

ISSUE PAPER

Consumer concerns on potential harmful applications around RFID BEUC

I) Problem definition

We recognise that RFID could be a technology beneficial to business management, environment and can offer consumer benefits such as helping product traceability. However, we are concerned about the negative impacts it will have on personal privacy (tracking and profiling of consumers, consumer discrimination), security (ID theft) and ethics.

As time passes by and costs decrease, this technology will be a real threat to consumer privacy. There is a risk that in the future consumers be constantly under surveillance, profiled and have their every move analysed. Indeed the information potential is theoretically limitless.

RFID tags may lead to the indirect identification of consumers through the combination of tags of several items of purely goods-related data with personal information contained on credit cards, loyalty cards, even bank notes in a near future, can deliver a certain customer profile.

It is of utmost importance that consumers are aware about RFID tags and readers around them. Consumers must have the possibility to know when, where and why an RFID tag is being read and what kind of information is generated via the readers and stored in their tags.

Consumers must have the choice to decide whether they want RFID or not. Purchasers of products containing RFID tags should have a possibility to have embedded RFID tags removed, deactivated, or destroyed.

RFID is a technology in transition. It is therefore important from the very beginning to take account of and address the potential risks of this technology and its development at a global level.

II) Objectives

The workshop “Consumer issues – data protection, privacy and security” shall provide a platform in order to discuss relevant consumers concerns about the possible harmful implications of RFID technology and how the development of RFID tagged products would affect consumers.

III) Policy options

Legal options

Before even considering the introduction of RFID tags linked to personal information or profiling consumer, one should first consider alternatives that achieve the same goal without collecting personal information.

These comments are only preliminary and do not represent an official position of BEUC. BEUC reserves the right to adjust and submit a more comprehensive position at a later stage.

The right to privacy is a fundamental right that must not be taken away just because it becomes easier or profitable to do so. Companies using RFID devices should – at the very least – fully respect existing legislation. They must fully comply with the EU Data Protection and the E-privacy Directives and with privacy guidelines. Existing directives relating to privacy and data protection should be analysed to see whether they adequately address the privacy risks that the applications of RFID present for consumers in different contexts and sector and be reviewed to take fully account of those risks. Individual Member States surveillance of the respect of the relevant rules on data and privacy is crucial.

The basic principles of consumer protection law must apply to RFID technology. The issue of consumer awareness needs to be addressed and it is important to reflect on how to best provide consumers with information on this new technology (campaign, labelling...).

It is important that appropriate legislation deals with RFID and that it is not left to industry self-regulation alone. Codes of conduct can only supplement but not replace the legal framework, especially when subjects as crucial as privacy and security are concerned. Involvement of all stakeholders – including consumer organisations- when drafting guidelines is necessary.

It is equally important to monitor whether RFID is being used in anti-competitive ways. For instance, the use of RFID in applications that control the use of products or force consumers to use products that are more costly would restrict consumer choice (tie-in products) and consequently impact competition.

The legal analysis of the Data Protection Directive carried out by the Article 29 Data Protection Working Party is essential.

- The Article 29 Data Protection Working Party Working Document on Data Protection Issues related to RFID Technology (WP 105, http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf),
- BEUC answer to the Art.29 Working party consultation on RFID: <http://www.beuc.org/1/GJMPNNJCHOMKGLAFFKEGCGMGPDB19DB62D9DW3571KM/BEUC/docs/DLS/2005-00350-01-E.pdf>
- OECD (2004) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html
- International Conference of Data Protection & Privacy Commissioners (2003) "Resolution on Radio-Frequency Identification Technology": <http://www.privacyconference2003.org/resolutions/res5.DOC>

Technical options

There is a need to reflect on the development of technical solution models that would ensure that consumers have control over their own personal data ("privacy mode"). Privacy protection could be incorporated technically into the RFID tag itself.

The distinction between 'active' and 'passive' tags, how they work, their use and their respective impact on consumers would also need to be considered.

IV) Analysis of impacts

See TACD resolution on RFID available at:

<http://www.tacd.org/cgi-bin/db.cgi?page=view&config=admin/docs.cfg&id=274>

These comments are only preliminary and do not represent an official position of BEUC. BEUC reserves the right to adjust and submit a more comprehensive position at a later stage.

V) Comparing the options

xxxx