Consumers' scenarios for a RFID policy

Joint ANEC/BEUC Comments on the Communication on Radio Frequency Identification (RFID) in Europe: steps towards a policy framework

COM(2007) 96

BEUC Contact: Cornelia Kutterer – cku@beuc.eu
Emilie Barrau – eba@beuc.eu
ANEC Contact: Chiara Giovannini – chiara.giovannini@anec.eu
BEUC Ref.: x/31/2007 – 03/07/07
ANEC Ref.: ICT-2007-G-059

SUMMARY

We welcome the adoption of the Communication on RFID technology by the European Commission. RFID is a domain that raises several consumers' concerns. Consumers need confidence to fully embrace RFID technology. The necessary trust can be achieved if the following measures are implemented:

- Consumers have a right to know about the use of RFID technology around them; this should be completed by impartial and comprehensive information campaigns on the RFID technology, its potential benefits and risks;

- Consumers have a right to choose whether they want RFID or not:

  ▪ We call for tags to be automatically disabled at the point of sale, unless the consumer expressly agrees otherwise (opt-in regime);

  ▪ Consumers shall not be discriminated against if they choose to disable, kill or remove the tags.

- A European committee dealing with ethics should be created and consulted ex-ante on any RFID or near field communication (NFC) technology applications raising potential ethical risks.

- Regulatory environment:

  ▪ We urge the Commission to proceed immediately with a gap analysis of the existing data protection legal framework, and to take the necessary steps;

  ▪ A future recommendation or code of conduct on RFID would be acceptable if fully respecting the minimum regulatory criteria of the Lund agreement.

  - Privacy and security:

  ▪ Privacy and security concerns must be taken into account as early as possible in the stage of deployment and shall be incorporated into the design;

  ▪ We favour research and development on PETs technology that is easy to use, available and affordable to all consumers;

  ▪ We call for the introduction of a liability scheme for damages caused to consumers by insufficiently protected RFID systems.

- Health and environment:

  ▪ We call for further research to assess potential health risks of RFID technologies together with exposure assessment procedures;

  ▪ Measures, from legal provisions to standards, to ensure proper waste, recycling and energy usage management of RFID tags should be developed.

- The Commission needs to address and control the risks to competition and market fragmentation issues raised by RFID applications.

- Standardisation:

  ▪ We call for the use of principals of good governance. Standards alone should not be used to address RFID consumer issues as this approach tends to shift decision-making from democratic institutions to standards bodies where consumer representation is not balanced;

  ▪ Standards should be widely available to all interested parties and not be used as a mean of market segmentation. Therefore, standards should preferably be free of Intellectual Property Rights or on FRAND basis.

INTRODUCTORY REMARKS

BEUC, the European Consumers Organisation, is the representative organisation of 40 independent consumer organisations from almost 30 European countries. BEUC is acting on behalf of consumers.

ANEC is the European consumer voice in standardisation, representing and defending consumer interests in the standardisation process and in legislation related to standardisation. It represents consumer organisations from all EU/EFTA countries.

Radio Frequency Identification (RFID) is a technology spreading rapidly, with an ever-increasing capacity. We thus welcome the timely adoption of the Communication and more generally the European Commission's pro-activity to safeguard consumers' privacy and security when this technology is applied.

The European Commission has repetitively accentuated that RFID technology has – besides tremendous economic effects - a great potential for improving the life of European citizens. Yet, this is still to be demonstrated. The results of the European Commission public online consultation on future radio frequency identification technology policy are not so obvious as far as the potential for RFID to improve the life of Europeans[1] is concerned.

Not all RFID applications raise consumer concerns or even concern consumers. Some usages may be beneficial to consumers, for example better food traceability or telecare for disabled and elderly people. However, the adverse effects that RFID could induce on consumers privacy (tracking and profiling of consumers, consumer discrimination), security (ID theft), health (EMF emissions) and ethics as well as on consumer freedom of choice, competition and environmental protection, are of concern to us.

ANEC and BEUC believe that the use of RFID technology should not be a goal in itself but a tool that consumers could derive benefits from. As the Commission rightly puts it: "*How can we make sure that these positive developments do not end up in nightmare scenarios?*"[2]

This joint ANEC/BEUC position paper expresses our views on possible future RFID scenarios and their impact on consumers, mainly focusing on RFID applications such as electronic tags (e-tags) in distribution/retail, in transport, payment services and counterfeiting. We suggest a number of policy measures meant to contribute to the current debate on RFID and further to the discussion on the Internet of Things. ANEC and BEUC therefore urge all European Institutions, to carefully debate about this technology and to take into consideration consumers' concerns on RFID in order to create a health, privacy and security enabling environment.

---

[1]   SEC(2007) 312, «About 44 % of respondents do not see great potential for RFID to improve the life of Europeans".

[2]   Policy framework paper for the RFID Security, Data Protection & Privacy, Health and Safety Issues workshop (May 16 and 17 2006),
      http://www.rfidconsultation.eu/?id_categoria=19&id_item=19&info=9

SCENARIO I: THE 'GLASS CONSUMER'[3]

1. RFID identification and tracing & tracking of consumers

RFID technology - sometimes combined with other technologies like GPS - will exponentially increase the possibilities of tracing and tracking consumers. The multiplication of readers and tags everywhere – from the workplace to the public transports to individuals' homes will facilitate this operation. For instance, transport cards in Paris (Navigo Pass) and London (Oyster card) already use RFID technology.

Tracing and tracking may raise serious ethical issues. For instance, the control of children's behaviour by parents, the surveillance of pupils' whereabouts by their schools or the controversial issue of RFID chips implanted in human body, are all applications with high ethical implications. An ethical assessment prior the implementation of such applications would be necessary.

  ➢ The Commission should not fund research and development of RFID applications aimed at tracing and tracking European citizens.
  ➢ A European committee dealing with ethics should be created; it should be consulted on any RFID or near field communication (NFC) technology applications raising potential ethical risks.

2. Respect of consumer basic rights

Objects, item-level tagging may lead to the direct or indirect identification and profiling of consumers through a 'constellation' of tags on several items; purely goods-related data could be combined with personal information contained on credit cards, loyalty cards or even bank notes in a near future. In fact, when combined with personal data or other identifying material, non personal data could become personal data, because it could lead to the clear or possible identification of a natural person[4].

Because RFID can lead to unnoticed consumer automatic identification, an essential prerequisite to effective data protection is that consumers know what their rights are. It is therefore important to reflect on how to best provide consumers with information on this technology.

---

[3] See 'The Glass Consumer: Life in a Surveillance Society', edited by Susanne Lace, National Consumer Council, 2005. "The properties and capacities of glass – fragility, transparency, the ability to distort the gaze of the viewer – mirrored our own potential vulnerability".

[4] See the Article 29 Data Protection Working Party document WP 105.

A. Right to know

The great majority of consumers has never heard of RFID and is not aware of the implications and risks to their rights to privacy and human dignity[5].

Consumers have a right to know about the use of any RFID technology around them. When entering a commercial or public environment consumers must be informed about the use and location of RFID tags and readers, whether the products they buy have RFID chips embedded and what the consequences are in terms of data gathering. However, it is important to stress that information alone will not solve all concerns about privacy.

> ➢ We encourage impartial and comprehensive information campaigns on the RFID technology, its potential benefits and risks, but also on data protection and privacy rights in general, organised and financed by independent public authorities.
> ➢ Information campaigns should consult consumer organisations and/or civil societies and take fully account of their opinions.
> ➢ We also advise to render legally mandatory harmonised and independent labelling (e.g. using pictograms) of products containing RFID and readers in order to inform consumers about their presence.

B. Right to choose

Consumers must have the choice to decide whether they want RFID or not and whether they want their data to be collected. The 'opt in' regime will thus allow consumers that so desire, to expressly ask for tags to remain 'on'. Exercising this choice should not result in any extra cost, damage or defect to a product or in any discrimination against the consumer who wishes to return an item.

> ▪ Destruction, removal or deactivation of RFID tags

The *destruction* or "kill" of an RFID tag may not always be the best option. However, if consumers wish tags to be "killed", this option should remain available. The *removal* of a chip is often a more appropriate solution. Yet, it can be problematic where chips are too small or not easily removable due to the specificities of a package or a product. To our opinion, *deactivation*, in the majority of cases, is an appropriate solution.

Two thirds of the respondents to the Commission consultation thought that RFID product tags in supermarkets should be automatically deactivated at the point of sale[6]. We suggest that all tags should be put on "privacy mode" or "silent mode" automatically once the consumers have left the store, thus rendering the data totally unavailable for reading, unless the consumer expressly and undoubtedly agrees otherwise (opt-in). Moreover, consumers should have the means to check deactivation so that they have the certainty that tags have correctly been deactivated.

---

[5]   61% of the respondents to the online consultation on RFID conducted by the European Commission consider that the information available for interested citizens on RFID is not sufficient and 66% asked for a clear indication of the presence of tag in supermarkets. The RFID Revolution: Your voice on the Challenges, Opportunities and Threats, Preliminary Overview of the Results, 16 October 2006 and SEC (2007) 312.

[6]   SEC (2007) 312. Similarly, in a recent study, 78% of respondents favoured the deactivation of tags at the check out (poll conducted by the German weekly Die Zeit and of the Humboldt University in winter 2005).

- ➢ Consumers shall not be discriminated against if they choose to disable, kill or remove the tags.
- ➢ In the light of current technical developments and for the time-being, we call for tags to be automatically disabled at the point of sale, unless the consumer expressly agrees otherwise (opt-in regime).
- ➢ Once in the shops, RFID tags should be on a 'read only mode (ROM)' and it should be impossible to embed a consumer's details into a RFID tag without his/her written and explicit consent.
- ➢ The Commission should make mandatory the provision of information on the status of tag (on, off, destroyed).

3. European regulatory framework

A. Existing European legislation

- ▪ Existing Directives

The EU Data Protection Directive[7] applies to data processed by automated means and aims to protect the rights and freedoms of persons with respect to the processing of personal data. This directive is technologically neutral i.e. it applies to RFID applications that collect information that is directly or indirectly linked to an identifiable or identified person and/or that store personal data.

The E-privacy Directive [8], actually being revised[9], applies to the processing of personal data in public communications networks.

- ▪ Shortcomings

However, in practice, the application of the above mentioned directives may not be so clear-cut. The Commission recognises that "*RFID devices raise fundamental issues on the scope of the Data Protection rules and the concept of personal data*"[10]. The definition of personal data is becoming more and more difficult to interpret[11] as well as other terms such as 'implicit consent', 'personal information' or 'legitimate interests'. The opinion of the Article 29 Working Party of Directive 1995/46/EC on the concept of personal data[12] is useful in providing general guidance. The data collected by RFID technology and other NFC technologies will most probably relate to an "identifiable" person in the sense of Directive 1995/46/EC, for instance through the combination of different pieces of information (e.g. trough data relating to objects) - even if one's name is never revealed - or because the technology itself gives the technical means that can be reasonably used by the controller or by any third party to identify a natural person.

---

[7] Directive 1995/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[8] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[9] The Commission considers in its communication on the review of the Telecommunications package that changes could be proposed to the ePrivacy Directive in the light of the RFID. See BEUC position paper, BEUC/X/063/2006.

[10] COM (2007) 87, p.7.

[11] See on that point the European Data Protection Supervisor's reflection on the definition of personal data in its 2005 annual report,
http://www.edps.europa.eu/EDPSWEB/Jahia/lang/en/pid/22

[12] Opinion 4/2007 on the concept of personal data, 20 June 2007.

For more legal certainty, we are looking forward to the further work of the Article 29 Working Party on the impact of data protection rules on the use of RFID.

The Commission also acknowledges that "*many RFID applications […] are not covered by the ePrivacy Directive*". The Directive requires that a processing of personal data is taking place within the context of a public communications network or a publicly available electronic communications service. However, RFID technology enables a communication without the need of a publicly available network[13].

The lack of enforcement of existing rules is equally essential. Several actions should be put in place to strengthen the respect of these rules such as compulsory data protection audits, regular compliance verification schemes and/or deterrent sanctions at national and European levels.

B. Reflection on further regulatory actions

▪ Revision of existing directives and new initiatives

The Commission proposes "*detailed guidance*" on the application of the existing directives to new technologies in the form of codes of conduct.

We invite the Commission to promptly, thoroughly analyse the existing legal framework to assess whether it adequately addresses the privacy and security risks that the applications of RFID and NFC technologies present for consumers in different contexts and sectors. Only then, could a decision be taken on the best way to ensure legal certainty.

➢ We urge the Commission to proceed immediately with a gap analysis of the existing legal framework, and to take the necessary steps to complement existing legislative measures, if necessary.
➢ We support the clarification brought by the opinion of the Article 29 Working Party on the concept of "personal data". Further reflection on the distinction between non-personal and personal data in the context of RFID technology and more generally, in the Ambient Intelligence world would nevertheless be necessary.
➢ In addition, further reflection on the notion of consent is required as data collection and processing are increasingly becoming the norm, rather than the exception.

▪ Other legal instruments and codes of conduct

The Commission plans to release a Recommendation – which is a non-binding instrument - to set out principles on RFID usage to be respected by all stakeholders, including public authorities. However, only 14 % of the respondents to the consultation mention a preference for self-regulation and best practices[14].

Enforceable guidelines, co-regulation and "soft-law" in general could have a role to play but are not enough as these instruments rarely provide for more consumer protection than existing binding rules. The Commission itself recognises the lack of

---

[13] Legal Issues for the Advancement of Information Society Technologies – http://www.rfidconsultation.eu/docs/ficheiros/Legal_issues_of_RFID_technology_LEGAL_IST.pdf

[14] The RFID Revolution: Your voice on the Challenges, Opportunities and Threats, Preliminary Overview of the Results, 16 October 2006.

quality of codes of conduct regarding the protection of personal data[15]. Therefore, ANEC and BEUC questions whether industry self-regulation instead of using traditional legislative instruments to address the critical issues raised by RFID, such as privacy protection, is a sound policy option.

➢ Whilst a recommendation or code of conduct may provide more flexible and rapid solutions in comparison to traditional law-making, such "soft law" measures would only be acceptable if fully respecting the minimum regulatory criteria of the Lund declaration16.

SCENARIO II: SECURITY FLAWS

1. A technology in development...yet, already in use

The desire to see RFID technology deployed and to keep the costs down, has so far put aside any serious consideration of security and privacy. Most existing tags have limited memory capacity, which means that they work without sophisticated data encryption techniques. However, consumers' responses to RFID technology will be crucial to its future. If the industry does not ensure proper privacy and security, consumers will definitely lose any confidence in RFID technology. Several technical and regulatory solutions must be developed (such as short range frequencies, encryption, authentication, removable antenna...).

RFID still has major technical vulnerabilities. For instance, governments around the world are adding RFID tags to identification documents to avoid forgery. However, it has not proven very efficient so far: the Belgian, Dutch, German and American e-passports have already been cracked by hackers and the content of the RFID tag copied[17].

2. Challenges for consumers' confidence: end-user control of the technology

A. Privacy and security by design

Due to security weaknesses in the design of email exchange, spams today constitute 50 to 75% of the total volume of email traffic which is not only annoying to consumers but also constitutes a macro-economic burden[18]. The same mistake must not be repeated with RFID technology. Moreover, the complexity of the RFID/NFC

---

[15] COM (2007) 87, p.5.
[16] European Seminar organised by the Swedish Presidency "Voice of the European Consumer" (Lund, April 2001). The Lund criteria are: efficacy, democratic legitimacy, consumer confidence, together with coherence and consistency in the context of the single market.
[17] 'Security risks of e-passports exposed', 07.08.06, ZDNet, http://news.zdnet.co.uk/communications/networks/0,39020345,39280536,00.htm At the Black Hat conference "researchers demonstrated that passports equipped with radio frequency identification (RFID) tags can be cloned with a laptop equipped with a $200 RFID reader and a similarly inexpensive smart card writer", even though the information cannot be changed. They also managed to copy corporate access cards.
[18] The Washington Post reported that the damage done by viruses and spy ware showed that US consumers paid as much as $7.8 billion over two years to repair or replace computers that got infected with viruses and spy ware. Consumer Reports, State of the Net, September 2006.

technologies environment will very often require a level of technical knowledge to protect one's privacy and security far beyond what an average consumer is expected to know.

We support the Commission's statement that "*privacy and security should be built into the RFID information systems before their widespread deployment*"[19] at the "*technological, organisational and business process levels*"[20]. Moreover, the Data Protection Directive emphasises the importance of taking appropriate technical and organisational measures both at the time of the design of the processing system and at the time of the processing itself[21]. Therefore, assessments prior to the deployment of RFID applications would be required[22]. In case where a security breach has occurred, e.g. where data has been copied or altered by an unauthorised third party, the affected consumer must be personally informed and appropriate steps taken to rectify the situation. Moreover, if a consumer consequently suffers damage, the company responsible should be held liable and thus should compensate the consumer. The burden of proof and the responsibility to produce relevant documentation should be held by the professionals.

> ➢ The Commission should develop privacy and security impact assessments (PIAs/ SIAs) to help developers and operators spot risks and build protection when designing new products/systems.
> ➢ We believe that the incorporation of consumers' concerns in the design phase, the user-friendliness of the technology and the prevention of 'information over-flow' are a prerequisite for a successful introduction of RFID and NFC technologies.
> ➢ It is critical that privacy and security safeguards are put in place at all levels of the system (chip, reader, database, backend systems) before further deployment of the technology.
> ➢ We call for the introduction of liability for damages caused to consumers by insufficient protected RFID systems.
> ➢ We welcome the proposal from the Commission to involve end-users and civil societies' representatives during the design of the system.
> ➢ RFID technology should fully respect the principles set out in the PRIME project (to which BEUC is a member)[23].
> ➢ In addition, discussion is urgently needed on governance in particular in respect of the object name system (ONS) and its potential impact on security.

---

[19] COM (2007) 97, p. 9.
[20] COM (2007) 96, p.6.
[21] Article 17 and Recital 46 of Directive 95/46/EC; see also the Article 29 Data Protection Working Party document WP 105.
[22] COM (2007) 96, p.6/7.
[23] PRIME principles: Design must start from maximum privacy; Explicit privacy governs system usage; Privacy rules must be enforced, not just stated; Privacy enforcement must be trustworthy; Users need easy and intuitive abstractions of privacy; Privacy needs an integrated approach; and, Privacy must be integrated with applications; https://www.prime-project.eu/

B.   PETs

Privacy enhancing technologies (PETs) have often been mentioned as a possible solution; both directives 95/46/EC and 2002/58/EC[24] encourage the use of PETs. In addition, 70% of the respondents to the consultation believe that PETs are the best way to reduce security, data protection and privacy concerns[25].

However, PETs have not proved very user-friendly so far as they are difficult to use and to understand for consumers. On top of little consumer awareness, PETs are also rather expensive.

> ➢   We would favour research and development on PETs technology that is easy to use, available and affordable to all consumers. We particularly support the PRIME project26 working on a privacy-enhancing Identity Management System.
> ➢   We think the Commission should support the elaboration of PETs performance standards in order to make products comparisons and help consumers with their choice.

SCENARIO III: IMPACTS ON HEALTH AND THE ENVIRONMENT

1.   Health

It is expected that RFID technologies will significantly contribute to exposures to Extremely-Low-Frequency (ELF) components. Little or no data is currently available to assess the potential health hazards arising from the use of these technologies. Moreover, as recently stated by the European Commission Scientific Committee on Emerging and Newly Identified Health Risks (SCENHIR)[27], ELF magnetic fields are possibly carcinogenic, mostly based on occurrence of childhood leukaemia.

Regarding electromagnetic fields (EMF) exposure, ANEC and BEUC regret the lack of data for the risk analysis of RFID applications and pervasive computing applications[28]. In particular, evaluation is needed if specific limits or extension to existing standards have to be added regarding on-body antennas (highly localised fields) or the combination of different sources operating at different frequencies or within different frequency bands.

> ➢   We believe that new exposure assessment procedures for testing compliance with safety guidelines are necessary. Moreover, further research is needed in order to assess potential health risks of RFID technologies together with exposure assessment procedures.
> ➢   In the meantime, we call the Commission, national governments and businesses to apply the "principle of precaution" to the deployment of RFID technologies.

---

[24]   Respectively in Article 17 and Recital 46 and in Recital 30.
[25]   SEC (2007) 312.
[26]   PRIME project website: https://www.prime-project.eu/
[27]   SCENHIR opinion on the possible health risks of Electromagnetic Fields (EMF), May 2007, http://europa.eu.int/comm/health/ph_risk/committees/04_scenihr/04_scenihr_en.htm
[28]   A number of countries and regions, including most EU countries, have adopted the ICNIRP limits within their own regulations. However, scenarios including different sources in close vicinity to the body are not taken into account.

2.   Environment

The amount of copper and other heavy metals but also silicon and adhesives used in RFID chips give rise to important environmental concerns for disposal and recycling processes[29]. It is therefore necessary to reflect on how the EU could promote sustainable, environment-friendly RFID chips and foster research on the way to include environmental concerns into the technology[30]. Although RFID chips would fall within the meaning of "waste electrical and electronic equipment"[31], including all components, subassemblies and consumables which are part of the product at the time of discarding, we would like to highlight the practical difficulty when the RFID tag is embedded in the packaging. Moreover, we believe that it would be appropriate to prevent the use of some chemicals in RFID tags[32]. The aim would be to achieve tags that are environmentally neutral or made of decomposable materials.This should be taken into account.

In addition, the widespread use of RFID networked technologies could lead to an increase of energy consumption due to the multiplication of microprocessors in objects continuously connected but also due to the data centres – having to deal with an ever-increasing number of data collected[33].

> ➢ The Commission should support the development of measures, ranging from legal provisions to standards, in order to ensure proper waste, recycling and energy usage management of RFID tags.
> ➢ Rules should be set throughout the value chain, assigning responsibility and accountability for the disposal of the tags.

SCENARIO IV: THE ECONOMIC IMPACT

1.   Competition

RFID technology has the potential to be used in anti-competitive ways, restricting consumer choice. For instance, a car manufacturer X would design software that exclusively works with the spare-parts of this same manufacturer X - parts that will have RFID chips embedded (tie-in products). The usage of RFID in applications that control the use of products or force consumers to buy products that are more costly would restrict consumer choice, and consequently impact competition. Similarly, RFID technology must not prevent the use of compatible, alternative printer refill cartridge, i.e. those not produced by the original manufacturer, by means of authenticity certificates.

> ➢ The Commission needs to start investigating, addressing and controlling the risks to competition and market fragmentation issues raised by RFID

---

[29]   'RFID from production to consumption- risks and opportunities from RFID- technology in the value chain', The Danish Board of Technology, June 2006.

[30]   Unlike a traditional silicon RFID chip, organic chips only use 100% organic compounds (plastic) and an inkjet printer. They are currently being developed.

[31]   Article 1(a) of WEEE Directive 75/442/EEC.

[32]   Restriction of use of certain hazardous substances in electrical and electronic equipments (ROHS) Directive 2002/95 EC.

[33]   See the article 'Data centres face cooling crisis', 13.04.07, ZDnet UK.

applications. It must use European anti-competition laws to prevent and, when applicable, sanction such abuses. Additionally, where required, the Commission should take the necessary steps to complement existing legislative measures.

2.   Prevention and dissuasion of counterfeiting

Technology could play a role in protecting intellectual and industrial property rights (IPRs) as well as ensuring consumer safety. We are nevertheless sceptical about the use of RFID technology as a means to avoid theft and counterfeited products (be it drugs, clothes, CDs or DVDs). In fact, the very technology that is used to protect IPRs can be forged, due to the very low or non-existent level of security of the tags used. Moreover, the use of RFID technology on sensitive products such as drugs also raises serious privacy concerns[34]. Other technologies, with lower privacy implications could be exploited. For instance, as reported in the Bridge report[35], the pharmaceuticals industry is supporting 2D barcode instead of RFID as the preferred identification technology.

> ➢   We believe that in terms of counterfeiting prevention and dissuasion, RFID technology falls short of proving its case.
> ➢   We favour the use of other technologies, raising less privacy and security concerns.

SCENARIO V: THE USE OF RFID STANDARDS

As the Commission[36], we believe in "*diversity, openness, interoperability, usability and competition as key drivers for security*" and for a successful technology beneficial to consumers. Standardisation, involving consumers' organisations, will help in the development of RFID open standards meeting consumer requirements.

We share the Commission's opinion on International standards meeting European requirements, especially when fundamental consumers' issues such as privacy and health are concerned. However, the use of industry fora and consortia deliverables should not be made at the expense of quality and democracy. From a consumer point of view, the lack of transparency and consensus involved raises concerns because they impede proper consumer participation and could lead to the adoption of non-open standards. Therefore, we believe that a balance between efficiency and openness must always be maintained.

We call the European Commission to use principles of good governance. With regards to RFID this includes decision-making from democratic institutions. The European Commission should not use standards to address RFID consumer issues - instead of regulation - as this approach tends to shift decision-making from democratic institutions to standards bodies where consumer representation is not balanced.
We are of the opinion that standards should be widely available to all interested parties and not be used as a mean of market segmentation. Therefore, standards should

---

[34]   Please refer to section I of this paper.
[35]   Bridge report, February 2007, funded by the European Commission, http://www.bridge-project.eu/data/File/European%20Passive%20RFID%20Market%20Sizing%202007-2022-v1.pdf
[36]   COM (2006) 251 - p.9.

preferably be open and free of Intellectual Property Rights, or licensable on a fair, reasonable and non-discriminatory basis (FRAND).

Given that lack of resources is one of the major obstacles for consumer participation in standardisation, it is crucial to provide adequate resources to consumer organisations.

END