

**Information Technology Association of America • European-American Business
Council • Food Marketing Institute • Grocery Manufacturers Association •
Healthcare Distribution Management Association • National Association of
Manufacturers • National Retail Federation • Retail Industry Leaders Association •
United States Council for International Business**

April 25, 2008

Commissioner Viviane Reding
Information Society and Media Directorate General
Member of the European Commission
BE-1049 Brussels
Belgium

Dear Commissioner Reding:

We appreciate the opportunity to comment on the draft recommendations concerning radio frequency identification (RFID) provided by the Directorate General for Information and Society of the European Commission. While many groups will provide comments through the on-line consultation, we want to provide a more consistent and structured reply to the draft recommendations.

The use of RFID technology offers significant societal benefits in many areas including ensuring: supply-chain efficiency; the potential for accurate tracking of pharmaceutical drugs; authenticity of goods; safe handling of hazardous materials; food safety/recall; transport, security, logistics; and stock control. As the technology matures and applications continue to proliferate, RFID has the potential to enable global commerce and spur innovation and competitiveness, while providing significant improvements in safety and security. While the RFID debate in the United States and Europe has focused on privacy and security, RFID technology and applications that do not implicate personally identifiable information (PII) continue to mature and proliferate. The majority of RFID deployments exist at the 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 is not associated with PII and only contains product information.

We believe there is an existing legal environment that clearly and comprehensively regulates the processing 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 Directive 95/46/EC and national data protection laws implementing the subject Directive, especially creates a coherent and extensive framework for protection of individuals in regards to the processing of personal data and the transfer of such data. This legal framework is technology neutral and covers RFID technology.

In particular, we agree with the European Commission decision to recognize, in Article 1 of the Recommendation, the applicability of Directive 95/46/EC (the “Data Protection Directive”) to the RFID technology. The Data Protection Directive, and national data protection laws implementing the Directive, creates a coherent and extensive framework for the protection of individuals with regards to the processing of personal data and the transfer of such data. In this respect, we welcome the efforts of the European Commission to provide 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, Paragraph 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 overly broad. RFID does not substantially change the way that information is currently used or stored. An RFID system is composed of the tag, the reader and an interface application between the reader and communications or back-end software. More general network, communications, software, and other back-end systems are not part of the RFID application, but rather communicate with the RFID application. Furthermore, the definition of the “*RFID Application Operator*” is too broad and inappropriate and creates a degree of 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 not only means destroying a tag. Protection of privacy does not require the cessation of all or “*any*” functionality. The definition of deactivation needs to take into account that a RFID tag could include different functionalities that have no impact on privacy or security.

We welcome the self-regulatory approach put forward in Article 3 as a means of ensuring the open, transparent, and responsible deployment of RFID, assuming the rewording of the definitions in Article 2.

As explained above, Article 3 provides useful guidance for conducting the risk assessments and Privacy Impact Assessments to be performed by RFID Application Operators. However, they should be considered in context and recognize that certain sectors may need to customize the

privacy impact assessment's tools to match 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 cannot cover the 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 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 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 some concerns. We appreciate the need to assure the public that information is being used responsibly, that companies remain accountable for their actions, and that they are using transparent processes. That being said, concerns have been raised that even comprehensive summaries of these instruments 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 to ensure that processes are undertaken and that findings are consistent with appropriate protection. This may be done in conjunction with the establishment of codes of conduct as suggested in Article 4. At the very least, clarifications on the extent and content of the summary information to be made available is needed.

The promotion of the codes of conduct in Article 4 is highly appreciated. However, in order to facilitate the review process by the relevant data protection authority, we would suggest that broader roles be considered for private sector intermediaries that provide leverage to such authorities. 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 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 internal EU market.

The provisions set out in Article 5 reflect the principle of good information to individuals established by the Data Protection Directive. When read in conjunction with some of the concerns related to the definitions in Article 2, however, these provisions create significant problems of interpretation and may result in additional 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 the development, implementation, use or

maintenance of application that is defined to include tags, readers, backend systems and network communications. If there is no link to personal data and no personal data stored in the tag what level of requirements application 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 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 for subjecting retailers not using RFID technologies 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 or not the tag itself contains personal data. The current provisions go well beyond this distinction.

The 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 this respect, particular attention should be given to the private sector and civil society organizations, which have already been doing work on possible codes of policy and practice to address the deactivation issue led by the International Chamber of Commerce.

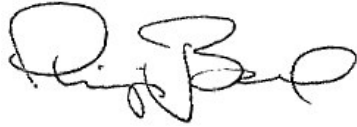
CONCLUSION

The vast majority of current RFID applications operates at a business-to-business level and deals with logistics and inventory management. RFID promises to enable innovation and competitiveness in manufacturing across the spectrum. 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 applications 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, we welcome 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 industry and society alike.

Sincerely,



Phillip J. Bond
President & CEO
Information Technology Association of
America



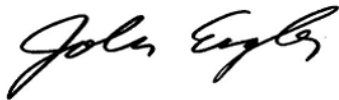
Michael C. Maibach
President & CEO
European-American Business Council



Sandy Kennedy
President
Retail Industry Leaders Association



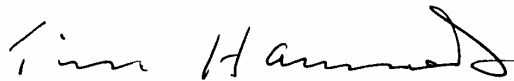
Peter M. Robinson
President
United States Council for International
Business



Governor John Engler
President & CEO
National Association of Manufacturers



Cal Dooley
President & CEO
Grocery Manufacturers Association



Tim Hammonds
President & CEO
Food Marketing Institute



Maureen Riehl
Vice President, Government & Industry
Relations Counsel
National Retail Federation



Scott Melville
Senior Vice President, Government Affairs
Healthcare Distribution Management
Association

cc: Dr. Gerald Santucci

About ITAA

The Information Technology Association of America (ITAA) is the premier IT and electronics industry association working to maintain America's role as the world's innovation headquarters. With the April 1, 2008 merger of the Government Electronics and Information Technology Association (GEIA), ITAA provides leadership in market research, standards development, business development, networking and public policy advocacy to some 350 corporate members. These members range from the smallest start-ups to industry leaders offering Internet, software, services and hardware solutions to the public and commercial sector markets.

About EABC

The European-American Business Council (EABC) is a Trans-Atlantic alliance of 70 multinational companies based in the US and Europe, dedicated to advancing Trans-Atlantic economic investment, innovation, and integration.”

About FMI

Food Marketing Institute (FMI) conducts programs in research, education, industry relations and public affairs on behalf of its 1,500 member companies — food retailers and wholesalers — in the United States and around the world. FMI's U.S. members operate approximately 26,000 retail food stores with a combined annual sales volume of \$680 billion — three-quarters of all retail food store sales in the United States. FMI's retail membership is composed of large multi-store chains, regional firms and independent supermarkets. Its international membership includes 200 companies from more than 50 countries.

About HDMA

The Healthcare Distribution Management Association (HDMA) is the national association representing primary, full-service healthcare distributors. Each day, the member companies of HDMA are responsible for ensuring that more than 13 million prescription medicines and healthcare products are safely delivered to 144,000 pharmacies, hospitals, nursing homes, physician offices, clinics, government and other providers in all 50 states. This essential public health function is provided with tremendous efficiency, saving the nation's healthcare system nearly \$34 billion each year. HDMA and its members are the vital link in the healthcare system, working daily to provide value, remove costs and develop innovative solutions to deliver care safely and effectively.

About GMA

The Grocery Manufacturers Association (GMA) represent more than 200 companies that manufacture and market branded and private label food and consumer packaged goods through retail, wholesale and foodservice channels of distribution. General members include retailers and foodservice companies that manufacture and market food and beverage products for sale.

About NAM

The National Association of Manufacturers (NAM) mission is to advocate on behalf of its members to enhance the competitiveness of manufacturers by shaping a legislative and regulatory environment conducive to U.S. economic growth and to increase understanding among policymakers, the media and the general public about the vital role of manufacturing in

America's economic and national security for today and in the future.

About NRF

The National Retail Federation (NRF) is the world's largest retail trade association, with membership that comprises all retail formats and channels of distribution including department, specialty, discount, catalog, Internet, independent stores, chain restaurants, drug stores and grocery stores as well as the industry's key trading partners of retail goods and services. NRF represents an industry with more than 1.6 million U.S. retail companies, more than 25 million employees - about one in five American workers - and 2007 sales of \$4.5 trillion. As the industry umbrella group, NRF also represents over 100 state, national and international retail associations.

About RILA

The Retail Industry Leaders Association (RILA) promotes consumer choice and economic freedom through public policy and industry operational excellence. Its members include the largest and fastest growing companies in the retail industry--retailers, product manufacturers, and service suppliers--which together account for more than \$1.5 trillion in annual sales. RILA members provide millions of jobs and operate more than 100,000 stores, manufacturing facilities and distribution centers domestically and abroad.

About USCIB

The United States Council for International Business (USCIB) advocates on behalf of over 300 members that are drawn from leading industrial and service companies in all sectors, and include major U.S. multinationals, law and accounting firms, and business associations.