activities on embedded systems/AmI are organised by the Infonomics and New Media Research Centre at Zuyd University, and will involve three half-day meetings in the course of the project's duration.

These meetings will be following the format of a few short expert presentations, aimed at informing the group of recent technical developments, after which all present are invited to participate in a round table discussion. The presentations are intended to kick off, provide input for, inspire, and provoke the afternoon round table discussion. This discussion will be semi-structured by the tentatively formulated questions in the discussion notes below, inviting all participants to freely contribute to further specification and reformulation of the key problem definitions, identification of critical issues, and, eventually, potential solutions.

The results of this discussion will be used as input for the ethical brief to be developed, and constituting the principal deliverable from the focus group work. The ultimate objective of the work of the focus group is to generate insights, data, and discussions aiding in the writing and presentation of an ethical brief that will serve as an informative and balanced appraisal for the Commission, policy makers, as well as other stakeholders.

## 4 Discussion Notes

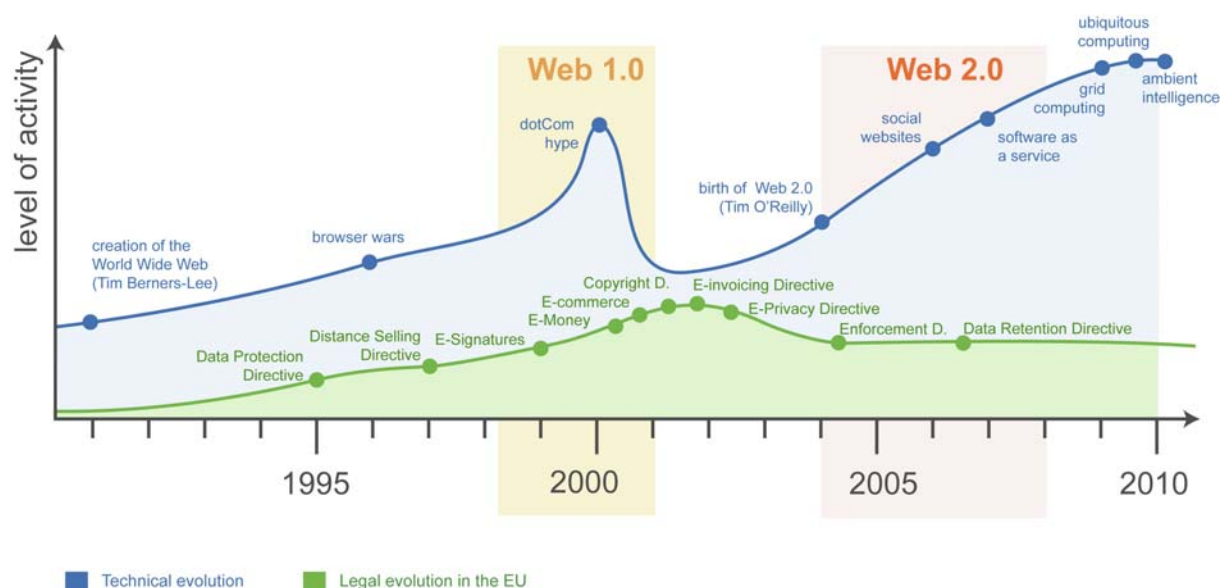
### 4.1 Subject of the FG : embedded systems and related concepts and technologies

'Embedded systems' is the title of this focus group. Since, however, only a limited number of embedded systems actually involve identification, personal or otherwise, it would be more adequate to the general purposes of HIDE to include in its scope the related and partly overlapping technological areas referred to as 'Ambient Intelligence (AmI)', 'Pervasive Pechnology', 'Ubiquitous Computing (UbiComp)', and 'The Internet of Things', all of which rely to a large extent on the possibilities afforded by Radio Frequency Identification (RFID). Although there is a large area of overlap between the various concepts, they all tend to emphasize or foreground different aspects. In view of the fact that HIDE is concerned in particular with personal and automated identification, the inclusion of the above mentioned technological areas in the subject matter of the current focus group seems justified.

The following discussion notes are developed from a review of a number of recent key documents published by various EC bodies (listed below), addressing issues and developments relating to the above mentioned technical areas. In the current European policy context, however, it appears that it is mainly RFID and The Internet of Things that tend to dominate the regulatory and legislative discourse, whereas AmI, UbiComp, pervasive technology, or embedded systems, while mentioned incidentally, are not to the same extent subject to policy debate and attempts at central regulation as such.

An exception to this is the recent Commission document on 'Europe's Digital Future', the following illustration taken from which clearly sees that near future as one of 'Ubiquitous Computing' and 'AmI':

Graph 2: Evolution of the legal and technical landscape



Source: DLA Piper, 2007, in EC COM(2008) 199 final *Preparing Europe's Digital Future*, p.7

The same document lists among its numerous `things-to-do`:

- Promote the *Internet of Things* through a Recommendation on *RFID*, focusing on privacy and security issues;
- Propose a set of actions to facilitate the transition to IPv6 (=requirement for the *IoT*, *IvdP*)
- Implement the eInclusion initiative: [...] *Ambient Assisted Living* flagship to respond to the challenge of an ageing population; [...]
- stimulate and increase investment by public-private partnerships in the form of Joint Technology Initiatives such as *ARTEMIS (embedded systems)* and *ENIAC (nanoelectronics)*.
- Respond to the challenges to privacy and trust stemming from new converging services in the future *ubiquitous information society*. (italics mine, IvdP)

Common element in these various concepts is the shifting out of computing power from PCs and desktop configurations to the physical and built environment, including the human body, appliances and instruments, the workplace, the home, the city, roads and highways, and eventually covering systems with global reach. From the perspective of the European Commission, the pivotal element and focal point in this development apparently is radio frequency identification (RFID), as its key enabler.

## 4.2 RFID as the object of EC Policy

Although this technology has been around for more than half a century, it is the more recent combination of RFID with information and communication technologies (ICTs) that brings possibilities within reach resulting in a shifting of gear with respect to its application potential and economic as well as social, political and ethical significance. Whereas at first the emphasis was on applications within production chain management and logistics within the retail sector, RFID has quickly become central to innovations spanning a much wider range of application areas such as transportation and traffic management, aviation, healthcare, security and access control, including border management.

Such are the prospects that, to quote the European Commission:

“RFIDs are indeed seen as the gateway to a new phase of development of the Information Society, often referred to as the "internet of things" in which the internet does not only link computers and communications terminals, but potentially any of our daily surrounding objects – be they clothes, consumer goods, etc.

It is this prospect that provoked the European Council of December 2006 to ask the European Commission to review the challenges of the next generation of Internet and networks at the 2008 Spring Council.

RFID is of policy concern because of its potential to become a new motor of growth and jobs, and thus a powerful contributor to the Lisbon Strategy, if the barriers to innovation can be overcome. The production price of RFID tags is now approaching a level that permits wide commercial and public sector deployment. With wider use, it becomes essential that the implementation of RFID takes place under a legal framework that affords citizens effective safeguards for fundamental values, health, data protection and privacy. “(COM(2007)96 final p.3)

The Commission sees its role as driving and fostering a coherent European approach which ensures common standards, harmonised legislation and compatible guidelines. The Commission also intends to foster complementary research into RFID implementation and its further evolution as part of an

Internet of Things. and to 'ensure that measures are established for securing Privacy & Security within the scope of the Data Protection Directive'.

Following the Communication, the Commission set up an RFID-Stakeholders Group, with the aims of providing an open platform allowing a dialogue between consumer organisations, market actors, and national and European authorities, including data protection authorities; it is also meant to support the Commission in its efforts to promote awareness campaigns at Member State and citizen level about the opportunities and challenges of RFID. (com p.9).

Also, alongside the European public debate, the Commission has strengthened its international contacts with foreign administrations in the United States and Asia. The stated objective is to agree on global interoperability standards and practices regarding data privacy and ethical principles. The Commission and the United States Government have started working together under the Transatlantic Economic Council (TEC) Initiative to develop a roadmap for cooperation in the field of Radio Frequency Identification (RFID), consisting of the short and long-term initiatives necessary to 'realize the potential of sharing information and best practices on the actual usages of RFID'. With this initiative, the Commission 'hope(s) to ensure that the deployment of RFID technologies in the business and consumer environments spurs innovation and helps society reap the benefits derived from the use of RFID in global commerce.' (see: The EU-US RFID Lighthouse symposium (Washington DC, September 22, 2008)

The Commission recognises that 'effective guarantees on data protection, privacy and the associated ethical dimensions are crucial for the public acceptance of RFID. Only then can the technology deliver its numerous economic and societal benefits.' Moreover, 'proper RFID governance is essential if RFID is to initiate a new wave of development of the Internet: the so-called "Internet of Things". Eventually, billions of smart devices and sophisticated sensor technologies could become interconnected into a global networked communication infrastructure.' From Europe's Information Society Thematic Portal on RFID we can glean a set of pertinent governance issues with respect to the world-wide organisation of RFID:

- ◇ Who will manage the storage of collected data? How will it be organised?
  - ◇ Who will have access to the databases which will register the unique digital code of each RFID-tag or tagged object? Who will be the owner of the databases?
  - ◇ What will the rules be for data-handling? Will third parties be able to use them?
- ([http://ec.europa.eu/information\\_society/policy/rfid/stakes/governance/index\\_en.htm](http://ec.europa.eu/information_society/policy/rfid/stakes/governance/index_en.htm))

### **4.3 Development of Policy on Privacy and Security**

Concern for privacy and security issues are repeatedly stated as among the primary concerns of the Commission.

Privacy and security should be built into the RFID information systems before their widespread deployment ("security and privacy-by-design"), rather than having to deal with it afterwards. The requirements of both the parties actively involved in setting up the RFID information system (for example business organisations, public administrations, hospitals) and the end users that are subjected to the system (citizens, consumers, patients, employees) must be considered during the design of this system. As end users typically are not involved at the technology design stage, the Commission will support the development of a set of application-

specific guidelines (code of conduct, good practices) by a core group of experts representing all parties. To this end, all security related activities and initiatives will be conducted in line with the strategy for a Secure Information Society set out in COM(2006) 251.

By the end of 2007, the Commission will issue a Recommendation to set out the principles that public authorities and other stakeholders should apply in respect of RFID usage. The Commission will in addition also consider including appropriate provisions in the forthcoming proposal for the amendment of the ePrivacy Directive and will, in parallel, take into account input from the forthcoming RFID Stakeholder Group, the Article 29 Data Protection Working Party<sup>19</sup> and other relevant initiatives such as the European Group on Ethics in Science and New Technologies. On this basis the Commission will assess the need for further legislative steps to safeguard data protection and privacy.

The Commission will continue to closely monitor the move towards the "Internet of Things", of which RFID is expected to be an important element. At the end of 2008, the Commission will publish a Communication analysing the nature and the effects of these developments, with particular attention to the issues of privacy, trust and governance. It will assess policy options, including whether it is necessary to propose further legislative steps to both safeguard data protection and privacy and address other public policy objectives.

The European Data Protection Supervisor (EDPS), in his opinion on this Communication (EDPS, 2007) concurs with the Commission's view of RFID as the 'gateway to a new phase of development of the Information Society' :

" 4. The EDPS agrees with the view that RFID systems could play a key role in the development of the Information Society usually referred to as the 'Internet of Things' and he also fully shares the concerns mentioned in paragraph 3.2 of the Communication that RFID systems may threaten individual's privacy and data protection rights. Indeed, in his Annual Report 2005, the EDPS identified RFID, together with biometrics, ambient intelligence environments and Identity Management Systems, as technological developments that are expected to have a major impact on data protection."

With respect to what is called 'item level tagging' (of consumer products, mainly in retail) the EDPS suggests certain elements of relevance to any impact assessment: the extent to which the item in question can be considered as '*personal*' (e.g. a wrist watch, as opposed to a can of softdrink), the *mobility* of the item; and the length of its *life cycle*.

The EDPS stresses, however, that an adequate assessment of RFID technology requires considering not the RFID tags alone, but the overall RFID infrastructure: the tag, the reader, the network, the reference database, and the database where the data produced by the association tag/reader are stored. Moreover, they insist that Privacy by Design should be at the forefront in all these developments, preferably by self-regulation and compliance to guidelines by the industry, but, if necessary, enforced through new legislation.

Clearly, the range of potential social and ethical issues associated with these broad developments is wide, and the discussions about the social, ethical and regulatory issues are well underway. For example, Both the Commission and the EDPS have made extensive use of the analyses provided already in 2005 by the Article 29 Data Protection Working Party, in its working document on RFID (see link below). Additional input to the Commission's Communication was provided by a public consultation on RFID, as well as a series of expert meetings.

Also, The European Parliament, more specifically, its Scientific Technology Option Assessment Service commissioned a study on RFID and Identity Management, carried out by the European Technology Assessment Group, in

order to inventorise current applications of RFID in the every day life of European citizens (ETAG, 2006).

One of the recurring conclusions in all these sources, is that there can be no general blue print covering the issues across the whole range of possible applications, and that any risks posed by these technologies to privacy, data protection, and fundamental rights and freedoms, depend very much on the specifics of any particular application or system configuration (e.g. the type of RFID tags used, the database architecture, the envisaged role of the end-user, the particular added functionalities, etc.)

To enhance the productivity of our FG deliberations, therefore, we propose to aim to devise:

A. a tentative *inventory* of the most important application areas / sectors

B a *taxonomy* of types of applications based on the particularities of system configuration and functionality.

#### **4.4 Biometrics and Body Data in Embedded Systems and AmI**

Moreover, to keep our focusgroup focussed, and increase the chances of bringing the debate forward rather than duplicate it, we propose to devote substantial part of our agenda to a particular subset of these technical developments and applications, the *intersection of these technologies with biometrics* and/or other body data.

Focussing on body-related technologies within Embedded Systems and AmI means that we look in particular at a paradoxical, dual development, namely the simultaneous 'shifting out' of computing power into the physical and built environment, and 'shifting in' towards the human body, its surface, and even internal functioning. Whereas on the one hand information and communication networks are extending, and becoming more all pervasive in our daily activities and movements through space, on the other hand, through various technologies and applications we become ever more intimately connected as embodied persons to these networks. As the European Group on Ethics argued (EGE 2005), becoming 'networked persons' is fraught with opportunities and threats. Threats, for example, to human dignity, freedom and autonomy, and inviolability of the human body. Indeed, what might be at stake could be as profound as a transformation of human embodied identity in the personal as well as the anthropological sense.

We therefore invite the participants to concentrate on identification of critical issues potentially arising from the use of biometrics, (and other personal and/or identifying body-data) in, or in combination with, the technologies subsumed under embedded systems, AmI, UbiComp, IoT, and RFID in particular, as well as applications of the latter that specifically involve the human body.

Possibilities here include:

- ◇ Biometric data *put on* RFID chips (e.g. e-passports) in ID-documents and cards
- ◇ Biometric identification/authentication in AmI systems

- for public security reasons , e.g. acces control/crime control in public events; continuous authentication in securing critical infrastructures (e.g. ACTIBIO)
- for system/network/information security reasons
- for convenience reasons (intuitive interfaces)
- ◇ RFID chips *linked to* body data (index to retrieve medical records), and possibly *implanted in* bodies (Verichip)
- ◇ Body monitoring sensors *combined with* RFID
  - for safety reasons in work environments (The Indian mine workers example), or home environments ('safe living' for the elderly), public sports events (marathon runners' pill)
  - for medical reasons in health care (e.g. telemonitoring)
  - for identification/authentication purposes (see above)
- ◇ Health risk profiling using RFID data

*We invite the participants to add to, fill out, and improve this list*

To be sure, most biometric systems to date have consisted of applications one could qualify as 'embedded', 'ambient', etcetera, under some definition, with biometrics used for PCs and desktop configurations, (log-ons and access control), forming a relatively insignificant part of applications.

The critical aspect coming to the fore more urgently with biometrics' co-evolution with AmI and UbiComp, however, is the emphasis on 'automated' identification, 'unobtrusive' and 'continuous' authentication, and covert data capture. The combination with RFID, for example, in many instances enables reading from a distance, without the biometric data subject noticing. Also, the 'user friendliness, and 'convenience', so high on the priority list of AmI developers, easily translates into 'as little conscious effort required from the end-user as possible'.

Moreover, biometric applications for securing public spaces develop increasingly towards (potentially) covert biometric data capture, such as, for example, in applications like 'smart' CCTV, or products like 'iris-on-the-move" .

Finally the application of RFID beyond the skin, that is in the form of implantable devices with a variety of added functionality, and networked connectivity, opens up a new horizon for serious controversy, and ethical deliberation, central to which is the debate on the informatisation of the body and the redefinition of what might mean the integrity of its boundaries.

#### **4.5 Questions to discuss**

Based on the considerations above we put the following tentative list of questions to the focus group:

*A Can we make a tentative inventory of the most important application areas / sectors*

*B Can we make taxonomy of types of applications based on the particularities of system configuration and functionality.*

*C Is it productive to restrict our FG to the particular subset of embedded technologies/applications involving human bodily identification and monitoring?*

1 What (type of) applications and systems enable surreptitious identification, tracking and tracing of individuals, and how?

2 To what extent is covert capture of personal and identifying data in Embedded Systems and AmI required for convenience and usability reasons? Can this be a matter of detail and nuance rather than an it being an either/or issue?

3 To what extent is covert capture of personal and identifying data, or secondary use of such data, for security and crime prevention interests justifiable? Where, at what point and by whom should such judgements be made?

4 How should issues of transparency, consent, and possibilities for democratic control be negotiated in such systems?

5 Are there prevalent reasons NOT to have identification/authentication procedures disappear into invisibility?

6 Are there viable technical options for reasonable balances between convenience and transparency?

7 How are systems targeting the human body different from an ethical point of view?

8 What kind of practices are enabled by data processing and profiling using body data generated by AmI systems?

9 What type of systems and applications targeting the human body gives rise to which issues in particular, and why?

10 What specific new vulnerabilities emerge with/from these systems, threatening whom in particular?

The **key reference documents** are:

- ◇ European Commission (2007) Communication: *Radio Frequency Identification (RFID) in Europe: steps towards a policy framework*, Brussels, march 15, COM(2007)96 final.  
[http://ec.europa.eu/information\\_society/policy/rfid/doc/rfid\\_en.pdf](http://ec.europa.eu/information_society/policy/rfid/doc/rfid_en.pdf)
- ◇ The European Data Protection Supervisor (EDPS) (2007) *Opinion on the Communication from the Commission on 'Radio Frequency Identification (RFID) in Europe: Steps towards a Policy Framework' COM(2007)96*, Brussels, December 26, 2007.  
[http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2007/07-12-20\\_RFID\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2007/07-12-20_RFID_EN.pdf)
- ◇ Article 29 Data Protection Working Party (2005), *Working Document on Data Protection Issues Related to RFID Technology*, January 19, pp.1-21  
[http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2005/wp105\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf)
- ◇ European Group on Ethics in Science and New Technologies (2005) *Opinion on Ethical Aspects of ICT Implants in the Human Body*, March 16.  
[http://ec.europa.eu/european\\_group\\_ethics/docs/avis20\\_en.pdf](http://ec.europa.eu/european_group_ethics/docs/avis20_en.pdf)

### **Additional reference documents.**

- ◇ European Commission Directive 2002/58/EC of the European Parliament and Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, July 12 2002 , Brussels. (*The ePrivacy Directive*)  
[http://www.dataprotection.ie/documents/legal/directive2002\\_58.pdf](http://www.dataprotection.ie/documents/legal/directive2002_58.pdf)
- ◇ European Commission Proposal for a Directive Amending (inter alia) Directive 2002/58/EC, Brussels, November 13. (*the ePrivacy Directive amendment*)
- ◇ European Commission COM(2005) 438 final *Proposal for a Directive of the European Parliament and Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC*, Brussels, 21.9.2005,  
[http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005\\_0438en01.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0438en01.pdf)
- ◇ Article 29 Data Protection Working Party (2008) *Opinion on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive)* , Brussels, May 15.  
[https://www.agpd.es/portalesweb/canaldocumentacion/docu\\_grupo\\_trabajo/wp29/2008/comunion/Opinion\\_GT29\\_modificacion\\_directiva\\_2002-58-CE.pdf](https://www.agpd.es/portalesweb/canaldocumentacion/docu_grupo_trabajo/wp29/2008/comunion/Opinion_GT29_modificacion_directiva_2002-58-CE.pdf)
- ◇ Article 29 Data Protection Working Party (2007), *Opinion 4/2007 on the Concept of Personal Data*, June 20, Brussels, pp. 1-26.  
[http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2007/wp136\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf)
- ◇ European Commission (2008) Communication: *Preparing Europe's Digital Future I2010 Mid-Term Review*, Brussels, April 17.  
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0199:FIN:EN:PDF>

◇ European Technology Assessment Group (2006) *RFID and Identity Management in Everyday Life*, The Rathenau Institute, The Hague.  
<http://www.itas.fzk.de/eng/etag/document/hoco06a.pdf>

◇ John Buckley (2006), *From RFID to the Internet of Things. Pervasive Networked Systems*. Final Report of the Conference organised by the DG Information Society and Media, Networks and Communication Technologies Directorate, March 6-7, Brussels, pp.1-32.  
[ftp://ftp.cordis.europa.eu/pub/ist/docs/ka4/au\\_conf670306\\_buckley\\_en.pdf](ftp://ftp.cordis.europa.eu/pub/ist/docs/ka4/au_conf670306_buckley_en.pdf)