

# Identifiability in RFID

Noriswadi Ismail<sup>1</sup>

## Introduction

Radio Frequency Identification (RFID) hype is still happening. Various market research prediction and analysis suggest that its contributing applications to various industries and sectors have proven to be a yielded investment. The world's today has witnessed how effective and efficient the deployment of RFID applications are. Such deployed applications can be seen through leading global events; the World Cup 2006 in Germany, Beijing Olympics 2008, Shanghai Expo 2010 and the soon London Olympics 2012.<sup>2</sup> These applications are deployed to manage various inventories, tracking, ticketing, assets tagging as well as security management. The actors behind these applications are many; ranging from the RFID service provider, the vendor, the customer, the software and middleware provider, other technical providers who contribute to such sophisticated large scale RFID applications, and most importantly, the users (or interchangeably be referred to as the consumers and data subjects). Whilst some of these actors' involvements are governed by contractual obligations, there is little discussion that touches the fundamental understanding who are the controller and processor in an enabled RFID application? And how identifiability is dissected in RFID application? To respond to these anomalies, in section 2, I pursue by narrating brief genealogy of RFID technology and how it evolves. In section 3, I attempt to provide brief observations and analysis in relation to the Article 29 Data Protection Working Party (A29DPWP) leadership on RFID. Subsequent to comprehend these backgrounds, in section 4, I further draw down the concept of identifiability in RFID.

## 2. RFID; The brief genealogy

There are three dissections that establish technical principles that compose RFID; the **R**adio, the **F**requency and the **I**Dentification. Without the integration of these, RFID may not be technically functional. All of these technology components shaped RFID with the presence of two devices; the chip (or interchangeably called as the tag) and the reader, which comprises an antenna and a demodulator that translates such analogued information from the radio into digital data. The reader also activates the reading of a particular item.<sup>3</sup> RFID works compatibly well within a specific frequency, depending upon the responsiveness of a tag (whether active, passive or semi-active or semi-passive). The tag contains unique identifiable code characteristics which are technically standardised as the Electronic Product Code (EPC), a recognisable and globally acceptable identification code. The EPC is regarded as a global standard that shapes the substitution of bar code usage. This means, arguably, by the usage of EPC within RFID application, the manual usage of bar code may decrease.<sup>4</sup> RFID was used in the military, which akin to the historical anecdotes of internet. It was deployed extensively during the World War II, to track and trace aircrafts via the Friends and Foe identification.<sup>5</sup> When the war ended, efforts were made to extend its potentials for commercialisation. It was when the seven collaborative leading Auto-ID Laboratories located in four continents begun to research and explore its potentials. In-house research & development labs of leading

---

<sup>1</sup> Doctoral Researcher in IT Law, Centre for Commercial Law Studies, Queen Mary, University of London.

<sup>2</sup> See generally London Olympics 2012 – track and shield - <<http://trackandshield.wordpress.com/tag/rfid-blocking/>> Accessed 1 March 2011.

<sup>3</sup> See Roy Want, *RFID Explained, A Primer on Radio Frequency Identification Technologies, Synthesis Lectures on Mobile and Pervasive Computing* (Morgan & Claypool, 2006).

<sup>4</sup> See Poulett, Y., Rouvroy, A. and Darqueness, D. (2008) 'The Law encounters communication and information technologies: the case of RFID', *Int. J. Intellectual Property Management*, Vol. 2, No. 4, pp. 377-378.

<sup>5</sup> See generally John Ayode, *Roadmap to solving security and privacy concerns in RFID systems*, pp 555-561, *Computer law and Security Report*, vol 23, 2007.

technology companies across the world have also researched and designed customised RFID applications.<sup>6</sup>

RFID is also hailed as The Internet of Things (IoT) or the Internet of Objects, which is self-configured through sensor wireless networks that are extendable to connect with any objects and living objects under the sun. It is one of the living testimonies of ubiquitous computing that makes our life convenient and quite alarming. This paradigm of ubiquitous computing is also interchangeably perceived as pervasive computing and ambient intelligence. Bearing in mind that these terms – IoT, Internet of Objects, ubiquitous computing, pervasive computing and ambient intelligence – generally, are inter-related, although philosophically it differs in terms of contexts and applications.<sup>7</sup> In the next decade, the world will be inter-connected with complex configured wireless network. By 2014, the world will witness the first of its kind Ubiquitous city (U-city); Songdo, in the Free Economic Zone of Incheon, Korea. This city is designed through interconnected networks and RFID is the key technology behind this. It has been learned that the Songdo U-city, which is known as the Tomorrow City, will be potentially recognised as the world's largest integrated urban operations centre that offer Ubiquitous-services (U-services) such as traffic, disaster prevention, surveillance, security and pollution control.<sup>8</sup>

### 3. RFID Leadership in Europe

In parallel, technological progress on RFID has sparked data protection and privacy concerns worldwide. The mixture of data protection and privacy approaches tend to suggest that the cliché of 'there is no one size fits all' is slightly ambivalent. Due to this, the European Commission (EC) has had called for stakeholders' participation to shape the RFID leadership, not only from the legal viewpoints, but also from the technical, business and policy viewpoints. This is evidenced through the RFID: Lisbon Strategy that sets the consensus and milestone on the need for Europe to analyse, assess and develop common strategies in RFID technology. Critically important, it emphasises the needs to safeguard and protect sensitive information and privacy of individuals. In this regard, at the European level, the A29DPWP leads the legal roadmap to clarify such principle and application issues that surrounds data protection and privacy.<sup>9</sup>

A29DPWP 105 has discussed on how such gathering and further processing of data through RFID via the application of Data Protection Directive 95/46/EC (DPD).<sup>10</sup> Recital 26 of the DPD states, "*account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person*". This recital is to be cross referred to the conditions as to whether the collected data relates to an individual; whether such collected data relates to identified or identifiable individual. In crux, the DPD (generally) applies if there is an involvement of identifiable data that relates to a person. Besides Recital 26, Recital 2 envisages that "*data processing systems are designed to serve man; (...) they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, in particular the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals*". These Recitals,

---

<sup>6</sup> See generally Auto-ID Lab < <http://www.autoidlabs.org/>> accessed 12 February 2011.

<sup>7</sup> See Interview around IoT/RFID Scenario Risk Assessment - <<http://www.enisa.europa.eu/media/news-items/iot-interview>> accessed 20 January 2011.

<sup>8</sup> See The Korea Times – Incheon to House World's Largest Ubiquitous City <[http://www.koreatimes.co.kr/www/news/nation/2010/07/281\\_56996.html](http://www.koreatimes.co.kr/www/news/nation/2010/07/281_56996.html)> accessed 29 March 2011.

<sup>9</sup> European Commission Justice < [http://ec.europa.eu/justice/policies/privacy/workinggroup/index\\_en.htm](http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm)> accessed 18 January 2011.

<sup>10</sup> See Working document on data protection issues related to RFID technology 10107/05/EN WP 105.

conjunctively, promote broader protection of data protection and privacy under the umbrella of fundamental human rights.

From these broader recitals' motivations, A29WDP 105 has further extended its advisory opinion on these pertinent points; data quality, legal grounds of processing, information request, data subject's right of access, security related obligations, technical and organisational requirements, standardisation and interoperability, technical and organisational measures that ranging from exercise of data access, rectification, deletion notification and data security. The key observation from these is that the array of principles of data protection in the DPD is applicable in a co-related manner. Emphasis has been given to Article 6 (a) - fair processing, Article 6(1)(b) – data quality, Article 6 (1)(d) – security, Article 7 – legal grounds of processing, which also includes Article 7(a) – withdrawal of consent on personal data, Article 10 – information request, Article 12 – Data subjects' right of access, which covers Article 12 (a) – access content (b) – notification and deletion, Article 14 (a) – withdrawal of consent and Article 17 – security related obligations. The contextual applications of these Articles will be depending upon the context of such RFID applications and actors' involvement.

A29WPDP 105 and 111<sup>11</sup> shaped the turning point of RFID leadership that resulted to the Opinion 9/2011 on the revised Industry Proposal for Privacy and Data Protection Impact Assessment (PIA) Framework for RFID applications (referred to as A29WPDP 180).<sup>12</sup> This opinion substantiated the Opinion of 5/2010 (referred to as A29WPDP 175). Three indispensable elements are addressed; firstly, a defined risk assessment approach, secondly, the consideration for RFID tags carried by persons beyond the operational perimeter of the application, and thirdly, the proposed deactivation principles in the retail sector that are established in the European Commission's Recommendation on the implementation of privacy and data protection principles in RFID applications. The A29WPDP 180 has also considered the adoption of an independent published opinion of the European Network and Information Security Agency (ENISA).<sup>13</sup> In essence, two phases of PIA processes are recommended. The first phase covers pre-assessment phase, which classifies an RFID application according to a 4 level scale, based on a decision tree. Based on the respective classified scales (from level 0 to level 3), such evaluation results will be able to determine whether PIA applies or otherwise. The second phase is the risk assessment phase that consists 4 structures steps, based on the risk management approach; the characterisation of the application, risk identification, recommendation of controls and the results of documentation of PIA.

Whilst the A29WPDP 105, 111 and 180 have dealt with RFID, A29WPDP 169 deals with the very fundamental concepts of controller and processor.<sup>14</sup> There are 26 cited examples that have been illustrated in refining the differences, roles and applications of controller and processor. Out of these examples, the advisory opinion of 169 maybe applied to RFID applications in eight conditions: firstly, within the context of telecom operators (if there shall be potential Mobile-RFID applications), secondly, when an RFID middleware provider is referred to as data processor but acting as controller, thirdly, secret monitoring of employees (potentially through RFID chips), fourthly, when such financial transactions may potentially involve RFID through money tagging, fifthly, when RFID applications are deployed within and throughout e-government portals (at the middleware and back end platforms); sixthly, when such

---

<sup>11</sup> See Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology 1670/05/EN WP 111.

<sup>12</sup> See Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications 00327/11/EN WP 180 adopted on 11 February 2011.

<sup>13</sup> ENISA Opinion on PIA < <http://www.enisa.europa.eu/media/news-items/enisa-opinion-on-pia/view?searchterm=PIA>> accessed 28 March 2011.

<sup>14</sup> Opinion 1/2010 on the concepts of controller and processor 00264/10/EN WP 169 adopted on 16 February 2010.

platforms for managing health data involve RFID applications, seventhly, when there shall be a potential RFID application in computer grids and lastly, when such RFID applications are involved in clinical drug trials. These eight conditions pose a complex environment, specifically, when one has to divide the roles, responsibilities. Liabilities of parties that are involved in an integrated and large scale RFID deployment.

From the perspectives of controller and processor, A29WPDP 169 emphasises the significance of interaction between all parties. This is to ensure a collective responsibility in complying with the data protection rules. The rule of thumb is to take the role of controller and processor based on factual circumstances. To justify such factual circumstances, three factors are taken into consideration: the determination to define personal aspect (“the natural or legal person, public authority, agency or any other body”), the possibility on pluralistic control (“which alone or jointly with others”) and the need to distinguish controller from other actors (“determines the purposes and the means of the processing of personal data”). All of these factors are inter-related between each other and may bear such complex and sophisticated factual circumstances. If these factors are to be applied within an RFID application, such participation of actors in the RFID, i.e., the vendor, the customer, the software and middleware provider, and other technical providers should be clearly defined. The chief rationale is to draw the clear lines of controls, responsibilities and liabilities. A29WPDP 169 has also drawn a clear line with regards to the concept of processor and third party. The former shall always be subjected to the decision by a decision of a controller - in deciding the data processing - whether it should be delegated fully or partly to an external actor. To achieve the status of being a processor in an RFID application environment, there should be a separate legal entity and a delegation by a controller to process such personal data. In practice (generally), a contractual agreement through data outsourcing processing agreement will be able to itemise the roles and responsibilities of the processor, which clearly outline the processor’s obligations to act on behalf of the controller. As far as the definition of the third party is concerned, it connotes as any actor who has no explicit and legitimate authorisation within a specific engagement. In short, any unauthorised actors are regarded as third parties, if, their roles and responsibilities are not explicitly outlined in a data outsourcing processing agreement.

#### **4. Concept of identifiability in RFID**

In RFID, the concept of identifiability is less discussed and touched. As explained in section 1 above, RFID comprises three dissected components. Out of these, the ID component represents the related subject that relates to data protection and privacy. Eleni Kosta and Jos Dumortier are of the view that it is an intriguing question in determining identifiability in RFID, especially when an RFID tag is incapable of linking its identification capability to such persons (data subjects).<sup>15</sup> Recital 26 of the DPD has been cited, in which, it fixes two criteria for identifiability; the inter-related relationship between probability and the difficulty. Interestingly, a thought provoking observations were mooted as to whether data protection legislation should be applied in all RFID applications due to the vague definitions of personal data and whether such identified information through the RFID tag from a natural person is regarded as personal data. In a similar vein, Yves Poulett, Antoinette Rouvroy and Denis Darquennes have posed a fundamental question as to whether such RFID applications fall under the field of the application of laws ‘protecting data of a personal nature’.<sup>16</sup> They generally affirmed that such information that are generated by RFID are not necessarily personal data and extend the observation through the concept of contactability by examining the European Directive 2002/58/EC’s notion

---

<sup>15</sup> Kosta, E. and Dumortier, J. (2008) ‘Searching the man behind the tag: privacy implicatios of RFID technology’, the case of RFID’, *Int. J. Intellectual Property Management*, Vol. 2, No. 3, pp. 278-280.

<sup>16</sup> *Ibid*, n. 4 at p. 386-387.

on personal data within the contextual applications of traffic in data and localisation.<sup>17</sup> The interesting conclusion from the examination suggests that such data may not be personal in nature and the search for a link with an identified or identifiable person is no longer necessary.

Against these backgrounds of observations, it is challenging to contextualise the present position of the DPD and other accompanying A29WPDP advisory opinions that touches on the notions of identifiability, data and personal data (if any). In view of this, I have taken a U-Turn approach to ask these fundamental questions; What is identifiability? Why identifiability is crucial? Who is involved in identifiability? And when does identifiability occurs? All of these questions are analysed from the perspectives of RFID.

Identifiability refers to the ability of an item or living object being identified through a mode or device directly and indirectly. It has a close connection with linkability. In an RFID component, the actors behind identifiability are the controller and the processor. In such factual circumstances, it may also be an automated generating design system integration and development, developed by the actors' employees. If we are to apply the relationship of identifiability and the actors, Articles 2 (d) and (e) of the DPD apply. This is by looking into the scenario in which such RFID application involves personal data of such natural persons. Identifiability in RFID is equally crucial to be determined in data protection and privacy context based on two chief premises. Firstly, it aims to distinguish the taxonomy of actors that are involved behind such RFID applications and secondly, it refines such intertwined relationship between the RFID actors. Determining identifiability involves customised processes ranging from the designing, trial, implementation and to post implementation stages. In these stages, the Privacy By Design (PBD)<sup>18</sup> and the PIA shall be the useful tools, which are practically applicable to dissect such categorisation. It may be able to identify at which stages or levels of RFID applications, such data, is categorised as identified personal data, identified sensitive personal data and anonymous data. By combining the PBD and PIA at these stages within an RFID application, it may arguably provide a customised practical solution and defies such philosophical and contemporary definitional discussions, arguments and debates of defining personal data.

The concept of identifiability that I am proposing is that in the absence of such clarity in defining the applicability of personal data or identified personal data in RFID applications, it is submitted that further understanding on identifiability and its actors behind the RFID applications are crucial. Once understood, the application of the relevant Articles in the DPD, and the advisory opinions of A29WPDP of 105, 169 and 180 should be painstakingly customised, both, in theory and practice. This concept is influenced by the foundational approaches of contextual integrity of privacy by Helen Nissenbaum.<sup>19</sup> She has explicitly and implicitly propounded that in order to capture the nature of challenges posed by information technology (in this context, RFID), contextual integrity tags adequate protection for privacy norms to specific context. This theory, in particular, could be mirrored upon the nature of RFID application, in which - identification of data, whether personal or otherwise, involves processing, aggregation and profiling – are regarded as the contextual points of identifiability by

---

<sup>17</sup> See <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML>> accessed 20 February 2011.

<sup>18</sup> See European Data Protection Supervisor – Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy <[http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-19\\_Trust\\_Information\\_Society\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-19_Trust_Information_Society_EN.pdf)> accessed 28 March 2011.

<sup>19</sup> Nissenbaum, H (2004) 'Privacy as contextual integrity', *Washington Law Review*, pp. 119-158.

the RFID actors. Her proposition is originated from the idea of “spheres of justice” developed by political philosopher, Michael Walzer.

## **Conclusion**

RFID, like other technologies and emerging technologies, is not alone to grappling with legal obligations. This is akin to the emergence of internet in early 1990s. In summation, I have briefly narrated 2 sections on RFID’s origin and the leadership that Europe has taken the lead. In the latter, I have described the tenacious efforts of the DPD and A29WPDP 105, 169 and 180 respectively, by looking into the affected articles and advisory opinions relating to RFID applications. The chief limitation in this section lies onto the complexity nature of RFID applications, which could go beyond to Mobile-RFID. I purposely drop the discussion and analysis on the application of the European Directive 2002/58/EC, as a separate and independent analysis might be worthy for future analysis. In section 3, I have further asserted that it is indispensable to dissect the roles of actors behind identifiability. This could be mapped and customised through the four-abovementioned stages. By looking into these stages and cross-referencing to the efforts advocated by A29WPDP, I conclude that the pre-emptive measures and controls to comply with data protection and privacy principles in RFID, do co-exist, at macro level. However, the starkest limitation lies onto the ability to merge the isolated pieces of measures and controls from various opinions and related articles in the DPD together, so that one could view the vertical and horizontal landscape on how the laws and RFID technology reconcile, between each other. Enthusiastically, on this note, we shall await and witness the forthcoming outcome of the DPD review and how it affects RFID technology this summer of 2011.<sup>20</sup>

---

<sup>20</sup> See generally Information Commissioner’s Office, Data Protection Officer Conference, March 2011 < [http://www.ico.gov.uk/news/events/~link.aspx?\\_id=13EE0F7706E3426CAC33320FC3555014&\\_z=z](http://www.ico.gov.uk/news/events/~link.aspx?_id=13EE0F7706E3426CAC33320FC3555014&_z=z)> accessed 28 March 2011.

## Bibliography

### Articles

David Flint, *RFID tags, security and individuals*, pp 165-168, *Computer Law and Security Report*, vol 22, 2006.

John Ayode, *Roadmap to solving security and privacy concerns in RFID systems*, pp 555-561, *Computer law and Security Report*, vol 23, 2007.

Kosta, E. and Dumortier, J. (2008) 'Searching the man behind the tag: privacy implications of RFID technology', the case of RFID', *Int. J. Intellectual Property Management*, Vol. 2, No. 3, pp. 276-288.

Nissenbaum, H (2004) 'Privacy as contextual integrity', *Washington Law Review*, pp. 119-158.

Poulett, Y., Rouvroy, A. and Darqueness, D. (2008) 'The Law encounters communication and information technologies: the case of RFID', *Int. J. Intellectual Property Management*, Vol. 2, No. 4, pp. 372-395.

### Article 29 Working Parties Paper

Opinion 1/2010 on the concepts of controller and processor 00264/10/EN WP 169 adopted on 16 February 2010.

Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications 00327/11/EN WP 180 adopted on 11 February 2011.

Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology 1670/05/EN WP 111.

Working document on data protection issues related to RFID technology 10107/05/EN WP 105

### Books

Daniel M. Dobkin, *The RF in RFID: Passive UHF RFID in Practice* (Elsevier Inc., 2008).

Emile H.L., *The New Everyday: Views On Ambient Intelligence* (Koninklijke Philips Electronics, 2003).

Joseph Ghetie, *Fixed-Mobile Wireless Networks Convergence* (Cambridge University Press, 2008).

Peter H. Cole, Damith C. Ranasinghe (ed), *Networked RFID Systems and Lightweight Cryptography* (Springer-Verlag Berlin Heidelberg, 2008).

Philip Robinson, Harald Vogt, Waleed Wagealla (ed), *Privacy, Security and Trust within the Context of Pervasive Computing* (Springer Science+Business Media, Inc., 2005).

Roy Want, *RFID Explained, A Primer on Radio Frequency Identification Technologies, Synthesis Lectures on Mobile and Pervasive Computing* (Morgan & Claypool, 2006).

Stephen Shephard, *RFID, Radio Frequency Identification* (Mc-Graw Hill, 2005).

Weber Werner, *Ambient Intelligence* (Springer, 2005).

### Legislation – European Union

Directive on Data Protection, 1995 (95/46/EC)

Directive on the Retention of Data Generated or Processed in connection with the Provision of Publicly Available Electronic Communications Networks and Amending Directive 2002/58/EC, 2006 (06/24/EC)

## Policy Papers

Commission Recommendation of 12.5.2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, Brussels, 12.5.2009 C (2009) 3200 final.

European Policy Outlook RFID final version, European Commission In cooperation with Federal Ministry of Education and Research.

## Websites

(Note: All websites were accessed between January 2011 – April 2011)

Article 29 Data Protection Working Party – Working document on data protections issues related to RFID 10107/05/EN WP 105  
<[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_en.pdf)>

Beijing Olympics: Going for the Gold with RFID<<http://www.aimglobal.org/members/news/templates/template.aspx?articleid=3205&zoneid=3>>

Dolby fits RFID tags in 3D Cinema Glasses - <<http://www.techeye.net/hardware/dolby-fits-rfid-tags-into-cinema-3d-glasses>>

European Commission Directives and Decisions – Coordinating European Efforts for Promoting the European RFID Value Chain <<http://www.rfid-in-action.eu/public/rfid-knowledge-platform/standards/application-independent-standards/european-commission-directives-and-decisions>>

Flying 2.0 – Enabling automated air travel by identifying and addressing the challenges of IoT & RFID technology - <<http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/flying-2.0-enabling-automated-air-travel-by-identifying-and-addressing-the-challenges-of-iot-rfid-technology-2/flying-2.0-enabling-automated-air-travel-by-identifying-and-addressing-the-challenges-of-iot-rfid-technology>>

Going for the Gold – RFID continues to impress the judges - <[http://www.webermarking.com/rfid\\_white\\_paper-printpro.html](http://www.webermarking.com/rfid_white_paper-printpro.html)>

Interview around IoT/RFID Scenario Risk Assessment - <<http://www.enisa.europa.eu/media/news-items/iot-interview>>

London Olympics 2012 – track and shield - <<http://trackandshield.wordpress.com/tag/rfid-blocking/>>

Radio tags set to combat the counterfeiters - <<http://www.bbc.co.uk/news/business-12358919>>  
RFID at the Olympics

[http://www.informationweek.com/blog/main/archives/2008/09/rfid\\_at\\_the\\_oly.html](http://www.informationweek.com/blog/main/archives/2008/09/rfid_at_the_oly.html);jsessionid=GR5TZDIAHKUURQE1GHPCKHWATMY32JVN

RFID in China <<http://www.marketresearch.com/product/display.asp?productid=1766074>>

RFID has been used by Beijing Olympic Game  
<<http://www.personal.psu.edu/bzl124/blogs/ben/2008/09/rfid-has-been-used-by-beijing-olympic-game.html>>

RFID Technology for Shanghai Expo 2010 Ticketing System <<http://www.rfid-blog.com/?p=25>>

The Korea Times – Incheon to House World's Largest Ubiquitous City  
<[http://www.koreatimes.co.kr/www/news/nation/2010/07/281\\_56996.html](http://www.koreatimes.co.kr/www/news/nation/2010/07/281_56996.html)>

The World Cup meets RFID <[http://www.forbes.com/2006/06/16/world-cup-rfid-technology-cx\\_0616rfid.html](http://www.forbes.com/2006/06/16/world-cup-rfid-technology-cx_0616rfid.html)>

World Cup Ticket will contain RFID Chips <[http://www.theregister.co.uk/2005/04/04/world\\_cup\\_rfid/](http://www.theregister.co.uk/2005/04/04/world_cup_rfid/)>

