Comments and Responses by FoeBuD for the EU Consultation on RFID, April 2008

Article 1 - Scope

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.

Comments / Responses by FoeBuD

- The Recommendation must not only address how RFID technology may be introduced, but also whether it may be introduced at all.
- RFID technology must not be introduced if its threats to society cannot be eliminated. No residual risk, however small, must remain.
- The previous discussion in connection with the first EU consultation on RFID discussed problems and risks mainly in relation to individuals. But there are further risks to society as a whole.
- Foremost in this respect is an emerging concentration of power through information. RFID is an information collecting technology. Possessing information is becoming increasingly synonymous to having power. A social debate is overdue on whether or

FoeBuD e.V., Marktstraße 18, 33602 Bielefeld, Deutschland
Tel: +49-521-175254, Fax: +49-521-61172, mail@foebud.org
Donations: 2129799, Sparkasse Bielefeld, BLZ 480 501 61

not such power is desirable in today's society, and whether this power needs to be restricted in order to maintain a balance and protect civil rights, and in what places and to which extents such restrictions are necessary.

- Point 3 contains a double negative.
- Point 3: The recommendation must also apply to activities outside the mentioned scope. The field of so-called security is especially prone to being abused as a backdoor for introducing undesirable technologies.

Article 2 - Definitions

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.

Comments / Responses by FoeBuD

- The definition of “monitoring” must be extended to consider that activities carried out for purposes other than those mentioned in paragraph (g) can “acquire” one of the mentioned purposes, e.g. if data is recorded and used at a later time (shifting of purpose over time).
- The definition must distinguish between RFID chips being deactivated permanently and irreversibly (“destruction”) or in a way that facilitates reactivation at a later time (“deactivation”).

Article 3 - Privacy and Data Protection measures

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.

Comments / Responses by FoeBuD

- Instead of “should”, the word “must” must be used.
- 1.: Such a privacy impact assessment is a mandatory requirement.
- 1.: The condition at the end must be extended to say, “[monitor an individual] directly or indirectly”.
- 2.: The experience of a round-table “partnership” at the German Federal Ministry of Economics and Technology has shown that there seems to be little interest in transparent cooperation with relevant stakeholders. Just as declarations of “voluntary commitment” by the industry have had a limited shelf-life in the past, the current draft does not show how this point, well-meant as it may be, would actually be enforced – but experience has shown that enforcement is a necessity.
- 3.: Mitigating these risks is a good intention, however there is no basis for evaluating whether the risks have been sufficiently reduced. To establish such a basis and ensure relevant support in society is a task that, among other institutions, the EU could undertake. Risks must not only be mitigated, they must be eliminated.
- It must be ensured that no person-relatable data is created, not even through combination with further data.
- 5. must be amended: “The RFID application operator should align the privacy impact assessment *to reach or exceed the standards established by* the overall information security risk management set out in Article 6 here after.”

FoeBuD e.V., Marktstraße 18, 33602 Bielefeld, Deutschland
Tel: +49-521-175254, Fax: +49-521-61172, mail@foebud.org
Donations: 2129799, Sparkasse Bielefeld, BLZ 480 501 61

- Add the following paragraph: The impact assessment and any accompanying documents must be made freely available for public evaluation. There must be opportunities to correct problems and deficiencies even after the RFID application has become operational.

Article 4 - Codes of Conduct

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.

Comments / Responses by FoeBuD

- Again, “should” must be changed to say “must”.
- 1.: Effective penalties for violations of these codes of conduct must be established.
- 2.: Instead of “encourage”, the word “prescribe” must be used.
- 3.: The “relevant national supervisory data protection authorities” and institutions must be given adequate funding for their tasks, and their independence must be safeguarded. They must be given powers to impose effective penalties against non-

compliant RFID applications.

Article 5 - Information on RFID use

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.

Comments / Responses by FoeBuD

- Again, “should” must be replaced by “must”, and “personal data” by “person-relatable data”.
- 1.: Before data are collected and recorded, explicit, written permission must be obtained.

- The specific situation that collection of the data does not require a line-of-sight connection must be pointed out.
- Alternatives and protection measures must be mentioned.
- The policy must be written in a neutral, rather than euphemistic, style. The display must be readable in terms of font, size, and colour.
    - (a): An email address must be included.
    - (c), add: and what links to person-relatable data can be made by combining the processed data with data from other sources.
    - (f): All identities and addresses, including email, of third parties that access the data or provide other services, must be given.
    - New item (g): How long the data is stored.
- 2.: Not only the fact that information may be broadcast without an individual engaging in any active action, but also that there is no visible indication of this broadcast must be pointed out.
- The words “where appropriate” must be deleted.
- The clear sign must follow the standard of a hazard symbol and not be euphemistic.
- The points in 1. (a)–(g) apply here as well.

Article 6 - Information security risk management

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.

Comments / Responses by FoeBuD

- Replace “should” with “must” as before.
- 1.: The security measures must be adapted to technological and social developments at appropriate intervals.
- 2.: The round table meetings at the German Federal Ministry of Economics and Technology, which are supposed to be “in partnership”, have shown little interest in a transparent cooperation with relevant stakeholders. Just as declarations of “voluntary commitment” by the industry have had a limited shelf-life in the past, the current draft does not show how this point, well-meant as it may be, would actually be enforced – but experience has shown that enforcement is a necessity. Relevant sanctions must therefore be established.
- 3.: To merely “encourage” is not enough. An “appropriate level of privacy and information security” must be proven by operators – before the application is put into operation, during, and after its use (the latter may need to include a certified proof of data deletion). Data protection authorities must be able and obliged to perform checks of protection measures at any time and without notice (data protection audit).
- Delete “strive to”.
- Add: “An exit strategy should be provided, such as bar codes, 2D/3D bar codes etc.”

FoeBuD e.V., Marktstraße 18, 33602 Bielefeld, Deutschland
Tel: +49-521-175254, Fax: +49-521-61172, mail@foebud.org
Donations: 2129799, Sparkasse Bielefeld, BLZ 480 501 61

Article 7 - RFID use in retail

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.

Comments / Responses by FoeBuD

- As before, “should” must become “must”, and “personal data” replaced with “person-relatable data”. In paragraph 4, “should not” must be changed to “may not”.
- 2.: The sign must depict the risk appropriately, and not be euphemistic. Alternatives must be pointed out; these must be made easily accessible by the operator or applied automatically.
- Instead of “harmonised”, the sign must be “standardised”.
- Third item: delete “likely reasonable”.
- 3 (a) (add at end): It is the operator’s obligation to carry out the deactivation before public areas (such as sales rooms) are reached, in an automatic and verifiable way.
- 4.: In “should not entail any reduction”, change “should” to “must.
- 5.: Citizens must not be subjected to any extra effort as they avoid the use of RFID (such as longer queues because only one non-RFID checkout is available).

Article 8 - Awareness raising actions

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.

Comments / Responses by FoeBuD

- 1.: Information must not be biased to communicate only potential benefits. Potential risks must be described in a balanced and non-euphemistic way. The term “potential benefit” must therefore be replaced with “potential risks”.
- 2.: Delete this paragraph in its entirety.

Article 9 - Research and Development

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.

Comments / Responses by FoeBuD

- Not just the industry and the Commission, also NGOs / groups of concerned citizens must be given a part in the cooperation. This includes a budget to finance necessary fees and expenses.
- The cooperation must also focus PET (Privacy Enhancing Technologies) as well as opportunities of creating inexpensive and functional applications without the use of RF technology.
- The development of appropriate verification and audit measures as well as technology and privacy assessment schemes must also be encouraged.

Article 10 - Follow-up

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.

Comments / Responses by FoeBuD

- The reporting process must also include all stakeholders from industry and society.
- Reporting must still focus not only how RFID may be introduced, but whether it may be introduced at all.

- RFID technology must not be introduced if its threats to society cannot be eliminated. No residual risk, however small, must remain.

Article 11 - Addressees

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.

Comments / Responses by FoeBuD

All participants in the follow-up process (after 18 months, according to Article 10) must also be named as addressees.

Additional comments by FoeBuD (12)

- Any measures must be financed not just be the legislature, but mostly by existing and aspiring operators in analogy to the “Polluter Pays Principle”.
- All occurrences of “should” must be changed to “must”.
- Where “personal data” is referred to, the term “person-relatable data” must be used. This is what is meant by “personal data”, but the term does not seem to communicate this fact clearly enough to most people.