Radio Frequency Identification (RFID)

Draft Commission Recommendation on the implementation of privacy and information security principles in applications supported by radio-frequency identification – "RFID Privacy and Security Recommendation"

Joint ANEC/BEUC comments

BEUC Contact: Emilie Barrau – legal@beuc.eu
ANEC Contact: Chiara Giovannini -chiara.giovannini@anec.eu
BEUC Ref.: X/029/2008 - 25/04/08
ANEC Ref.: ANEC-ICT-2008-G-017

BEUC, the European Consumers' Organisation, www.beuc.eu
ANEC, The European Consumer Voice in Standardisation, www.anec.eu

Summary

Consumers need confidence to fully embrace Radio Frequency Identification (RFID) technologies. As rightly stated by the European Commission: "*a precondition for the successful take-up of RFID is that it be introduced by industry in full respect of privacy, and that consumers remain in full control of their personal data*"[1].

ANEC and BEUC welcome the adoption by the European Commission of the draft Recommendation focusing on privacy, data protection and security aspects of RFID technology which, we believe, takes into consideration most of consumers' concerns.

In particular, we fully support the following measures:

- In retail, the opt-in approach will guarantee that tags will be automatically and immediately deactivated at the point of sale if personal data are likely to be collected and processed, unless the consumer explicitly asks to keep the tags on.
- More transparency and information obligations; Consumers must know where, when, why and how RFID is being used in their surroundings. Signs or logos showing the presence of tags and readers are to be welcomed.
- Privacy and security impact assessments that would guarantee that privacy and security questions are addressed prior to the implementation of RFID applications.

In parallel, the enforcement of existing rules is equally essential. Several actions should be put in place to strengthen the respect of these rules.

Finally, the use of RFID technology also raises ethical, competition, health and environmental concerns that are also paramount/strategic to consumers' acceptance of the technology. Therefore, ANEC and BEUC strongly encourage the European Commission to start addressing those aspects as soon as possible.

[1] European Commission Frequent Asked Questions on RFID, MEMO/08/145, 5 March 2008.

Comments on the articles of the draft recommendation

Article 1

1. This Recommendation provides guidance to Member States and stakeholders on the design and operation of RFID applications in a lawful, ethically admissible and socially and politically acceptable way, respecting the right to privacy and ensuring protection of personal data and appropriate information security.

2. This Recommendation concerns measures to be taken with respect to the implementation of RFID applications, which will ensure that national legislation implementing Directives 95/46/EC, 99/5/EC and 2002/58/EC is respected when such applications are deployed. This Recommendation is without prejudice to the legal obligations resulting from the national legislation implementing Community Law.

3. This Recommendation shall not apply to activities which fall outside of the scope of the Treaty establishing the European Community, such as those referred to in titles V and VI of the Treaty of the European Union, and in any case to activities concerning public security, defence, state security and the activities of the state in the areas of criminal law.

Article 1 – Scope

The recommendation focuses on privacy, data protection and information security, which we believe are the most pressing issues to be tackled. A reference to the European Charter of Fundamental Rights and the European Convention on Human Rights should be made in Article 1.2.

The European Commission should nevertheless continue to work and promote research on other aspects of RFID – in particular competition, environment and health aspects, equally important for consumers.

Article 2

For the purpose of the Recommendation the definitions set out in Directive 95/46/EC shall apply. The following definitions shall also apply:

(a) 'Radio frequency identification' (RFID) means the use of electromagnetic radiating waves or reactive field coupling in the radio frequency portion of the spectrum to communicate to or from a tag through a variety of modulation and encoding schemes to uniquely read the identity of a radio frequency tag or other data stored on it.

(b) 'RFID tag' or 'tag' means either a RFID device having the ability to produce a radio signal or a RFID device which re-couples, back-scatters or reflects (depending on type of device) and modulates a carrier signal received from a reader.

(c) 'Reader' means a fixed or mobile data capture and identification device using a radio frequency electromagnetic wave or reactive field coupling to stimulate and effect a modulated data response from a tag or group of tags.

(d) 'RFID application' means a system to process data through the use of RFID tags and/or readers, a back-end system and/or a networked communication infrastructure.

(e) 'RFID application operator' means the natural or legal person who develops, implements, uses or maintains a RFID application.

(f) 'Information security' means the preservation of confidentiality, integrity and availability of information.

(g) 'Monitoring' means any activity carried out for the purpose of detecting, observing, copying or recording the location, movement, activities, image, text, voice, sound or state of an individual.

(h) 'Deactivation' of a tag means the process that causes the cessation of any functionality of the RFID tag. The deactivation can be permanent, so that the tag no longer responds to any command, or can be temporary, so that the tag only responds to specific commands that make the tag partially or entirely functional again.

(i) 'Public place' means any area, including non-stationary means of public transport such as buses, planes, railways or ships, which can be accessed at all times or at certain times by everybody.

Article 2 - **Definitions**

Article 2 (h) – Deactivation

It will be very confusing for consumers to use the same term "deactivation" for two different realities.

At the very least, the definition of "deactivation" should be split into two: (1) "permanent deactivation" and (2) "temporary deactivation". One single definition may lead to confusion amongst stakeholders and consequently to a situation where consumers are told that their tag has been deactivated – without clearly telling them if it is permanent or temporary. Today this distinction might not be very relevant as temporary deactivation is not yet available but it will certainly be crucial in the future as the technology develops.

Moreover, there is an inconsistency in this definition: How deactivation would cause "cessation of any functionality" while still allowing "tag [to be] partially or entirely functional again". Furthermore, it is not clear who initiates the "specific commands" that would render the tag functional again.

Furthermore, it would be appropriate to give a definition of 'privacy impact assessment'. Finally, those definitions should be "technically neutral" and apply to all kind of RFID technologies.

Article 3

1. Before a RFID application is implemented, the RFID application operators should conduct, individually or jointly within a common value chain, a privacy impact assessment to determine what implications its implementation could raise for privacy and the protection of personal data, and whether the application could be used to monitor an individual.

2. The level of detail of the assessment should be proportionate to the risks associated with the particular RFID application. The assessment should comply with good practice frameworks to be established in a transparent way in partnership with all relevant stakeholders, and in consultation of the relevant supervisory data protection authorities.

3. Where it cannot be excluded that data processed in RFID applications can be related to an identifiable natural person by an RFID application operator or a third party, Member States should ensure that RFID application operators and providers of components of such applications take appropriate technical and organisational measures to mitigate the ensuing privacy and data protection risks.

4. RFID application operators should designate a person responsible for the conduct, review, and follow-up measures as described above.

5. The RFID application operator should align the privacy impact assessment with the overall information security risk management set out in Article 6 here after.

6. The RFID application operator should make the privacy impact assessment, or an adequate and comprehensible summary of it, publicly available through appropriate means, no later than on the date of deployment of the application.

Article 3 - **Privacy and Data Protection measures**

Privacy Impact Assessment (PIA)

The best way – and the most (economically) efficient way - to ensure that a specific RFID application is fully compliant is to assess its potential impacts on privacy and security before its deployment i.e. from the very beginning.

We therefore fully support the systematic use of privacy impact assessments (PIAs) and the development of technical and organisational measures to limit the risks "*where it cannot be excluded that data processed in RFID applications can be related to an identifiable natural person by an RFID application operator or a third party*". Of course, PIAs and information security risk management go hand in hand. We nevertheless regret that the wording "privacy and security by design" is not mentioned as such in this article. We also miss the lack of reference to Privacy Enhancing Technologies (PETs) in the draft recommendation. It should be further clarified that "a third party" also includes parties outside a contractual relationship.

More clarity is needed as to what "*good practice frameworks*" mean and the level at which they should be established (at national, regional and/or European level?). The method on how to conduct a PIA is essential and we regret that no clarifications have been brought as to – at least - the main steps such an assessment should follow. The involvement of data protection authorities is to be welcomed. References to the Information Commissioner Office PIA Handbook[2] mentioned in the consultation as well as any other relevant documents could be inserted in an annex to the recommendation.

The European Commission with the help of the Article 29 Working Party and Member States should also ensure consistency across Europe of the different approaches towards PIAs.

Transparency

As regards Article 3.6, we welcome the publication of the results – both in full and a summary - of PIAs. Such publications should be easily available (e.g. on the website of the RFID application operator), written in:

- plain/intelligible language (but allowing for more technical details in the full report);
- accessible at no costs; and,
- at the latest on the date of the deployment of the application.

Responsibility (Article 3.4)

Clear responsibility is paramount to the good functioning of the system. We agree that RFID application operators should designate a person – who should be named expressly in the PIA results published - responsible for the conduct, review, and follow-up

[2] http://www.ico.gov.uk/upload/documents/pia_handbook_html/html/1-intro.html

measures. It goes without saying that a PIA should be regularly reviewed taking into consideration state of the art technology and new potential threats to data protection and privacy.

Article 4

1. Member States should encourage trade or professional associations or organisations involved in the RFID value chain to provide detailed guidance on practical implementation of RFID technology by drawing up specific codes of conduct on RFID use. Where appropriate, this work should be undertaken in collaboration with the concerned civil society organisations, such as consumer organisations or trade unions, and/or the competent authorities concerned. Codes of conduct should contain specific measures designed to ensure that signatories adhere to their principles. They should be widely disseminated with a view to informing affected individuals

2. With regard to data protection aspects, Member States should encourage drawing up of codes of conduct intended to contribute to proper implementation of the national provisions adopted pursuant to the Directive 95/46/EC, taking account of the specific features of the various sectors.

3. In conformity with Directive 95/46/EC, national codes of conduct should be submitted to the relevant national supervisory data protection authorities for endorsement, and Community codes of conduct should be submitted to the Article 29 Working Party for endorsement at Community level.

Article 4 - **Codes of Conduct**

In general, ANEC and BEUC are sceptical about the use of codes of conducts. These instruments rarely provide more consumer protection than existing binding rules, lack consumer redress and effective sanctions when codes are violated.

<u>For the implementation of data protection rules (Article 4.2 and 4.3)</u>

As long as it is clear that codes of conduct only complement legislation and fully respect the minimum regulatory criteria of the Lund declaration[3], we can support this provision. We welcome the endorsement by the relevant national supervisory data protection authorities but Member States must ensure that the resources of these authorities are sufficient to handle this task.

Nevertheless, we like to recall that the European Commission has itself recognised the lack of quality of codes of conduct regarding the protection of personal data[4].

<u>For the practical implementation of RFID (Article 4.1)</u>

In the specific case of practical implementation of this recommendation however, codes of conduct may provide more flexible and rapid solutions for "detailed guidance" in comparison to traditional law-making. Where such alternative mechanisms exist, it is crucial that proper sanctions are put in place in case of non-compliance. This must be clearly reflected in the text of the article.

[3] 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.

[4] COM (2007) 87, p.5.

Article 5

1. Where RFID applications are implemented in public places, RFID application operators should make publicly available a written comprehensible policy governing the use of their RFID application.

Without prejudice to the obligations of data controllers, in accordance with Directives 95/46/EC and 2002/58/EC, the policy should state:

(a) the identity and address of the RFID application operator,
(b) the purpose of the RFID application,
(c) what data is to be processed by the RFID application, in particular if the location of tags will be monitored,
(d) which link, if any, is made with personal data,
(e) what is the data storage policy followed by the operator,
(f) if the data can be accessed or received by third parties.

The policy should be concise and generally understandable by individuals.

2. Where RFID applications are implemented in public places, RFID application operators should inform individuals on the use of RFID by providing at least a clear sign, accessible by all, that signifies the presence of RFID readers. Information should include, where appropriate, that RFID tags and readers may broadcast information without an individual engaging in any active action, a reference to the policy governing the use of the RFID application and a point of contact for individuals to obtain additional information.

Article 5 - Information on RFID use

As the European Commission rightly recalls, RFID is a contactless and invisible technology that can process data without anyone noticing.

We thus welcome more transparency in the use of RFID technology in the form of reliable, to the point, fully understandable (not "*generally understandable*") and apparent information. Such information should be targeted to the audience to which it is aimed at (e.g. consumers; employees…) and be available in different formats (e.g. text, logo, video, voice) so as to reach all consumers, irrespective of their age and abilities. In particular, consumers should be informed about the presence of readers and reading activities and distance - even "*without an individual engaging in any active action*". It is equally essential that the presence of tags is notified to consumers by a harmonised sign or logo. We ask the Commission to modify the text accordingly.

The article foresees that a written policy should be made "*publicly available*" without stating how. The Commission must add in the article that such information should at least be available to consumers on the spot (i.e. at the point of sales/premises of the operator), where possible, before entering the area, and, where relevant, on the website of the operator.

However, providing this information to consumers should by no means be interpreted as an explicit consent from consumers on the use of RFID tags for collecting their personal data or as a transfer of responsibility.

This article only provides for minimum information requirements and, in order to foster consumers' confidence in RFID, we would encourage RFID operators to be as open as possible on their RFID use. In particular, having sufficient and adequate information about the security features of RFID is an essential consumer need.

Article 6

1. Member States should encourage RFID application operators to establish information security management according to state-of-the-art techniques, based on effective risk management in order to ensure appropriate technical and organisational measures related to the assessed risks. The security threats, and the corresponding security measures, should be understood as covering all the components and interfaces of the RFID application.

2. Member States should provide guidance to identify those RFID applications that might be exposed to information security threats with implications for the general public. Member States should also stimulate RFID application operators that provide these applications to develop application-specific guidelines, in partnership with all concerned stakeholders. Public and private sector organisations should strive to ensure that their members comply with these guidelines. The dissemination of Best Available Techniques for these applications at European level should be encouraged with a view to achieving a coherent internal market approach towards information security.

3. Member States should encourage the RFID application operators, together with national competent authorities and civil society organisations, to develop new, or apply existing, schemes, such as certification or operator self-assessment declaration, in order to demonstrate that an appropriate level of privacy and information security is established in relation to the assessed risks, related to RFID applications.

Article 6 - **Information security risk management**

Information security risk management – sometimes also called Security Impact Assessments (SIAs) – before the deployment of a RFID application is crucial to ensure the security at all levels of an application (tag; reader; the interaction between the chip and the reader; databases – be it databases solely containing RFID data or customer databases containing RFID data which is linked to customer information; back-end system…). The use of inappropriate levels of security for one component could endanger the whole RFID application.

In the past, the European Commission stated that "*privacy and security should be built into the RFID information systems before their widespread deployment*"[5] at the "*technological, organisational and business process levels*"[6]. Besides, 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[7]. We fully support privacy and security by design and would suggest this wording to be restated in the text of the Recommendation.

Member States, as part of the Information Security Risk Management, should have an obligation to invest in research and development (R&D) to ensure continuous enhancements of the infrastructure. The possibility of permanent improvements and updating was not foreseen in the case of the Internet, which created the spam problems we know today.

The guidelines should also include a requirement for interoperability, i.e. the technical RFID architecture should be based upon open standards so that different systems – proprietary as well as open – can function together.

As regards responsibility, we regret the lack of provision on the designation of the person responsible for conducting, reviewing and ensuring the follow-up of the information

5 COM (2007) 97, p. 9.
6 COM (2007) 96, p.6.
7 Article 17 and Recital 46 of Directive 95/46/EC; see also the Article 29 Data Protection Working Party document WP 105.

security risk management but also informing consumers should a security breach has occurred and taking appropriate steps to rectify the situation. A paragraph similar to Article 3.4 on PIAs should be added to this article.

Member States should foresee a mechanism at national level where, if a consumer suffers damage from a security breach, 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.

Article 6.3

In order to meet consumer expectations, defined and clear qualitative security requirements should be identified. In this context, we believe that the primary information that influences consumers' choice is compliance of the product with declared security features and that the product has passed an external conformity assessment procedure. Such compliance could be identified by a mark. Products and services not meeting declared requirements lead to a loss of consumer confidence.

Article 7

1. RFID application operators acting at any level of the value chain should ensure that they provide sufficient information and means to operators down the chain so that the provisions of this recommendation can be followed.

2. RFID application operators, where appropriate in cooperation with retailers, should adopt a harmonised sign to indicate the presence of tags within retail products and ensure that consumers are informed:

- *about the presence of a RFID tag in a retail product;*
- *whether this tag has a specified, explicit and legitimate purpose after the sale;*
- *about the likely reasonable privacy risks relating to the presence of the tag and of the measures consumers can take to mitigate these risks.*

3. (a) Where a RFID application processes personal data or the privacy impact assessment (undertaken in accordance with Art 3.1) shows significant likelihood of personal data being generated from the use of the application, the retailer has to follow the criteria to make the processing legitimate as laid down in directive 95/46 and to deactivate the RFID tag at the point of sale unless the consumer chooses to keep the tag operational.

(b) Where a RFID application does not involve processing of personal data and where the privacy impact assessment has shown negligible risk of personal data being generated through the application, the retailer must provide an easily accessible facility to deactivate or remove the tag.

4. Deactivation or removal of tags should not entail any reduction or termination of the legal obligations of the retailer or manufacturer towards the consumer. Deactivation or removal of tags by the retailer should be done immediately and free-of-charge for the consumer. Consumers should be able to verify that the action is effective.

5. Within three years after the entry into force of this recommendation, the European Commission will review these provisions in order to assess the effectiveness and efficiency of systems to remove or deactivate tags with a view to providing automatic deactivation at the point of sale on all items except where the consumer has specifically opted-in to the RFID application.

Article 7 - RFID use in retail

Consumers should not have to take the initiative to protect their personal data against unwanted reading of RFID tags; nor should they be required to give up their privacy in order to participate/engage in normal day to day activities such as retail shopping. We believe that the protection of personal data and privacy is a fundamental right. It is the duty of other parties, including especially data controllers, to respect and protect that right.

Article 7.1

We believe that it is crucial for a well functioning system and for proper information of consumers/end-users that all relevant information and means are passed "down the chain" to RFID operators – which include sales persons/employees having contact with consumers.

Article 7.2

We welcome the use of a sign or logo to inform consumers about the presence of RFID tags. Obviously, this has to be read in conjunction with Article 5 on general information on RFID use (including on the presence of readers and reading activities).

As regards the information on the "*legitimate purpose*", this has to be interpreted in the light of the European data protection Directives.

In addition to the measures foreseen in this recommendation, consumers should only take "additional" measures to protect their privacy against RFID threats. The text of the recommendation should be modified accordingly.

Complementary information

RFID might be of added-value for consumers where tags exclusively provide complementary information on products (e.g. about the production, origin, quality, energy use….). Means to read this additional information should be made freely available to consumers in the shop and before the point of sale.

Article 7.3

We warmly welcome the opt-in principle when personal data are generated and processed as consumers must have the choice to decide whether they want RFID or not and whether they want their data to be collected. In an 'opt in' regime, the retailer has to deactivate the RFID tag at the point of sale unless consumers that so desire, expressly ask for tags to remain operational. On the contrary, in an opt-out scenario, the consumer has to ask for the tag to be deactivated.

The opt-in option reflects the unequivocal choice of European consumers: Two thirds of the respondents to the European Commission online consultation thought that RFID tags on products in supermarkets should be automatically deactivated at the point of sale[8]. Similarly, in a recent survey carried in the Netherlands, 85% of respondents want to decide whether the chips stays active and 62% want default deactivation (opt-in system)[9].

8 European Commission public consultation on RFID, 2006.

9 Consumentenbond, the Rathenau Institute, ECP.NL survey 2007.

This principle is further supported by the Opinion of the European Data Protection Supervisor (EDPS) according to which "*the opt-in principle at the point of sale is a legal obligation that already exists under Data protection Directive in most situation*"[10].

It is also the only way to reinforce European consumers/citizens' confidence in adopting RFID technology. In fact, in a recent survey on RFID carried in the Netherlands, 57% of consumers believe that unauthorised persons will probably gain access to databases[11] and 50% have little or no confidence in businesses dealing carefully with RFID generated personal data[12]. An opt-out solution would go against what European citizens want and would be totally unacceptable.

For more legal certainty though, the wording of article 7.3 (a) should be changed to "[…] explicitly chooses to keep the tag operational".

There is no cost justification to rule out the opt-in approach as whether the regime chosen is opt-in or opt-out, the same infrastructure (i.e. the same investment) is needed to allow for "immediate" deactivation. The price of automatic deactivation is a grain of sand compared to the overall costs of building and implementing a fully functioning RFID infrastructure (from the warehouse, to buying RFID readers and tags…, to the back-end system).

Nevertheless, as pointed out by many, including the EDPS[13], a RFID tag raises potential data protection, privacy and security concerns outside a specific RFID application – especially since the tags used in retail are totally unprotected. For instance, where a specific RFID application does not involve processing of personal data, it does not mean that once the consumer has left the store, no one will be able to read the unique RFID identifier on the products he or she is carrying around. For instance, the person seating next to you in the bus could find out that you have these famous little blue pills in your bag or what the brand and size of your underwear are. This is why, when the tag remains operational after the point of sale, consumers must also be protected - using encryption for instance. In this context, we fully support further R&D on "privacy and security by design".

We believe that, for the next three years, the current text is a reasonable compromise that will allow some protection while not entirely resolving the issue of protection of personal data, privacy and security in a RFID environment. In the meantime, further reflection on how to better protect consumers from unwanted reading of his/her RFID tags is necessary to ensure consumers will gain benefit from using RFID technologies.

Article 7.4

We fully support that deactivation or removal of tags by the retailer is "immediate"[14], "free of charge" and can be verified by the consumer.

Further to legal obligations, it should be added that the purchase or any purchase advantages (e.g. contractual guarantee) may not be conditional to the consumer keeping the tag operational.

Even where no risk to privacy has been found, the burden to deactivate should not be put on the consumer as he/she would most certainly not know where the tag is and how to proceed. The current text in Article 7.3 (b) states that "*the retailer must provide an easily accessible facility to deactivate or remove the tag*" thus implying that consumers

---

10 European Data Protection Supervisor opinion on the communication of the European Commission on RFID, December 2007.

11 Consumentenbond, the Rathenau Institute, ECP.NL survey 2007.

12 Consumentenbond, the Rathenau Institute, ECP.NL survey 2007.

13 European Data Protection Supervisor opinion on the communication of the European Commission on RFID, December 2007.

14 Consumers should not wait and queue again after the point of sale to have the tags on the products they bought deactivated.

should deactivate tags themselves. This is in contradiction with Article 7.4 that requires tags to be deactivated "*by the retailer*" "*immediately*".

Article 7.5

The review of the provision of article 7 is to be welcomed. Automatic deactivation (i.e. opt-in) on all items at the point of sale is certainly a political choice that we wholeheartedly back. R&D on privacy enhancing technologies (PETs) and on tags that can be deactivated and reactivated[15] by an authorised party should be supported.

In general, we regret the lack of requirements for user-friendliness in relation to RFID tags. RFID-technology's use should be simple for consumers. In the future, the user should be able to intuitively manage and understand the opt-in and opt-out options and gain complete control over the daily use of the technology.

Article 8

1. Member States, in collaboration with industry and other stakeholders should take appropriate measures to inform and raise awareness among companies, in particular SMEs, on the potential benefits associated to the use of RFID technology. Specific attention should be placed on information security and privacy aspects.

2. Member States, in collaboration with industry, consumer associations and other relevant stakeholders, should identify and provide examples of good practice in RFID application implementations. They should also take appropriate measures, such as large-scale pilots, to increase public awareness of RFID technology, its benefits and implications of use, as a prerequisite for wider take-up of this technology.

Article 8 - **Awareness raising actions**

We support this proposal as awareness raising actions are necessary to inform all the players – be it tag developers, employees, SMEs, all the companies down the supply chain, and consumers – about the potential benefits and threats of the use of RFID technology.

Awareness raising campaign should be balanced, fit the level of understanding of the public it wants to reach and inform about the various uses, benefits and risks of RFID technologies.

We believe, however, that examples of "*good practice in RFID application implementations*" should be aimed at professionals rather than at consumers.

Article 9

Member States should cooperate with industry and the Commission to stimulate and support the introduction of the 'security and privacy by design' principle at an early stage of the development of RFID applications, in particular through the development of high-performance and low-cost solutions.

Article 9 - **Research and Development**

We fully support R&D on "*security and privacy by design*" as we do believe that it would foster consumers' acceptance and trust in RFID technology. In addition, a reference to

[15] Tags that can be switched on and off already exist (EPC Gen 2 tags - electronic article surveillance function -http://www.rfidjournal.com/article/articleview/3818/)

research on Privacy Enhancing Technologies (PETs) – in accordance with the Commission's communication promoting PETs[16] – should be added.

Article 10

1. Member States should inform the Commission 18 months from the publication of this Recommendation in the Official Journal of the European Union of action taken in response to this Recommendation.

2. Within three years from the adoption of this Recommendation, the Commission will provide a report on the implementation of this Recommendation and its impact on economic operators and consumers, in particular as regards the measures recommended in Article 7. Where appropriate, the Commission shall amend this Recommendation or submit any other proposal it may deem necessary, including binding measures, in order to better achieve the goals of this Recommendation.

Article 10 - **Follow-up**

We welcome the commitment of the European Commission to report on the implementation of this recommendation. Nevertheless, given the rapid development and growth of RFID technologies, we believe that the Commission should produce two years after the publication of this recommendation, a report to be presented to the European Parliament and the Council.

In addition to focusing on Article 7, the report should also focus on the application of Article 5 on information of RFID use.

Article 11

This Recommendation is addressed to the Member States and to all stakeholders which are involved in the design and operation of RFID applications within the Community.

Article 11 - **Addressees**

We support the fact that the recommendation is aimed at both Member States and stakeholders.

Participants to this consultation who are interested in submitting additional comments that are not directly linked to a given article but rather cover the entire Recommendation or that fall outside of the suggested articles are invited to do so hereunder.

[16] COM(2007) 228.

- **Additional comments**

European ethics committee

A European committee dealing with ethics should be created and consulted ex-ante on any RFID technologies applications raising potential ethical risks.

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

Standardisation

We call for the application of good governance principles. 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.

END