Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

07-Feb-2006

English text only

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

DSTI/ICCP(2006)7
Unclassified

FORESIGHT FORUM "RADIO FREQUENCY IDENTIFICATION (RFID) APPLICATIONS AND PUBLIC POLICY CONSIDERATIONS": PROCEEDINGS

5 October 2005

This document contains the proceedings of the OECD Foresight Forum on Radio-frequency identification (RFID), held in Paris on 5 October 2005.

Contact: Karine Perset; tel: +33-1 45 24 19 83; E-mail: karine.perset@oecd.org

JT00200639

English text only

MAIN POINTS

1. The OECD ICCP Committee hosted the Forum on "Radio-Frequency Identification (RFID): Applications and Public Policy Considerations", in Paris on 5 October 2005. The event was part of the OECD "ICCP Foresight Fora" and attracted some 150 participants.

2. The objectives of the Forum were to:

- Provide the venue for an exchange of views and information between governments, experts from the business community and from academia, and civil society.
- Take stock of current and future RFID applications and their potential economic and social benefits; and
- Have a forward-looking policy discussion on critical issues raised by RFID, including infrastructure and standards, as well as security and privacy.

3. The morning sessions concentrated on current RFID applications and their business cases, on future applications foreseen and on RFID within the wider "Internet of things" or "ubiquitous Internet". The afternoon sessions were dedicated to discussing critical issues raised by RFID for policy makers, with perspectives offered from public, private, academic and non-governmental organisation(s) experts on standards development, privacy, and security.

The strong economic and social drivers for RFID applications create the prospect of an "Internet of things"

4. The economic and social drivers to adopt RFID are strong for certain types of applications and participants agreed on the potential of the technology to become pervasive in the long-term. Beyond RFID, a set of intelligent sensor technologies were predicted to enable "ubiquitous/pervasive computing" and the creation of an "Internet of things" that would bridge the physical and the virtual/information worlds, and ultimately enable "ubiquitous network societies". The notion of time utility to both companies and individuals, chiefly in the form of faster transactions, was mentioned by many participants.

"One size does not fit all" i.e. the wide variety of applications of RFID calls for differentiation

5. There is perception of a major difference between open loop applications, *e.g.* the open supply chain with Ultra High Frequency (UHF) Electronic Product Code (EPC) tags, and closed loop applications, such as contactless payment cards used within a closed payment system or inventory applications such as tracking reusable assets.

6. Within the open supply chain, the difference between use of RFID at pallet-level and use of RFID at item-level retail goods was further stressed. In the supply chain, clear economic benefits can already be demonstrated for pallet-level tagging on a case-by-case basis The use of RFID was said to relate to the transformation of the whole supply chain towards greater productivity and predicted to modify the dynamics of competition from enterprise-level competition to supply chain-level competition. However,

pilots for tagging of individual goods in retail environments suggested that economic benefits were probable only in specific cases and only with time, widespread adoption, and a virtuous circle of innovation in supporting technologies.

Implementation is at an early stage, and challenges remain

7. Although long-term and possibly short-term economic benefits are expected from adopting RFID in the supply chain, currently there appears to be unequal distribution of costs/benefits between actors in the supply chain. Challenges to implementation by manufacturers were raised by several participants. These included process re-engineering, developing a business case and obtaining return-on-investment, which for now was often an afterthought, whilst the drivers were often mandates by large retailers and governments, and regulations. Another challenge was dealing with the large volumes of data generated and ensuring data quality.

The deployment of RFID requires a coherent policy framework

8. The need was stressed for a strong multi-stakeholder partnership between industry, governments, and civil society to address new policy issues raised by RFID.

Global interoperable standards will be key to maximise the benefits of RFID

9. Global interoperable standards would avoid the costly past choices of different standards for different regions and maximise the benefits of the technology. Some participants further emphasised that standards should be open, similarly to the core Internet standards, so as to enable innovation "from the bottom-up" as key to future growth and prosperity. However, while EPCGlobal aims to provide royalty-free standards for RFID used in supply chains, the intellectual property (IP) policy of both EPCGlobal and ISO standards-making activities is based on Reasonable And Non Discriminatory (RAND) IP claims.

Demands for scarce and unlicensed spectrum will increase

10. Within the EPCGlobal context and for pallet-level tagging of goods, Ultra High Frequency (UHF) generates the most interest and there have been efforts to co-ordinate spectrum worldwide (Europe, Asia and US). However, issues remain for certain countries. Regarding the broader sensor environment, it was predicted that increasing amounts of spectrum would be required and that this should preferably be unlicensed spectrum.

There is a window of opportunity to integrate security and privacy by design into RFID applications

11. The parallel between RFID infrastructure and the Internet's infrastructure was made several times and participants particularly stressed the opportunity to build privacy and security into the RFID infrastructure (privacy and security by design) before widespread deployment, rather than having to deal with it afterwards, as has been required for the Internet.

Addressing privacy and security issues is a pre-requisite to widespread adoption of RFID

12. Integrating privacy and security by design in the conception of RFID applications was viewed by a majority as a key lever to ensure the widespread adoption of RFID and maximise benefits from this technology. Several participants stressed that not addressing privacy and security concerns would generate large-scale opposition by consumers and by individuals.

13. Many participants stressed the need to differentiate between applications that do not implicate privacy and security (including many of the business-to-business applications predicted in the short-term

future) and those that do. Regarding supply chain applications, uses of RFID before the point-of-sale (POS), where security is a main concern, should be differentiated from uses after the point-of-sale (POS), where both privacy and security are of concern.

14. Security experts stressed that RFID generates many new threats to security – including those of fraud/rogue parties accessing data – that the simple security technologies available were insufficient, and that efforts to effectively address security issues were only at their very beginning (*e.g.* in the case of the electronic seal standard). They added that additional research and development in light-weight security protocols, more sophisticated key distribution mechanisms, and different ways of using existing standards – including existing industry standards – were needed in order to provide necessary security as well as privacy. Some expressed the belief that security issues would be solved by industry because there was a business need for it and it was further noted that without security, confidentiality availability and integrity, RFID would not work for business or governmental use.

15. Regarding privacy, the various types of identities that could be associated with RFID were differentiated: person identity, service identity, and product identity. Several participants noted that there would be some trade-offs between privacy and other benefits – convenience, mobility, access to information, and personalised services. It was stressed that RFID privacy issues related to individuals, not just consumers, and that government applications of RFID were likely to be perceived as a greater issue than business applications of RFID. Others noted the technological challenge of enabling people to be in control of their privacy preferences and of the data associated with them.

16. It was also noted that current privacy protection frameworks might need to be refined and adapted to the context of an "Internet of things" that might enable data to be gathered and shared via general purpose collectors placed any and everywhere without straightforward ways to detect them. Such "electronic footprints" could be disseminated without the individuals' knowledge and/or consent, raising issues of notice, choice, purpose and access to data. While some technical limitations of RFID technology which currently provide *de facto* privacy protection were viewed as temporary, the use of Privacy Enhancing Technologies (PETs) was highlighted as one means to mitigate privacy risks. It was further noted that contactless cards (*e.g.* payment, identity, passports, transportation, loyalty) generate significant privacy and security concerns that are less present in contact cards.

The role of governments

17. Participants suggested that governments could play an active role in the development of RFID by participating in comprehensive policy initiatives. The examples of u-Japan (“u” for ubiquitous), u-cluster in Korea, the European Commission and the US RFID intergovernmental Forum were given. These various policy frameworks include: *i)* technical strategies including supply side elements such as network infrastructure and demand side elements such as applications in social security systems; *ii)* trials to identify challenges such as process redesign; *iii)* privacy protection and; i*v)* international co-operation. Suggested RFID-related policy matters in the realm of governments also included:

- Careful allocation of spectrum.
- Encouraging well thought-through government mandates for RFID implementation by suppliers in relevant areas.
- Promoting open standards.
- Considering the need for adapting national regulations, *e.g.* to address privacy concerns.
- Research and development to complement private sector efforts, *e.g.* on privacy-enhancing technologies.

- Addressing the health effects of a vastly expanded electro-magnetic environment.
- Addressing the impact of RFID and related technologies on employment (*e.g.* addressing job losses by re-training employees to perform other tasks than inventory checking) as well as on education systems (*e.g.* the need for more RFID-trained experts).

The role of the OECD

18. Participants suggested that given the OECD's past success in developing lasting guidelines/frameworks on privacy, security, and authentication, there was an opportunity to leverage existing OECD guidelines in a proactive way so as to stay "ahead of the curve" by helping to set ground rules in an "Internet of things", including principles that target the ways in which the technology is used, rather than the technology itself, and at the same time meeting the needs of multiple stakeholders by:

- Providing a forum where international awareness of the issues can be raised and promoting a "culture of security", extended to cover RFID.
- Providing guidance to evaluate the relevant OECD existing guidelines (privacy, security and cryptography) in a new environment.
- Possibly expanding OECD existing privacy guidelines to mandate transparency in RFID data collection.

19. Participants suggested that further input by the OECD could include:

- Formalising and sharing experience in the status of research and development, and deployments
- Providing guidance to governments on promoting the growth of use of RFID (*e.g.* Recommendation of the OECD Council on Broadband Development) and on following best practice in implementation
- Providing new metrics *e.g.* for measuring the impact of RFID on supply chains

REPORT ON THE ICCP RFID FORUM

Session 1: Welcoming remarks and introduction

20. The Forum was opened by **Hugo Parr**, Chair of the OECD Committee for Information, Computer and Communications Policy. He underlined that while RFID technology has been around for a long time, deployment until now has been hampered by lack of interoperability and by cost. He highlighted that RFID technology is important to the OECD, because its economic potential is so important that it can impact on economic growth, but that, in order to realise this potential, a number of issues needed to be addressed at the onset including: *i)* interoperability and *ii)* Privacy and data protection issues.

21. Mr. Parr concluded his remarks by emphasising that the OECD is ideally suited to strike the balance in the above-mentioned areas, because the organisation has credibility on the issues cited above with a wide range of stakeholders. He expressed the desire for the OECD to analyse these issues and to formulate guiding principles.

Session 2. Description of RFID technology and its potential

22. **Jonathan Collins**, European Editor of the RFID Journal and moderator for the session, introduced the session, to focus first on current applications in the key sectors which use RFID technologies to-date, including manufacturing, transportation and the pharmaceutical industry and to then cover possible applications, time-frames for implementation and likely socio-economic impacts of RFID.

2.1. Panorama of RFID current applications and potential economic benefits

23. **Dan Caprio**, Deputy Assistant Secretary for Technology Policy and Chief Privacy Officer, U.S. Department of Commerce, underlined that many RFID applications do not involve privacy and security problems and that a number of other RFID applications are based heavily on consent (as examples, he cited maritime applications or Quickpass). He indicated that the United States has set up an RFID intergovernmental forum for standards and regulatory issues, and that among other public agencies, the US Department of Defense (DoD) is using RFID for supply chain tracking.

24. Pointing out that a strong partnership between industry, government and civil society is required, Mr. Caprio stressed that privacy and security must be addressed at the beginning. He concluded that the OECD can play a forward-looking role in bringing all stakeholders – governments, the private sector and civil society – together to ensure an effective ongoing dialogue, evaluate societal impacts and favour the rapid and harmonious deployment of RFID.

25. **Naji Najjar**, Director of Wireless Broadband & Sensing Solutions, IBM Southwest Europe, stressed the need for governmental initiatives, open standards and public/private partnerships, to ensure adoption and beneficial usage of RFID. He gave an overview of IBM's activities relative to RFID technology, including: *i)* standards and patents; *ii)* using RFID in the semiconductor industry; *iii)* IBM's heavy investments in middleware to link RFID devices to IT system back-end applications and; *iv)* efforts by IBM in each geographical region to educate companies on RFID and its uses.

26. Mr. Najjar underlined that RFID provides the flexibility to track information from an end-to-end perspective, giving full visibility of activity in the physical world and potentially linking it to information technology systems, such as billing systems. He stressed that the bulk of business opportunities provided by RFID did not touch on privacy issues and that RFID, here to stay, is not just technology but rather involves process strategy and implementation, and safety and security. He believes governments and public organisations have a role to play in stimulating demand and use through well thought-through mandates and through ensuring that the necessary regulations are in place. He concluded that, independently of the technology itself, implementations needed to be based on open standards.

Panel questions

27. Q: **Jonathan Collins** asked how privacy had been dealt with in existing applications.

28. A: **Dan Caprio** replied that the US government-wide RFID council (set up to deal with policy formulation concerns, including privacy, security, standards, etc.) is well aware of the importance of addressing privacy and security throughout government applications and also understands the need, on the government side, to stimulate demand. The US Department of Defense (DoD) is imitating Wal-Mart by demanding that suppliers use it.

29. A: **Naji Najjar** replied that the bulk of applications which have large short-term potential are business-to-business applications – focussed on business processes, etc. – and mostly do not involve privacy issues. IBM is advising retailers on how they could implement item-level RFID and still respect privacy, but consumer cases are still to evolve.

2.2. Future applications, ubiquity of RFID and potential economic and social benefits

30. **Taiichi Inoue**, Senior Consultant - Head of IT for Society Consulting Group, Nomura Research Institute, Ltd., provided an overview of the Japanese Ministry of Information and Communications' (MIC) new proposed ICT strategy, "ubiquitous Japan", based on the development of mobile communications networks, RFID, sensor networks, etc. and on a vision to realise an ubiquitous network society in Japan by 2010. "U-Japan" is based on four pillars: *i)* Developing ubiquitous network infrastructure; *ii)* Advanced usage of ICTs (applying ICTs to the social security system, fostering the development of digital content, promoting standards design, improving the efficiency of the work force); *iii)* Trials to identify problems and issues; and *iv)* International and technical strategies.

31. Mr. Inoue outlined some of the outcome elements of RFID verification tests conducted over the last few years. He stressed some of the challenges yet to be overcome, including: *i)* Education of users and response to their needs, as RFID tags must generate benefits for customers at home; *ii)* Improving technology and systems; *iii)* Overcoming barriers related to process redesign (such as existing administrative or data entry and management tasks) and related to developing business models that generate cost reductions and find fair ways to apportion costs among stakeholders. Regarding privacy protection, in June 2004 the Japanese government introduced guidelines which aim to ensure freedom of choice.

32. **Indro Mukerjee**, Executive Vice President, Automotive & Identification business unit, Philips Semiconductors, provided an industry perspective on the potential of RFID. He emphasised that RFID is more than the supply chain – its many applications including healthcare and wellness. RFID also improves customer experiences and experienced-based services (*e.g.* by putting RFID into mobile phones for faster check-out and payment). Mr. Mukerjee stated that RFID could be the most pervasive electronic market ever and as such it deserves focus by governments and the OECD, about *how* it could realise this potential.

33. Mr. Mukerjee stressed the importance of standards and of education. He surmised that, considering the huge social and economic benefits, people will accept trade-offs in their concerns over privacy and security of data. In concluding, he called for more mandates from government and industry and for government, industry and civil society to collectively address consumer concerns. He also called on governments to stimulate further R&D work in complement to the large amounts invested by the private sector in this market.

34. **Elliot Maxwell**, Fellow of the Communications Program at Johns Hopkins University, offered to consider ways of thinking about RFID other than applications. He stated that the RFID is to be huge as it will allow an "Internet of things", with every object being able to communicate. Such an ability would provide access to information about the object, with the only limitation being the economics of data entry. This however raises the issues of the sheer volume of data that the objects and the readers will generate. He further stressed that strong economic and social reasons support the adoption of the technology.

35. Considering privacy and security issues, Mr. Maxwell stated that principles that have already been built for other uses should be built into RFID systems by design, rather than retrofitted. Mr. Maxwell brought up other challenges, including spectrum availability, the potential health effects of exposure to a more intensively used electromagnetic spectrum, as well as the impact on employment and the need to evolve educational systems accordingly. In concluding, he emphasised the importance of openness including open standards, interoperability and open innovation, the need for governments to take these into account while developing policy, and the role that OECD might play in refining existing privacy and security guidelines to take into account changes in technology and social and economic developments.

Panel questions

Rogue usage of RFID

36. Comment: **Joseph Alhadeff** noted that, with regards to the numbers of tags and their functionalities, in most situations the tags do not contain personally identifiable information. Personally identifiable information appears only when the tags are associated with a relationship, which implies a return to the situation in which a data controller is responsible to a party that has a relationship with a client – as in the supply chain. Consequently leverage still exists to control who has access to the database back-end information. He indicated that therefore the most pertinent issue was how to deal with fraud/rogue party usage.

37. A: **Elliot Maxwell** replied that this was true of the supply chain and that, while the information technology (IT) world was working hard to extend personal privacy preferences to travel with the data (sensors and associated data), it was also indeed wrestling with the issue of rogue parties accessing data. The ability to "kill the tags" which was included in the EPC standards was a good start but using the kill function undermined many important social uses such as recycling; the challenge to the technology community is to increase consumer choices such as being able to turn the chip on and off. He noted other challenges of a sensor-rich world: the vast numbers of the sensors, the persistence and malleability of the data, and its movement among various parties with the possibility of repurposing the data and matching it with personally identifiable information. This suggests the need to revisit the OECD guidelines and develop new solutions.

38. A: **Naji Najjar** replied that there are ways to allow consumers to be in control but that this subject needed further debate.

39. A: **Dan Caprio** added that there was an opportunity to build on the OECD privacy and security guidelines in a proactive way for RFID, rather than dealing with it afterwards as was the case with the Internet, in particular regarding architecture and design.

On robustness and accuracy of RFID

40. Question from the floor: Noting that most of the current RFID applications are not critical, a participant asked about the level of experience regarding the robustness of the technology, and about what could be done in terms of technology development and best practice to ensure the reliability of RFID applications.

41. A: **Najji Najjar** (IBM) replied that good progress has been achieved on the physical side, but that more work was necessary to improve the accuracy of reading. He added that each application needed to be looked at, case by case, and that in certain cases some process changes needed to be made in order to personalise the usage. He added that much work had been done on the integration of the data with the back-end, using robust middleware and integration with enterprise applications, such as messaging technologies, which are embedded in the middleware near the readers to enable a robust link with the back-end.

42. Question from the floor: A participant brought up spectrum allocation issues; including *i*) potentially detrimental interferences between devices in a dense environment of over a trillion radio-frequency devices; *ii*) the question of whether to license spectrum or to exempt certain spectrum bands from licensing; and *iii*) national and international co-ordination of frequency allocation.

43. A: **Elliot Maxwell**, acknowledging the importance of spectrum, responded that, in the EPC world, there had been efforts to co-ordinate spectrum bands worldwide (Europe, Asia and the US), so as to reduce the chip costs. He added, regarding the broader sensor environment, that more and more spectrum will be required. While stressing that governmental intervention and especially co-ordination is required, he suggested that the innovation that the United States has experienced in the unlicensed bands means that unlicensed provision of spectrum would be significantly preferable.

Session 3. Costs/benefits in different types of applications

44. **Richard Rees**, President, Scanology Group, Chair of the British Standards Institution Technical Committee "Automatic Identification Techniques" and moderator for the session, introduced the session's agenda covering a wide range of applications. He gave examples of the revolutionary effects of RFID, such as using UHF for returnable items or providing information not only on food but also on its transportation, and stressed that value-add per transaction is the key to both create better ways of doing business and new ways of doing business. He noted that drivers to implementation were often mandates and regulation, whilst return-on-investment (ROI) was more of an afterthought and that, while "defensive" applications including anti-theft and anti-counterfeiting were most prominent, "positive" applications were also being developed.

3.1. Smart tags along the supply chain

45. **Claudia Loebbecke**, Professor, University of Cologne, following-up on previous comments, stated that RFID is not a stand-alone market, but rather an enabler of other markets such as the health market, and also stressed that applications for customers and those for citizens should be treated differently. She added that in supply chain management there is a huge difference between RFID on pallets or cases, where the economics look very promising, and RFID on items.

46. Ms. Loebbecke warned that for RFID on items, there are not many applications yet in the business world, but there is a high potential for advertising, security and theft protection as well as for copy protection. She further explained that the current disagreement on the frequency range to be used for item-level tagging (868 MHz versus proposing 13.56 MHz) has a major impact on the applications possible. She concluded that the widespread use of RFID on items could take quite some time, but that in an increasing number of cases the benefits will become obvious so that people/consumers may adopt sooner rather than later.

47. **Masakazu Fujita**, Research Director, Next Generation Electronic Commerce Council of Japan (ECOM), listed three keywords for the RFID policy of METI (Ministry of Economy, Trade and Industry): international co-operation, low-cost RFID production and field trials. He presented case studies of RFID in the retail and publications sectors in Japan. A field trial of RFID in retailing involving a shoe manufacturer, a wholesaler, and the shoe department of a department store showed a 180% increase in the number of queries from terminal, a 25% decrease of the number of round trips to the backyard, a 54% decrease of the service time per customer, an 82% increase in product choice and 10% increased sales. Mr. Fujita concluded that RFID was key for staying competitive and that its overall impact will be better customer service.

3.2. Smart tags at the item-level and smart cards in service applications

48. **Elie Simon**, Chief Executive Officer, TAGSYS SA, as the CEO of a global leader in item-tagging space, sees a large potential for item tagging, *e.g.* luggage packing, and for real-time inventory to be a killer application. He pointed out that the economic value of an innovation is generated by the mandates (*e.g.* Wal-Mart, DoD, FDA) which create a virtuous circle, where the need for higher read rates fuels discussion and information-sharing on standards that, in turn, create new needs.

49. He noted that to understand the business needs in the item-tagging field, one has to look at the end-to-end item-tagging infrastructure solution that delivers the response to the need, for example, in some cases the package can be the tag. He cited as applications: cash envelopes with an RFID antenna (tracking and theft-protection), brand protection (copy protection) and biobanks (global network in order to share knowledge, with ruggedised "nano" tags that can resist extreme temperature variations). He concluded by saying that he saw privacy as a very serious issue and that, if the industry takes privacy seriously, privacy concerns may be addressed better by the industry than by regulatory bodies.

50. **Mark MacCarthy**, Senior Vice President for Public Policy, Visa USA, stated that more discussions, such as this one, were needed on RFID, so that issues could be out in the open and added that it was necessary to make clear distinctions between the different applications which use/require very different ISO standards. In the case of Visa, users only need their cards to be read from a one inch range and they do not want devices to be read widely or interoperate with other readers, such as EPC readers. Consequently, Visa does not want to be part of a “ubiquitous” network.

51. Referring to privacy, Mr. MacCarthy noted that in the context of the payment world there was no interest in information being more widely available and seeing separate proprietary networks erode. Since consumers with contactless Visa cards require the same types of protection as they have with regular credit cards (*e.g.* zero liability in the United States means that any misuse is not the card-holder’s responsibility but the responsibility of the card issuers. Therefore, the financial institutions in the Visa system have the incentive to make sure the system is secure. The built-in security features of the current contactless Visa cards are 128-bit encryption, and a new security code is generated with each transaction and decrypted by the issuer.

Panel questions

52. **Richard Rees** noted the fact that source tagging and hands-free checking were vital to the success of RFID. He noted the notion of time utility had been raised by many presenters; both time utility to merchants and to consumers.

53. **Marc Rotenberg**, while recognising that the way Visa intends to use the contactless card is not for sharing information, pointed out that there are privacy and security issues raised with the contactless card that are not raised in magnetic strips, such as reader range, encryption, and that what makes the Visa system work is that the challenges of privacy and security have been addressed, whereas for others that fail to address these issues there will be very serious problems.

54. **Mark MacCarthy** agreed that there are challenges, less so on privacy – as long as people know that the information will not be widely available – but more so on security issues – not less than in magnetic strips but no more either, thanks to the built-in security features.

RFID demonstrations

55. **Marc de Freminville**, on behalf of IBM, introduced three scenarios for RFID in supply-chain management applications:

1. RFID-enabled dock-door portal at case level – typically RFID labels are printed and slapped on cases by the manufacturer. Readers filter all the RFID tag generated information and aggregate them into data that has a meaning for specific business applications. The data gathered by readers can be displayed and uploaded to back-end applications through RFID middleware, which can also convey information that is not on the tags but scattered on other information servers anywhere in the world.

2. Information kiosk at the shelf-level as a functionality for consumers – The EPCGlobal architecture also proposes to combine data on the tags with data that is on information servers through the Internet to gather additional information on the product, *e.g.* who manufactured the medicine, when, what is the composition of the product and whether another product with the same unique ID has been sold – as a way to fight against counterfeiting. The Information server is called EPCIS server, allowing data to be accessed only by people who have the appropriate rights.

3. Fast check-out, putting all items in a plastic bag and moving through the cashier which is a Point of Sale terminal connected to an RFID reader/RFID antenna combination and pressing one button to obtain a printed ticket. Such an application is relevant only in a specialised retail environment as opposed to large retail environments with large numbers of products.

56. **Omar Rifaat,** on behalf of Philips and Visa, demonstrated payment applications with a contactless RFID-enabled Visa card, showing how contactless pay cards can speed up payment. The contactless card is the same as a common Visa card but contains an antenna: equipped merchants input transaction amounts and consumers just need to show their card. Visa's business opportunity/driver is that it can target a large percentage of the low-value "cash" market by focusing on a small number of merchants (groceries, newsagents, pubs, fast foods etc.).

Session 4. Critical issues for policy makers

4.1. Infrastructure/standards panel discussion

57. **Dave Wollman**, Scientific Advisor and RFID Coordinator, National Institute of Standards and Technology (USA) and session moderator, explained the three main subjects to be discussed in the session: *i)* RFID standards and the status of standardisation for different RFID technologies and in particular, how security and interoperability are being built into the standards; *ii)* spectrum and whether there are spectrum regulations in specific regions that might be changed to better accommodate RFID as well as industry approaches that could effect such changes; and *iii)* information infrastructures associated with RFID and the implications of their access across IP networks.

58. **Henri Barthel**, Technical Director, EPC Global, pointed out that GS1, with 1.1 million member companies worldwide, is a very well established standards-making body with significant experience in bar codes, which has been expanded to develop standards for e-commerce and then for RFID. Recalling that intellectual property is a complex and important issue which aims to achieve a balance between commercial interests, technology development and affordable products, he noted that, while EPCGlobal aims to provide royalty free standards, Reasonable And Non Discriminatory (RAND) IP claims are exceptionally accepted and that ISO is also working on the basis of an Intellectual Property rights policy based on RAND. He mentioned that a patent pool was created recently for RFID Gen 2 products and considered this a good approach for users and solution providers as it made it simple, fair and cost effective to use IP from this pool of companies.

59. Mr. Barthel differentiated two aspects of the standards-making process: *i)* the technical protocols, *e.g.* Air Interface Protocol, and *ii)* the regulations on radio frequency spectrum. He indicated that ISO has developed standards in different areas, *e.g.* animal identification, cards and personal identification, containers ID and that for item management applications, standards are expected to be completed by March 2006. He further explained that within EPCGlobal, ultra high frequency (UHF) generates the most attention and that EPCGlobal standards include: Standard data, Standard air protocol, Standard software Interfaces, Standard query language and Standard network architecture. He added that EPCGlobal provides training, education and support; supports further R&D through Auto ID centers and facilitates mass adoption.

60. **Simson Garfinkel**, Postdoctoral Fellow, Center for Research on Computation at Society at Harvard University, stressed that RFID identifiers may be cloned and, unlike with barcodes, there is the possibility of covert readers/tags. He then presented the various privacy solutions proposed so far by industry and their limitations. With the "kill" function, many of the consumer post-sale applications (recycling etc.) are lost after purchase and in addition, the kill cannot readily be verified. With encryption, he pointed out the difficulty of providing security in the context of very high volumes: if every item has a different key it is difficult to manage all the different keys, and if the key is the same then the protection is not valuable.

61. Referring to the contactless payment solution demonstrated by Visa, Mr. Garfinkel pointed out that merchants would be able to remotely read what is included in the chip. He provided an overview of the rights people should have to curb the most obvious abuses including: *i)* the right to know if the product has an RFID tag; *ii)* the right to disable it; *iii)* the right to obtain a first-class alternative without RFID; *iv)* the right to know what information is in the tag and to correct the information; and *v)* the right to know if, when, and why a tag was being read.

62. **Kyo-il Chung**, Director, ETRI (Electronics and Telecommunications Research Institute, Korea) highlighted the many security problems in RFID systems, including those of signal interception,

unauthorised reading, spoofing, hacking, and RFDump and that such security threats include both passive signal interception from the RFID tag or reader and unauthorised reading. He highlighted that both lightweight security protocols as well as more sophisticated key distribution mechanisms were needed.

63. Mr. Chung outlined Korea's "ubiquitous-cluster" strategy. Korea's plan for the ubiquitous Information Society involves: *i*) Services, including RFID-based Service among others (WiBro, DMB Service, Telematics Service, Internet Telephony etc.); *ii*) Infrastructure, including the Ubiquitous Sensor Network among others (broadband convergence network and next generation Internet protocol – IPv6); and *iii*) Growth engines (mobile telecommunications handsets and equipment, digital TV and peripherals, home networks HW/SW, system-on chips, next generation PCs, embedded software, digital content and software solutions and telematics).

64. **Bernard Benhamou**, Senior Lecturer, Political Science Institute, Paris, stressed that the implications of the "Internet of things" for public policy were considerable. He stated that it was important to maintain three principles: *i*) interoperability; *ii*) openness; and *iii*) the end-to-end principle or neutrality principle which means the network remains a decentralised entity providing neutral transportation without a central authority.

65. Mr. Benhamou stressed the need for a new model of co-operation as security and privacy of networks are evolving with new technologies added on to the Internet and the need for action at the three levels of technology, education and awareness of users, and also a legal part of this action. He stated his hope to see co-operation towards an Information Society that is democratic and respects the values of the entire community.

Panel questions

Question: Role of OECD

66. A: **Elliot Maxwell** stated that reviewing the history of OECD guidelines and the OECD's characteristics -- multinational, multi-stakeholder, neutral forum in that it is reasonably transparent, traditionally data-driven – the organisation offers the opportunity for a constructive dialogue about the issues raised by RFID. He added his belief that the OECD could help develop a set of lasting privacy and security principles that can be applied as the technology and the practices evolve.

67. A: **Simson Garfinkel** stated that the OECD privacy guidelines have been extremely important for the adoption of fair information principles in many of the world's developed countries. He noted that, in contrast, work on RFID so far has been conducted by a small group of users and manufacturers with limited awareness of individual liberty, privacy or security issues. He asserted his belief that the OECD could change the balance and bring values of transparency, security, privacy and personal liberties.

Question: Spectrum allocation

68. A: **Henri Barthel** stressed that spectrum allocation standardisation for interoperable EPC requires effort and that a statement by the OECD stressing the need for global harmonisation would be important. He added that the role of the OECD vis-à-vis standards was less clear.

4.2. Privacy panel discussion

69. **Joseph Alhadeff**, Vice President for Global Public Policy and Chief Privacy Officer, Oracle Corporation, recalled comments by previous speakers differentiating between before the point-of-sale (POS), where security is the main concern and after POS, where privacy and security are both concerns.

70. **Marc Rotenberg**, Executive Director, Electronic Privacy Information Center, stated that of all the issues the privacy issues are the most challenging but that people and consumers were organising to address RFID-related privacy issues. He noted that RFID technology, by its nature, conceals information and, as a result, privacy guidelines and the distinction between different uses of RFID (implantation vs. tagging of pharmaceutical goods) are crucial. He stressed five questions relating to transparency in the use of RFID that are necessary to supplement the current OECD privacy guidelines: *i)* where is the tag? *ii)* when is data collected? *iii)* who collects the data? *iv)* what kind of data is collected? and *v)* why is data collected? In addition to this, individuals should be informed about of the presence of RFID tags.

71. Question from the floor: does basic access control for ICAO constitute a minimal level of protection for a contactless card such as an ID card?

72. **Mark Rotenberg** confirmed that basic access control was a minimal requirement without which the risks associated with RFID applications are likely to exceed the benefits. He recalled that basic access control in ID documents means that the holder of the card is the owner of the information contained in the card/document and noted that, while the issue was favourably resolved with the US passport program, it was an ongoing debate with the US Visit program.

73. **Florent Frederix**, Scientific Officer for RFID, European Commission Infosoc D-G, noted that RFID has taken quite a priority in the public debate today because applications are moving into deployment very fast, and that discussions must go on and a more holistic approach adopted. He outlined the different questions that require solutions: *i*) Is there a technical solution to protect privacy? *ii*) Should we rely on self-regulation or codes of conduct *iii*) Is privacy legislation sufficient? He mentioned the 2005 working document on data protection issues by the European Commission, which provides guidance for RFID technology manufacturers to design privacy compliant technology and for standardisation bodies.

74. **Stephania Congia**, International Department of the Italian Data Protection Commission, explained the regulatory framework in Italy. She stated that the majority of basic principles are already laid down in OECD guidelines, EU directives, the Council of Europe Convention, but that RFID technology has an impact on personal dignity and integrity as well as on freedom of movement and that personal data can be processed without the knowledge of the individual. She explained that Italy had created RFID-specific regulations, extending traditional data protection principles to RFID technologies for item tagging and prohibiting under-skin implants under normal circumstances in Italy.

75. **Jeroen Terstegge**, Corporate Privacy Officer, Philips, and speaking on behalf of the ICC Privacy and RFID Working Groups and of EICTA (Chair), presented the business perspective of RFID-associated privacy issues, solutions and the role of governments. He differentiated between three "identity types": *i)* RFID linked to persons (biometrics, personal data in database, employee badge); *ii)* RFID linked to services, either used in combination with person ID (*e.g.* banking cards) or used anonymously with no link to a person's ID (*e.g.* some types of transportation cards); and *iii)* RFID linked to products/objects, where product information is in a database (*e.g.* EPCs), or provided directly (*e.g.* car keys).

76. Mr. Terstegge stressed that RFID will increase electronic footprints. He considered various privacy-enhancing technologies (PETS) to increase the accuracy of footprints while maintaining consumer control. He distinguished two types of PETS: *i)* **system-solutions** in which PETs are built in (encryption, tag/reader authentication, range reduction, or antenna size/design) and *ii)* **consumer-in-control solutions** ("Kill-switch", removable tags, Blocker tags, shielding, confirmation via a user interface). When the privacy risk is high, he prones the use of smart cards and PETs, when the risk medium, the use of smart cards, smart tags and PETs, and when the risk low, the use of smart tags (with PETs optional). Stressing that RFID is only an enabling technology, Mr. Terstegge suggested that regulatory bodies should not legislate RFID-technology itself, but only those applications and uses containing a privacy risk. He

concluded by calling on industry and governments to promote the use of PETs where relevant, and on governments to stimulate R&D and standardisation in PETs as well as the use and acceptance of PETs.

Session 5. Roundtable discussion & conclusion

77. Chaired by **Hugo Parr**, Director General, Ministry of Modernisation, Norway, and Chair of OECD Committee for Information, Computer and Communications Policy, this discussion focused on what should the future contribution from the OECD be – both in terms of substance and of timing: what it should do as well as what it should avoid.

5.1 Summary of important elements from the Forum

78. **Richard Foggie**, Assistant Director, Electronics and IT Services, DTI, pointed out that RFID is merely a technology and that the key to its successful implementation is the realisation of a business case: value will come from process re-engineering. He summarised the key issues, first of all handling the volumes of data. Security is an issue, but one that will be fixed because there is a business need to fix it and RFID is just a new way of doing "old crime". Privacy remains clearly an issue, but is being discussed by consumer groups as well as business and governments. Politicians need to keep a very close eye on those issues as they relate to important concepts of identity: can vast amounts of data be collected on individuals' behaviour, where meta-data can be devised which narrows options in terms of individuals? Concepts of partial identity need to be explored by the OECD.

79. **Tony Taylor**, European Director, EPCGlobal Inc., noted that users are increasingly joining EPCGlobal because of the low cost of the technology and because of interoperability (open standards) and that large and small users need to use the technology in a safe, secure, responsible way, thinking about all consequences of the system. He sees the role of the OECD as providing a neutral environment where industry, governments and civil society representatives can talk, in a positive manner, since the benefits are real and the technology will be of great help if is approached in the right way.

80. **Jeremy Ward**, Director of Service Development, Symantec EMEA, emphasised that RFID could be as ubiquitous as the Internet, where standards led to the creation of many real-world applications and new standards, but that security was "bolted on" afterwards instead of being "baked in" and that history should not be repeated. He stressed that without security, confidentiality availability and integrity, RFID will not work for businesses nor for users and that it is essential that people be able to trust the system. Mr. Ward sees the role of OECD as providing a forum where international awareness of the issues can be raised and where the promotion of a "culture of security" can be extended to cover RFID.

81. **Peter Ferguson**, Director, Electronic Commerce Policy, Industry Canada, summarised the key issues. RFID technology creates real economic benefits and growth, but the current metrics might be too loose and new indicators may be needed. While there will be economic growth and social benefits, there will be many policy issues and the need for ground rules for an "Internet of things" (including standards, principles, industry guidelines and law). He stated that the challenge will be targeting behaviour rather than the technology — as business laws and privacy laws will continue to apply — and meeting the needs of multiple stakeholders. Mr. Ferguson sees the role of the OECD as providing guidance to explain existing laws in the new environment, in addition to providing new metrics.

5.3 Open discussion of important elements from the Forum

82. Question from the floor: a participant asked whether governments should have an active role in promoting the growth of use of RFID, making the analogy to government promotion of other enabling technologies like broadband. Similarly, should governments mandate the use of RFID, the way e-Government is mandated, or alternatively should government be some kind of launching customer.

83. **Najji Najjar** responded that, while a lot of time was spent in the forum discussing privacy and security, most applications today do not implicate security and privacy and have large economic benefits and that consequently, it is desirable to separate applications that have privacy implications from those that do not.

84. Another participant commented that the time was right to address these issues and that RFID signals the development and next generation of information society issues. The forces behind RFID are getting stronger, bringing vast economic benefits but also threats such as privacy and reliability. One of the problems so far has been the difficulty to quantify returns on investment, but an even more significant problem is the difficulty to quantify the threats. He called upon the OECD to help go beyond opinion and hype, mainly by sharing experiences, as the organisation has done with other technologies.

85. **Dan Caprio** commented on the need for partnerships in order to consider the privacy and security issue.

86. **Marc Rotenberg** stated that privacy positions that can be sustained over time are not those that are against technology or business success. He felt that privacy issues raised by RFID are real. To the extent it is possible to separate the applications: those without privacy/security issues should be allowed to go forward and succeed, but for others, there are very real reasons to think about privacy, autonomy and liberty. Mr. Rotenberg sees the role of OECD as being of great importance, as it has been with its pioneering work on privacy, security and encryption, in providing best practices or model applications of RFID technology incorporating security/privacy principles.

87. A participant commented that one issue that was not addressed in the forum is the impact of RFID on employment and that in some sectors, there may be a positive impact but in other sectors (*e.g.* retail storage, re-assortment), there may be a very large negative effect on human employment. It was stated that the privacy issue does not apply to consumers because they are consumers, but because they are individuals and that these issues – principle of consent – apply also in the supply chain to workers and management.

5.3 Overall summary and next steps

88. **Hugo Parr** concluded that solutions must be found, but that, if done right, a win-win situation was a possibility, building security/privacy into the design of RIFD applications. He felt the OECD was in a good position to provide guidance in this area, in particular in interpreting existing privacy measures under new circumstances.

ANNEX: PROGRAM

FORESIGHT FORUM

"RADIO-FREQUENCY IDENTIFICATION (RFID): APPLICATIONS AND PUBLIC POLICY CONSIDERATIONS"

Convened by

The Committee for Information, Computer and Communications Policy (ICCP)
of the Organisation for Economic Co-operation and Development (OECD)

5 OCTOBER 2005, 9:30 – 18:00
at OECD headquarters, Château de la Muette – Room 1
2, rue André Pascal, 75016 Paris

Introduction

Description of the Technology, its Economic Potential & Applications

Radio Frequency Identification (RFID) is an emerging technology consisting of three key pieces: RFID tags (miniaturised chips); RFID readers; and a data collection, distribution, and management system that has the ability to identify or scan information with increased speed and accuracy. Compared to the bar code system, RFID promises long-term gains in supply chain management, transportation, defence and health care, to mention a few. RFID is increasingly used in commercial supply chain applications through aggregate level tagging, for example tagging of pallets.

RFID, because it is a cross-cutting and enabling technology, adds to the important role Information and Communication Technology (ICT) plays to promote innovation, economic growth, and global commerce. Looking toward the future, as the information infrastructures associated with RFID are increasingly accessed across IP networks, the OECD is well positioned to discuss with stakeholders how best to create a positive environment for growth, and promote best practices for the implementation and use of RFID.

RFID, like the Internet, requires effective privacy and security policies that address questions that arise as a result of the growth and interconnectedness of information and communications networks. In particular, disclosure, transparency and choice are important considerations for consumers as RFID migrates to item level tagging over the next few years. Policies that are informed by industry best practices and consumer concerns will foster the potential of ICT and facilitate development of emerging technologies such as RFID.

Critical issues for policy makers

The ICCP Forum "Radio-Frequency Identification (RFID) Applications and Public Policy Considerations" will bring together government delegations, academia, private sector and non-governmental organisations to address important questions such as:

- In the key sectors and supply chains that use/have implemented RFID technologies to-date (including retail, transportation, pharmaceutical and livestock), what are current Supply Chain Management (SCM) applications and their impacts? What are other applications throughout the value chain?
- What are the factors affecting RFID rollout in value chains? How are gains measured?
- What important developments are in progress that may prompt widespread deployment of RFID within the ICT infrastructure (including sensor networks, smart devices, and context-aware technologies)?
- What are some of the future applications that RFID promises to offer, and what are the ensuing growth and productivity gains associated with them?
- What role do technological solutions, industry self-regulatory best practices and policy interventions play in current implementation practices?
- What privacy and security issues have come to the forefront as RFID moves closer toward item-level tagging?
- What new approaches are required and/or are already available, such as effective privacy and security policies, to both sustain innovation, and offer awareness of technology applications for consumers to make informed choices?
- What are some of the important public policy and international co-operation discussions underway that may encourage widespread deployment of RFID, including interoperability, standards and data protection?

ICCP Foresight Forum "Radio-Frequency Identification (RFID): Applications and Public Policy Considerations"
To be held at the Château de la Muette, Paris – Room 1
5 OCTOBER 2005, 9:30 – 18:00

1. WELCOMING REMARKS AND INTRODUCTION BY THE CHAIR [9:30 – 9:40]

Hugo Parr, Director General, Ministry of Modernisation, Norway, and Chair of OECD Committee for Information, Computer and Communications Policy

2. DESCRIPTION OF RFID TECHNOLOGY AND ITS POTENTIAL [9:40 TO 11:00]

Introductory remarks and session moderator: **Jonathan Collins**, European Editor for RFID Journal

2.1. Panorama of RFID current applications and potential economic benefits [9:40 – 10:10]

- What is the panorama of applications possible, time-frames for implementation and likely impacts?
- In the key sectors for the use of RFID technologies to-date (including manufacturing, transportation, pharmaceutical), what are current applications?

Dan Caprio, Deputy Assistant Secretary for Technology Policy and Chief Privacy Officer, U.S. Department of Commerce
Naji Najjar, Director of Wireless Broadband & Sensing Solutions, IBM Southwest Europe

2.2. Future applications, ubiquity of RFID and potential economic and social benefits [10:10 – 11:00]

- What important developments are likely to prompt the shift to widespread deployments of RFID within the information and communication technology (ICT) infrastructure (including sensor networks, smart devices, and context-aware technologies)?
- What implications does RFID have for the ICT infrastructure and vice-versa?

Indro Mukerjee, Executive vice president, Automotive & Identification business unit, Philips Semiconductors

Taiichi Inoue, Senior Consultant - Head of IT for Society Consulting Group, Nomura Research Institute, Ltd.
Elliot Maxwell, Fellow of the Communications Program at Johns Hopkins University

COFFEE BREAK [11:00 – 11:30]

3. COSTS/BENEFITS IN DIFFERENT TYPES OF APPLICATIONS [11:30 – 12:30]

Introductory remarks and session moderator: **Richard Rees,** President, Scanology Group, and Chair British Standards Institution Technical Committee "Automatic Identification Techniques"

3.1. Smart tags along the supply chain [11:30-12:00]

- What are the factors affecting RFID rollout in supply chains? How are gains measured?
- What are total costs of investment and operation and expected return on investment?
- What are likely economic impacts of RFID on SCM applications at the firm, sectoral and economy-wide levels?

Claudia Loebbecke, Professor, University of Cologne
Masakazu Fujita, Research Director, Next Generation Electronic Commerce Council of Japan (ECOM)

3.2. Smart tags at the item-level and smart cards in service applications [12:00 – 12:30]

- Where has RFID been implemented in services or item-level tracking?
- What drivers/inhibitors have been encountered?
- What opportunities for CRM applications? How are consumer concerns addressed?

Elie Simon, Chief Executive Officer, TAGSYS SA
Mark MacCarthy, Senior Vice President for Public Policy, VISA USA

LUNCH BREAK: LIGHT BUFFET IN ESPACE PASCAL [12:30 – 13:15], Courtesy of Philips and VISA

RFID DEMONSTRATIONS IN ROOM 1 [13:15 – 14:15]

- Demonstration by IBM: RFID in supply-chain management applications.
- Joint demonstration by Philips and VISA: payment applications with contactless pay cards and RFID-enabled mobile phone.

4. CRITICAL ISSUES FOR POLICY MAKERS [14:15 – 17:00]

4.1. Infrastructure/standards panel discussion [14:15 – 15:30]

Introductory remarks and session moderator: **Dave Wollman**, Scientific Advisor and RFID Coordinator, National Institute of Standards and Technology (USA)

- What is the status of standardisation for different RFID technologies? In particular, how is security and interoperability being built into the standards?
- Are there spectrum regulations in specific regions that might be changed to better accommodate RFID? What industry approach could effect such changes?
- As the information infrastructures associated with RFID are increasingly accessed across IP networks, what are the implications for IP network architectures?

Henri Barthel, Technical Director EPCGlobal, GS1

Simson Garfinkel, Postdoctoral Fellow, Center for Research on Computation at Society at Harvard University

Kyo-il Chung, Director, ETRI (Electronics and Telecommunications Research Institute, Korea)

Bernard Benhamou, Senior Lecturer, Political Science Institute, Paris

COFFEE BREAK [15:30 – 15:45]

4.2. Privacy panel discussion [15:45 – 17:00]

Introductory remarks and session moderator: **Joseph Alhadeff**, Vice President for Global Public Policy and Chief Privacy Officer, Oracle Corporation

- What privacy and security issues have come to the forefront as RFID moves closer toward item-level tagging?
- What smart safeguards are required, for instance privacy and security policies that will both sustain innovation, while providing consumers with education and awareness, tools and choices to protect themselves?
- What role for technological solutions, industry self-regulatory best practices and policy interventions in the medium-term future? In particular, to which extent is existing privacy and data protection legislation adequate? Is new legislation or a strengthening of the enforcement of existing legislation called for in some circumstances?

Florent Frederix, Scientific Officer for RFID, European Commission Infosoc D-G

Jeroen Terstegge, Corporate Privacy Officer, Philips, and Member of the EICTA (Chair) and ICC Privacy and RFID Working Groups

Marc Rotenberg, Executive Director, Electronic Privacy Information Center

Stephania Congia, International Department of the Italian Data Protection Commission

5. ROUNDTABLE DISCUSSION & CONCLUSION [17:00 – 18:00]

Chaired by **Hugo Parr**, Director General, Ministry of Modernisation, Norway, and Chair of OECD Committee for Information, Computer and Communications Policy

5.1 Summary of important elements from the Forum [17:00 – 17:20]

Peter Ferguson, Director, Electronic Commerce Policy, Industry Canada

Richard Foggie, Assistant Director, Electronics and IT Services, DTI

Tony Taylor, European director, EPCGlobal Inc.

Jeremy Ward, Director of Service Development, Symantec EMEA

5.3 Open discussion of important elements from the Forum [17:20 – 17:50]

5.3 Overall summary and next steps [17:50 – 18:00]

- Overall summary by **Hugo Parr**, Director General, Ministry of Modernisation, Norway, and Chair of OECD Committee for Information, Computer and Communications Policy
- Potential future work by the OECD: next steps

Cocktail at the delegates' bar [18:15], Courtesy of IBM