

EABC response to the European Commission's Draft Recommendation on the Implementation of Privacy and Information Security Principles in RFID Applications

April 25 2008

INTRODUCTION

- Consumer concerns exist regarding information privacy and security that are directed at RFID technology. Most of these concerns are in-fact not specific to RFID – but rather generic privacy & security concerns.
- In the majority of current RFID applications, there are no data protection concerns because the tags do not store or communicate personal data, and are not linked to an identifiable individual.
- Concerning the range of consumer perceptions and concerns, there are in fact numerous existing technology and market protections that address them. These technology protections, developed by industry and used throughout the marketplace, and policy guidelines – developed by international, European, and national authorities – are comprehensive and adequately address consumer concerns. Examples include the UK Information Commissioner's Office August 2006 publication of Data Protection Technical Guidance for RFID, as well as cooperation between NXP and the German Federal Office for Information Security (BSI) in establishing joint technical guidelines for the secure implementation and utilization of RFID, to be deployed throughout Germany.
- Moreover, beyond these market protections and official guidelines, there is an existing, comprehensive legal environment that clearly regulates the process of personal data and serves as both a deterrent to the misuse of RFID or of any technology and as a means of redress. The EU Data Protection framework, including the Directive 95/46/EC and national data protection laws implementing the concerned Directive, especially create a coherent and extensive framework for protection of individuals with regards to the processing of personal data and to the transfer of such data. This legal framework is technology neutral, and covers RFID technology.
- Considering that a robust set of market protections exists and is working within an existing legal environment the policy approach on RFID should:

Promote Innovation: Any kind of regulation or legislation must be based on a thorough understanding of the RFID technology focusing on responsible use and not stifle growth and investment in a vital yet still burgeoning technology with global applications.

Encourage Market Solutions: Industry respects and protects the consumers need for privacy and security and is invested heavily in voluntary market-based solutions to the issue. Industry, consumers, and governments have already worked together to develop secure, effective RFID systems that protect private information. This kind of initiative should be promoted.

Focus on Enforcement of Existing Laws: Policy makers are successfully protecting consumers through existing privacy and security laws. Therefore, the focus should now be given on resources for the enforcement of those laws in general, and specifically, as it applies to RFID technology.



EABC appreciates that the Directorate General for Information and Society of the European Commission (DG INFSO) has granted the opportunity to submit comments related to the Draft Recommendation concerned. While EABC will, therefore, provide comments through the on-line consultation, we also want to provide a more consistent and structured response that address issues of interpretation and application of RFID policy and technology.

EABC agrees especially with the European Commission to recognize, in Article 1 of the Recommendation, the applicability of Directive 95/46/EC (hereafter called the “Data Protection Directive”) to the RFID technology. The Data Protection Directive, and national data protection laws implementing the Directive, provides a coherent and extensive framework for protection of individuals with regards to the processing of personal data and to the transfer of such data. This legal framework is technology neutral, and covers RFID technology. In this respect, EABC welcomes the efforts of the European Commission to provide with the Recommendation guidance on privacy and security aspects of RFID use. However, the Recommendation should be general and provide guiding principles on aspects that are directly related to RFID, rather than detailed guidance, in order to allow for flexible and innovative solutions.

In this respect, we are, therefore, concerned by the breadth and the lack of clarity of a number of the definitions in Article 2 that sweeps in tags not including personal data. Monitoring for example, refers to “*movement... or state of an individual*” as opposed to an identified or identifiable individual. The fact that a reader or portal might be able to discern the movement of an object because a person in motion is holding it, but have no other tie to the person’s image or identity should not be considered a privacy issue. This issue is again evident in Para 1 of Article 3 where the reference is to individual, rather than identified or identifiable individual. Interestingly, Para 3 of that Article does make reference to an identifiable natural person.

The inclusion of the back end systems in the context of “*RFID application*” is also overbroad. RFID does not substantially change the way that information is used or stored today. An RFID system is composed by the tag, the reader and an interface application between the reader and communications or back end software. More general network, communications, software, and other backend systems are not part of the RFID application, but rather communicate with the RFID application. Furthermore, the definition of the “*RFID Application Operator*” is also too broad and not appropriate and at the end creates uncertainty. While all of the persons/organizations listed play a role in ensuring privacy for a single RFID application, all do not have the same obligations, control or associated risk related to data protection. There needs to be more granular and context sensitive treatment of the various actors in a RFID development and deployment in order to assure that requirements are commensurate with obligations and risk. In addition, the fundamental differences between operators of a technology and developers or implementers should be recognized.

Furthermore, the definition of “*deactivation*” is unclear. Deactivation can not only mean destroying a tag. It is not adequate as the protection of privacy does not require the cessation of all or “*any*” functionality. The definition of deactivation needs to take into account that an RFID tag could include different functionalities that have no impact on privacy or security.



EABC welcomes the self-regulatory approach put forward in Article 3 in view of ensuring an open, transparent and responsible deployment of RFID. Provided the rewording of the definitions in Article 2 as explained above, Article 3 especially provides useful guidance for the risk assessments and Privacy Impact Assessments to be performed by RFID Application Operators. However, they should be considered in context and that certain sectors may need to customize the privacy impact assessment's tools to suit the risks that may be present in their particular uses of RFID. They can only be made responsible for their own data security measures in order to prevent the malicious use of data by third parties. Accordingly, the privacy impact assessment can not cover the sole possibility of an unauthorized third party linking RFID data to a natural person. Only appropriate data security measures on the part of the operator can be subject of the privacy impact assessment. In addition, the key element should be "*the reasonable likelihood of linkage*" and not where it "*cannot be excluded*" that data will become potentially personal. Furthermore, standard assessment documents and processes may need to better take into account the policy and technology methods of risk mitigation and privacy protection that may be available in relation to RFID. Users of such tools would also need to take into account policy controls relate the association of previously collected or related information to product/tag information.

While industry can readily agree with the self-regulatory approach, Article 3(6) raises several concerns. EABC appreciates the need to assure the public that information is being used responsibly, that companies remain accountable for their actions and that they use transparent processes. That being said, concern is raised by even comprehensive summaries of these instruments for fear that they may provide insight on how to compromise systems because they tend to identify infrastructure elements or provide visibility into security architecture. A possible compromise methodology might be to work with sectoral associations that may assure that processes were undertaken and that findings were consistent with appropriate protection. This may be worked in conjunction with the codes of conduct suggested in Article 4. Clarification on the extent and content of the summary to be made available is anyhow needed.

The promotion of the codes of conduct in Article 4 is highly appreciated. However, in order to facilitate the review process by the data protection authority concerned, we would suggest that broader roles for private sector intermediaries, that provide leverage to such authorities, need to be considered. The good work that has been done in relation to Binding Corporate Rules is an example of the strain that most of these authorities are under. The potential benefits of current RFID technologies and future sensor-based technologies to the economic growth and competitiveness of the EU should not be unduly delayed in deployment because of insufficient bandwidth in the review process. In addition, the Recommendation should recognize that international codes of conduct for the privacy-friendly operation of RFID already exist and are followed by RFID application operators. The introduction of national codes of conduct risks creating new burdens in the EU internal market.

The provisions set out in Article 5 reflect the principle of good information to the individuals established by the Data Protection Directive. However, when read in conjunction with some of the concerns related to the definitions in Article 2, these provisions create significant problems of interpretation and may result in significant consumer confusion. For instance, the broad definition of "*public space*" would create huge implementation problems, as transportation of RFID tagged shipments on public roads could be seen as "*application in public space*", therefore positioning internal supply chain processes within the scope of the recommendation. While providing the identity and address of the RFID application operator in accordance with Article 5(1)(a) seems reasonable it may also not be helpful in light of the fact that the definition would require identifying the parties related to development, implementation, use, or maintenance of application that is defined to include tags, readers, backend

systems and network communications. Furthermore, different products may have different people involved in development and maintenance that would preclude the possibility of addressing multiple products in a policy. The practical impact of these requirements needs to be considered to evaluate both the potential unnecessary burdens they create as well as the possible unintended consequences of confusion that could result. A further complication and unintended consequence may also be that with the development of more distributed application, the inclusion of “users” in the definition of operators might have implications for consumers who may be able to program some RFID applications in their home. Besides, Article 5 fails to address the aspect of shared responsibility for a RFID application and potentially creates a burden along the process chain that could reduce the benefits of RFID. In addition, if there is no link to personal data and no personal data stored in the tag what level of application of requirements is needed? The negative implication of Article 5(1)(d) is that compliance with all other requirements would still be expected, yet may not be proportionate in light of the potential threat to personal information.

Article 5(2) and Article 7(2) begin to recognize some of the practical limitation of notice related to RFID. It is clear that some form of symbol-based approach will be needed to address this issue, since even short notices which have been endorsed by a number of Data Protection Authorities are not a viable solution at a per product/tag level. This practical issue related to accomplishing notice is directly related to the problem of providing choice. While a symbol based system may provide at least some of the notice requirements outlined, and a link or way to get more information, notice about choices available related to information collection are much harder to develop. This is a threefold problem. First, there is the issue of how to describe the multiple choices that may be related to information collection, use and sharing. Next an issue arises on how to effectively convey any associated benefits, risks or mitigation related to the choices; and finally how to provide notice related to management of choice. Future developments may enable portable devices (smart phones, PDA etc) to have readers embedded that provide some of this functionality, but for now we are mostly limited to the interaction between a symbol based notice and some form of policy, most likely web-based. Some have suggested that some of this functionality may be provided at the point of sale terminal but that would create unacceptable delays for consumers at check out since not all items will have the same policies or requirements.

Article 7 raises also several practical problems, related especially to deactivation. Article 7(1) creates enormous interpretation problems and brings significant complexity, cost and uncertainty in the national and international supply chains with negative effects not only for retailers but also for manufacturers, logistics providers and the entire RFID industry. There is also no justification why retailers not using RFID technologies are subject to Article 7. The Recommendation fails to take into account impact assessments as well as measures to be put in place to safeguard data protection and privacy by the retail RFID application operator. The focus on opt-in deactivation (deactivation by default) as the only measure to protect privacy is not justified nor legally required. The decisive element should be whether the tag itself contains personal data or not. The current provisions go beyond this distinction.

Opt-in approach as stated in Articles 7(3) and 7(4) is not economically feasible nor operationally viable. The Recommendation should not be so detailed as requiring the method of deactivation and it should allow practical differences between easily removable tags and those which are not. Opt-out solutions (at request of the consumer) after the point of sale without undue burden to the consumer strikes the right balance between high consumer protection and the possibility to viably carry out the RFID application, while assuring consumer empowerment. In addition, Article 7(4) shall provide for a **clear exception from deactivation for tags that are necessary for the functioning of the product or**



product life cycle, so that certain critical benefits inherent to the product are not lost. In this respect, particular attention should be given to the private sector and civil society organizations, which have already been conducting work on possible codes of policy and practice to address the deactivation issue led by the International Chamber of Commerce Principles for Responsible Deployment and Operation of Electronic Products Codes, EPCglobal Guidelines for Consumer Products, The Center For Democracy and Technology (CDT) Privacy Best Practices for Deployment of RFID Technology, and the Electronic Privacy Information Center (EPIC) Guidelines on Commercial Use of RFID Technology.

Article 7 (5) and Article 10 are predicated upon a three year opt-in trial on the assumption that consumers will demand deactivation by default as a general rule. In absence of mass deployment and real consumer exposure to retail Item level tagging, this provision is not justified.

EABC welcomes the measures to raise awareness among individuals, companies (in particular SMEs) on the potential benefits of RFID. Awareness about RFID is extremely low among people, and many misconceptions and fears expressed in the media can be overcome by supporting information and education programs on RFID. EABC is ready to contribute as much as possible to this information campaign.

CONCLUSION

There are many current and potential examples of the societal benefits of RFID including: product food safety recalls; ensuring the use of genuine products to build and service airplanes; sustainable consumption to help take end of product cycles into account; transforming global transportation and logistics to improve security, reduce loss and theft, and streamline more sustainable cargo processes; protecting and securing global ports; making logistics more efficient; and improving inventory and stock control to manage assets.

However, the vast majority of those current RFID applications operates at a business-to-business level and deal with logistics and inventory management. These applications do not present privacy issues as RFID in the pre-point-of sale space are not associated with an individual and only contain product information (most likely a unique identification number). RFID in these types of application continue to feed into the same logistics and supply chain applications, which are usually controlled by the owner of the supply chain. In that sense they provide no further intelligence across participants to that supply chain, unless the system owner/operator so desires. New strict rules for all RFID applications with no relation to the specific privacy risks incurred and failure to appropriately take into account of technology and policy based solutions could, and often do, result in unintended consequences. Such unnecessary burdens could impair innovation in and deployment of beneficial applications of RFID technology.

Therefore, provided that the above comments and concerns are taken into account, EABC welcomes the Recommendation guidance on privacy and security aspects of RFID use, which should give legal certainty to the industry while ensuring privacy to individuals. The Recommendation should bring the legal framework ensuring further deployment of RFID technology applications for the benefits of the industry and of the society alike.

For more information, contact:

Alexis Serfaty, Policy Director: 202.828.9103 or Alexis@eabc.org

Jan Barnes, Europe Director: +32 (0)2 513.38.72 or Jan.Barnes@eabc.org

www.EABC.org