
Radio Frequency Identification Technology (RFID): Is legal risk management relevant in consumer privacy?

Noriswadi Ismail¹

Institute of Computer and Communications Law,
Centre for Commercial Law Studies,
School of Law, Queen Mary,
University of London,
67-69 Lincoln's Inn Fields, London WC2A 3JB, UK
E-mail: n.ismail@qmul.ac.uk

Abstract: RFID is regarded as technological perfection. Prediction of market analysis asserted that the Return of Investment of RFID might reach its widespread deployment by 2010. Despite that, there are handfuls of debates on the risks of RFID data surveillance. This paper reveals some of its flaws, if uncontrollable, and how it leads to privacy debates in the spectrum of regulatory and commercial developments of selected jurisdictions. It outlines the respective stakeholders' positions and feedbacks. Significantly, it attempts to argue the relevance of legal risk management in consumer privacy as a consideration towards balancing the approach between RFID technology and privacy.

Keywords: legal risk management; privacy; UK; European Union; Malaysia; Singapore.

Reference to this paper should be made as follows: Ismail, N. (2010) 'Radio Frequency Identification Technology (RFID): Is legal risk management relevant in consumer privacy?', *Int. J. Technology Transfer and Commercialisation*, Vol. 9, No. 3, pp.268–279.

Biographical notes: Noriswadi Ismail is currently an MPhil/PhD Candidate at the Institute of Computer and Communications Law, Centre for Commercial Law Studies, Queen Mary, University of London. His PhD research is funded under the banner of Malaysian Government Agency (Majlis Amanah Rakyat) Excellent Student Scheme Scholarship Programme. His career as a counsel involves in technology related matters is in excess of ten years. Whilst in HeiTech Padu Berhad, his Key Performance Indicators involve various technology laws and strategies, regulatory compliance, intellectual property, risk management and corporate works across leading jurisdictions globally.

1 Introduction

RFID has been generally cited as one of the most evolving technologies in the world. This powerful technology remains incompatible in these industries: retails, logistics, military, libraries, surveillance and banking, yet it endures endless debates in some legal regimes and contours. When the technology was first deployed by the military,

the impact of the technology was never intended to be as sensitive as it is today. Besides, global RFID spending has increased by leaps and bounds and provides an ongoing deployment by these various industries to enjoy its value chain and business continuity. Many will view that RFID substitutes the role of barcode as a means of tagging technology despite the inhibiting level of protection towards the internal subject of the tagging – which is the data and most importantly – privacy. Because of the latter, it has prompted potential data protection and civil liberty debates across the globe. Whilst this concern is ongoing, this paper will attempt to look into how RFID technology leads to potential questions of privacy. The central attention will be on consumer privacy. Two substantive developments are discussed:

- regulatory and commercial landscapes
- legal risk management as a tool towards managing consumer privacy.

2 Radio Frequency Identification Technology (RFID): an overview

RFID is a technology which illustrates any system of identification that uses radio frequency or magnetic field variations, wherein an electronic device that activates the variations is attached to an item (Glover and Bhatt, 2006).² A tag and a reader are the components of an RFID. Tag is the identification device attached to the item for tracking, whilst reader is a device that can recognise the presence of RFID tags and read the information stored on them. The reader can then inform another system about the presence of the tagged items. The system with which the reader communicates usually runs software that stands between readers and applications, which are called RFID middleware (Glover and Bhatt, 2006).³ Even if the historical trail of this technology remains ambivalent, generally, it goes back to 1920s during the World War II (Ward et al., 2007).⁴

2.1 Radio Frequency Identification Technology (RFID) general functions

RFID could not function without frequency.⁵ The operating frequency is the electromagnetic frequency that the tag uses to communicate or to secure power. Owing to the nature of RFID that broadcast electromagnetic waves, they are regulated as radio devices. Thus, RFID systems must not interfere with other existing protected applications such as emergency service radios or television transmissions. In relation to the technical standard of Ultra High Frequencies (UHF), there are different ranges of applications in different parts of the world. Even if each country requires a different range of UHF, it is suggested that one possible global standard known as EPC global standard will be able to match varying local regulatory requirements.⁶

As mentioned, the tag and the reader are two key components to operating an RFID system. The reader functions as transmitter of the system, which contains electronics that use an external power source to generate the signal that drives the reader's antenna. In effect, it creates the radio wave. The radio wave may be received by an RFID tag, which 'reflects' some of the energy it receives in a particular way, based on the identity of the tag (Hodges and Horison, 2007).⁷ Whilst this reflection is going on, the RFID reader is also acting as a radio receiver so that it can detect and decode the reflected signal to identify the tag.

2.2 Types of categorisations

There are essentially three types of categorisations within an RFID system, which is based on the power source used by the tag, as particularised:

- *Passive tag.* This requires no power source at the tag. It does not require any batteries but utilises the energy of radio wave to effect its operation (Hodges and Horrison, 2007, p.9).⁸ In this category, it results in the lowest tag cost at the expense of the performance. Example that could be seen in practice is the usage of passive tag in individual product items for applications in supermarket checkouts and smart cards.⁹
- *Semi-passive tag.* This relies on the battery built into the tag to achieve a better performance within the operating range. In this category, the battery powers the internal circuitry during the communication; however, it is not used to generate radio wave.¹⁰ This tag is mostly fragile and expensive in the market.¹¹
- *Active tag.* It utilises batteries for their entire operation, which can generate radio wave actively in the absence of a reader.¹² In this category, the tag is capable of a peer-to-peer communication. It has larger memory when compared with the passive tag, possesses higher processing capabilities and security.¹³

Without any doubt, the semi-passive tag is the only category that does not require the involvement of a radio wave. It is also because of the costly price that compels the RFID provider to opt for the first and second categories.

3 Regulatory and commercial landscapes

Besides the USA, there are regimes that have been very serious to addressing RFID policy and regulation, such as the EU and the UK. These regimes have undertaken a very smart move to advocate a possible RFID policy in the very near future. The European Commission is undertaking an open public consultation towards establishing an RFID policy for Europe.¹⁴ The outcome will be disseminated and diffused to the member states once the European Commission would have duly substantiated the consultative deliberations. However, for the purpose of this paper, it shall restrict generally to the governing Directives of the EU and the guidance by the UK.

3.1 The European Union (EU)

In the EU, Article 29 of the EU Working Party, which is established under the auspices Article 29 of Directive 95/46/EC articulates existing privacy and data protection issues.¹⁵ On the data protection front, the Working Party has mooted the concerns on the effect of RFID technology, which may lead to violation of human rights and data protection rights. The main concern exceedingly surrounds on the possibility of businesses and governments, which have deployed RFID that is accruing and prying into the privacy sphere of individuals (Pitkanen and Niemela, 2007).¹⁶ cursorily, the published summary of responses by the RFID stakeholders has achieved a general satisfaction. In practice, however, it is asserted that the examples of RFID applications technically illustrated in the working document may not match the reality (Pitkanen and Niemela, 2007, pp.1, 2).¹⁷

It is argued that societal benefits and realistic appreciation of technical possibilities should be painstakingly inferred whilst analysing RFID applications.

Two governing Directives are applicable within the EU: Directive 95/46/EC on the protection of personal data and Directive 2002/58/EC on the protection of personal data in the electronic communications sector. These Directives outline the pre-emptive mechanism of data processing that should be complied with, by the member states.¹⁸ In Directive 95/46/EC, it could be asserted that not all RFID applications are governed under the provisions. This is due to the complex nature of RFID technology itself via the tags, the reader and middleware. Technically, the tags possess the capability to exchange information and thus, the existing provisions in the Directive have, in a way ignored and limited its scope of regulation, thus, fails to achieving technology neutrality approach. It also leads to a certain level of biasness towards existing RFID middleware and applications that are integrated with other components of technologies. In Directive 2002/58/EC, services must provide continually the possibility of using a simple means and free of charge, of temporarily refusing the processing of certain personal data for each communication. It is asserted that a PC-based system would fulfil the needs of the provision, but RFID may struggle to comply with the spirit owing to the nature of its technical interface.

3.2 Guidance in the United Kingdom (UK)

In the UK, the Data Protection Act 1998 regulates the processing of personal data. Supporting the provisions of the Act is The Data Protection Technical Guidance Radio Frequency Identification. It has outlined two scenarios in which personal data might be processed using RFID.¹⁹ First, personal data may be stored on the tags themselves, or linked to a database containing personal data. Second, if tags or individual items can be used to identify the individual associated with the item, they will be personal data.²⁰ The Act also applies when the personal data is collected, generated or disclosed using RFID either directly or indirectly. RFID users should also adopt the data protection principles of fair processing, use limitation, data quality, data retention and security. The guidance has also mentioned extensively specific data protection concerns that involve security, monitoring, profiling and technical solutions.²¹

From these developments, the UK Information Commissioner has put a very high concern on the level of surveillance in the UK's society. In a report on surveillance society, issued by the Surveillance Studies Network,²² RFID has been highlighted as one of the central issues and discussions. Even if the report does not critically analyse the technical aspects of RFID and its dangers to privacy and surveillance in detail, it has however outlined future directions to the data protection actors whenever potential RFID issues take place. Invariably, the report has analysed various social, technical, regulatory and economic perspectives, which could be applied in today's context in achieving a balanced surveillance society.

3.3 Singapore²³

Singapore was one of the earliest users of RFID technology in the world.²⁴ Singapore Land Transport Authority has been deploying RFID since 1998 in what was the world's first Electronic Road Pricing system, an automated toll-collection system used to control and manage traffic volume in the city. Singapore's National Library Board was one of the

first to harness RFID in a library environment back in late 1998, when it embedded RFID tags on books to automate the borrowing and returning of library books as well as to expedite the process of sorting books and returning them to shelves.

As Asia's leading convention venue, Singapore has long used RFID technology for tracing delegates at large conferences and conventions in the city. Singapore became the first pilot port in Asia under the USA Container Security Initiative. The island-republic is now implementing the usage of RFID seals for all containers bound for the US seaports. Selective local research institutions teamed up towards developing solutions to deploy RFID for tracing SARS contacts in local hospitals. At present, Singapore wants to leverage its existing expertise to undertake RFID research and development.²⁵

It is evident that Singapore RFID deployment has positioned the republic as the leader in the Asia Pacific region. Whilst the commercial development looks positively encouraging, it is to note that data protection provisions in Singapore legal regime is rather sectorial and piecemeal.²⁶ However, recent development in Singaporean parliament suggests that data protection and privacy should be the main priority for Singapore's industries.²⁷

3.4 *Malaysia*

Based on IDC's forecast, the Malaysia's RFID market is expected to hit RM77 million by 2010²⁸ with a compound of annual growth rate of 45.84%. Significant developments have taken place in Malaysia's RFID growth. In December 2006, the Malaysian Road Transport Department had initiated the usage of RFID license plates with the attempt to reduce the number of car thefts in the country. The plate will contain the information about the owner of the car and the vehicle. This will help the police official to know if the car has been stolen.²⁹

On 24 February 2007, Malaysia had released the world's smallest RFID microchip, which measures 0.4 mm × 0.4 mm with a built-in antenna, which can be embedded on paper.³⁰ The microchip, developed under the Malaysia Microchip Project, at a cost of US\$ 50 million (RM180 million) based on Japanese technology, is the first with multi-band frequencies.³¹ These developments envisage promising RFID growth in the Malaysian market and if the IDC analysis remains prevalent, it is predicted that Malaysia will be the central RFID investment within the South East Asian region.

In Malaysia, the effort to draft the PDP Bill started in 2000. However, the legislation is yet to be seen (Azmi, 2007).³² Rumours claimed that the Bill was motivated by the EU regulatory approach when compared with the self-regulation approach of safe harbour of the USA (Azmi, 2007; Islamy, 2007).³³ But now, the situation is otherwise and it has given quite a general setback to various industries in implementing possible data protection and privacy strategy within their organisations.

The issue of the PDP Bill delay was also mentioned in the parliament. One of the members of parliament lamented that the government was taking too long to pass laws on personal data protection, which existed in 90 countries. He further viewed that it is imperative that Malaysia hastened the enactment of the law and poignantly added that it could affect efforts to sustain Malaysia's position as a competitive outsourcing country after India and China (Ritikos et al., 2007).³⁴

The moans and groans are not only commonly shared by the Malaysian public but also multi-national corporations and foreign investors. The next question to be asked is whether the RFID technology undermines privacy and data protection. There are two

possible and skeletal answers. First, in the event the Bill has analysed thoroughly the application of emerging new technology and its convergence³⁵ vis-à-vis the privacy and data protection provisions, it is believed that it would not generally undermine due to its technology neutrality approach. Second, in the event the Bill has not achieved the same, a secondary review to the existing draft should be made pedantically. However, it should be noted that these answers may be duly substantiated once the Bill takes place in Malaysia.

4 Radio Frequency Identification Technology (RFID) and consumer privacy

The regulatory and commercial developments in different legal regimes lead to different principles and approaches. Appropriately, these regimes are undertaking a multi-layered effort to ensure that RFID remains relevant, yet there should be certain pre-emptive measures in protecting privacy. Civil liberties have also raised their eyebrows questioning the legitimacy of RFID tracking technology. The technology reveals worried danger within the privacy sphere that needs to be defused.

In 2005, consumer privacy advocates had initiated a website boycotting TESCO, which was aimed to encourage consumers' participation and awareness on the danger of this 'spy chip' technology.³⁶ Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) launched the campaign nationwide evidencing the level of protest on privacy fears. CASPIAN was particularly concerned about item-level RFID tagging, especially the potential for retailers to be able to track goods after they leave the store – which it views as invasion of consumer privacy.

The boycott against GILLETTE is also another profound example advocated by CASPIAN in 2003. It was claimed that the GILLETTE product had been embedded with an RFID chip that was able to 'spy' on consumers. Subsequently, a website to boycotting GILLETTE product was established to educate consumers the danger of RFID.³⁷ On the similar stance, BENETTON was also the subject of boycott by CASPIAN. It was claimed that the clothing that was on sale within the BENETTON's premises were embedded with an RFID chip, which was simultaneously prying on consumers' data and privacy.³⁸

CASPIAN's intention to educate the consumer privacy is commendable. On the one hand, the boycott websites suggested consumers to abandon their intention to purchase the products due to the danger of potential data intrusion via the RFID technology. But, on the other hand, CASPIAN has slightly failed to address the recommended best practices to consumers towards risk mitigation whenever the consumers would have purchased such products. Realistically, the outcome of boycott consultation between CASPIAN and the relevant RFID users like TESCO should also be channelled to the consumers for an informed notification.³⁹

4.1 Legal risk management in consumer privacy

Business continuity has always been the life cycle of organisations and companies. The term 'legal risk management'⁴⁰ is neither a new nor a coined terminology. It is a hybrid approach or strategy assessing issues within the application of risk management module and legal principles.⁴¹ Because of the hybrid nature of the module, akin to the RFID technology, RFID users should be able to adopt a strong risk management culture.

A strong risk management culture commences with these levels of risk processes: risk identification, risk analysis, risk profiling, risk mitigation, risk control and risk scorecard.⁴²

The traditional approach of risk management is mostly centred upon internal auditing exercise and internal control of organisations and companies. However, as the global market matures, risk management has been extended to controlling or pre-empting specific problems and issues, in the absence of a clear legislation or technical standard. The ultimate aim of adopting a legal risk management strategy for RFID users is to complement the industries' readiness in complying privacy and data protection provisions (Thiesse, 2006; Atkinson, 2004; Cavoukian, 2004).⁴³ This will also enable data controllers to self-regulate consumer privacy and be able to avoid potential boycotting.

Legal risk management does not favour any organisation or company but it complements these entities within their risk appetites. Generally, risk management requires a pre-emptive strategy that is realistic and achievable. For organisations, the essential strategy starts with the establishment of an RFID risk manual.⁴⁴ This manual will be able to outline brief technical illustration of the RFID usage, the sensitive technical areas that lead to privacy issues as well as how to mitigate and manage the RFID and privacy-related risk perceptions. The manual should also provide the commitment to manage the risk and at the same time, eliminating the risk that would have been derived from RFID middleware, applications and deployment. It is submitted that the manual should take into account various aspects which include cost, technical, legal, research and development, liability, operations, third party and reputation. Appropriately, RFID risk manual should also incorporate the privacy risk checklist⁴⁵ that could serve as a useful guidance and tool for the users. It is emphasised that the checklist should be based on the risk appetites of organisations and companies.

A strong RFID risk manual should be supplemented with ongoing training, dissemination, careful review and control. This is deemed to be essential to companies and organisations. In the context of consumer privacy, strong risk management processes would be able to cover potential liabilities of the RFID service provider, retailers, data controllers and any third parties who are involved with the deployment. This will boost strong confidence to existing consumers and potential consumers who intend to purchase any products or items without privacy fear and danger.

4.2 Potential arguments against legal risk management

The option to adopt this legal risk management strategy is an open option to preserve consumer privacy. It is not meant to compel organisations and companies to adopt the same in the absence of a clear privacy and data protection provisions. Apropos, this option should also be taken into consideration as a means of internal control and thus, complementing privacy and data protection terms of other countries and regimes. This option also helps retailers, hypermarkets, RFID technology service providers and data controllers to disclaim their privacy liabilities. There may be two potential arguments that underpin the adoption of legal risk management strategy, besides the typical cost and resources arguments.

First, one may argue that there are also other technical standards that could mitigate such RFID-related privacy risks. However, to counter argue, it should be borne in mind that such existing standards are restricted on specific technology adoption and the risk

assessment that is featured within any existing standards do not, in most cases, carry the levels of risk management in a whole package.

Second, one may also argue that relying on data protection terms are sufficient to overcome privacy issues and there is no need to extend such existing standards or models to examine the level of privacy and data protection within RFID technology. To debunk, it is asserted that the purpose of legal risk management model is to add the value to privacy and data protection provisions. It does not, however, lead to duplication and interface other existing standards or models. Moreover, legal risk management is deemed to be pragmatic in mitigating the issues between RFID and privacy. Besides being the added value tool towards privacy and data protection, what this model adopts is that the commendable practice is corporate governance.

5 Privacy impact assessment

It is undeniable that RFID deployment involves multi-layered relationship ranging from the service providers, third parties' applications, and third parties' middleware and to the users. In the event RFID technology has been deployed, it carries different levels of liabilities. It is very essential for these parties to conduct a privacy impact assessment so as to ascertain the sustainability of the technology in the long run. Arguably, there are no specific models that could be developed for specific industries. However, it is asserted that this assessment will be able to carry a balanced weight, which complements the legal risk management approach.

Appropriately, such an assessment should involve four layers: technical, legal, economic and social.⁴⁶ The assessment could be designed through detailed checklists corresponding to the structure of the RFID technology, based on specific industries' demands and needs. For consumer privacy, retailers should be able to ascertain the sustainability of their RFID-related policy so that an informed notification has been channelled and disseminated to the consumers. It is also indispensable for retailers to model a tailor-made RFID privacy policy for consumers' attention so that the choice and option of consumers to purchase a specific product shall not be abandoned. Strategic privacy impact assessment between CASPIAN, the retailers and consumers should also take place in the very near future. The rationale is to establish a dynamic co-existence between these focused groups, which will equalise a unique level of cooperation towards pre-empting privacy fears derived from RFID technology.

6 Conclusion

From the foregoing developments, it can be concluded that caution steps should be taken by all parties who are involved directly and indirectly with RFID deployment. Whilst the EU and the UK have provided a general model of RFID guidance, Malaysia and Singapore should expedite the lobbying to pass the motherhood of privacy and data protection legislation at the first instance. With that, it will enable to bridge the gap between RFID technology development vis-à-vis regulations. Even if the legislation would have been in place, it shall take some considerable time for both countries to reach the tested maturity stage like those of the EU and the UK.

With regard to consumer privacy, CASPIAN, being the leader of civil liberties, and consumer advocate should play a more effective cum strategic role in RFID. Whilst the boycotting and lobbying the consumers to abandon such purchases tend to be a brave move, it needs effective yet resourceful dissemination and diffusion for consumers. As suggested, a trilateral consultative process between CASPIAN, retailers and consumers shall lead the headway towards a privacy compliant RFID environment.

It is very interesting to await the outcome of the European Commission RFID EU Policy consultation. The impact shall change the current RFID landscape and consumers should be able to monitor its developments tenaciously. Whilst the outcome remains to be speculative, it is timely for RFID players and actors to embark on with the best and strategic option, which may fit their companies and organisations. As the notion 'no one size fits all' is deemed to be applicable in RFID technology context, it is needful for the industries to consider the best and practical options from various perspectives, technically, economically, legally and socially. By this, it is believed that privacy will not be a nightmare and overexaggerated by unqualified justifications and assertions. RFID remains relevant and indeed it is.

References

- Atkinson, W. (2004) 'Tagged: the risks and rewards of RFID technology', *Risk Management Journal*, Vol. 51, No. 7, pp.12–19.
- Azmi, I.M. (2002) 'E-commerce and privacy issues: an analysis of the personal data protection bill', *International Review of Computer Laws and Technology*, Vol. 16, No. 3, pp.317–330.
- Azmi, I.M. (2007) 'Why has data protection law been delayed in Malaysia? Nothing to do with Islam and who needs it anyway?', *BILETA 2006*, Malta, 6–7 April 2006, See generally: <http://events.um.edu.mt/bileta2006/29DP&I%20v1%20Ida%20madiha%20Aziz.pdf>, accessed 22 February, 2007.
- Cavoukian, A. (2004) *Tag, You're it: Privacy Implications of Radio Frequency Identification Technology*, Information and Privacy Commissioner Ontario, Toronto, see also an interesting Australian perspective: http://www.privacy.gov.au/news/04_07.html, accessed 24 March, 2007.
- Glover, B. and Bhatt, H. (2006) *RFID Essentials*, O'Reilly, pp.1–19, http://books.google.com/books?id=K2-gdK21RVEC&pg=PA74&lpg=PA74&dq=Glover+B+Bhatt+H+RFID+essentials&source=bl&ots=EhFZegfr9e&sig=z4j5ZAVALMEyrf1zdJj3RKjNlz8&hl=en&ei=cB0BS67KA5-hjAeasb2ICw&sa=X&oi=book_result&ct=result&resnum=5&ved=0CB0Q6AEwBA#v=onepage&q=&f=false
- Hodges, S. and Horrison, M. (2007) *WHITE PAPER – Demystifying RFID: Principles and Practicalities*, Auto-ID Centre, Institute for Manufacturing, University of Cambridge, Published 1 October, 2003 at pp.8, 9; see also <http://www.ifm.eng.cam.ac.uk/automation/publications/documents/CAM-AUTOID-WH024.pdf>, accessed 20 February.
- Islamy, H.E. (2007) 'Privacy and technology', *BILETA 2005*, Belfast retrievable at: <http://www.bileta.ac.uk/Document%20Library/1/Privacy%20and%20Technology.pdf>, accessed 22 February.
- Pitkanen, O. and Niemela, M. (2007) *Privacy and Data Protection in Emerging RFID-Applications*, Helsinki Institute for Information Technology HIIT, Helsinki University of Technology and University of Helsinki, VTT Technical Research Centre of Finland. This paper was presented in the EU RFID Forum 2007, retrievable at: <http://www.rfidconvocation.eu/Papers%20presented/Business/Privacy%20and%20Data%20Protection%20in%20Emerging%20RFID-Applications.pdf>, accessed 22 March.

- Ritikos, J., Samy, F.A. and Looi, E. (2007) *Same Law Apply for Bloggers, Say BN Rep*, The Star Online, Thursday 22 March; see also: <http://star-techcentral.com/tech/story.asp?file=/2007/3/22/technology/20070322114048&sec=technology>, accessed 22 March.
- Thiesse, F. (2006) *Managing Risk Perceptions of RFID*, Auto-ID Labs White Paper WP-BIZAPP-031, pp.11–17, <http://www.rfidconvocation.eu/Papers%20presented/Business/Coping%20with%20public%20perceptions%20of%20privacy%20risks.pdf>
- Ward, M., van Kranenburg, R. and Backhouse, G. (2007) 'RFID: frequency, standards and innovation', *JISC Technology and Standards Watch*, May 2006 at pp.4, 5, Retrievable online: http://www.jisc.ac.uk/uploaded_documents/TSW0602.pdf, accessed 20 February, 2007.

Notes

- ¹General Counsel/Company Secretary of HeiTechPaduBerhad. See <http://heitech.listedcompany.com/management.html>. This paper has been selected for publication subsequent to the International Law and Trade Conference (ILTC), 10-12 May, 2007 *Istanbul, Turkey*. For detailed RFID research blog: <http://the-rfid-nexus.blogspot.com>. See also his paper presented in the British Irish Legal Education Technology Association 2007, hosted by University of Hertfordshire on 16–17 April, 2007 titled "RFID: Malaysia's privacy at the crossroads?" readable at the RFID research blog.
- ²Glover and Bhatt (2006).
- ³Glover and Bhatt (2006) en above at p.1.
- ⁴See generally Ward *et al.* (2007).
- ⁵RFID typically operates within a Low Frequency (LF), High Frequency (HF), Ultrahigh Frequency (UHF) and microwave. In practice, the actual frequencies available to RFID are limited to those frequencies set aside as Industrial Scientific Medical (ISM). Frequencies lower than 135 kHz are not ISM frequencies, but in this range RFID systems are usually using powerful magnetic fields and operating over short ranges, so much so, interference is less of an issue than it might be otherwise.
- ⁶It is argued that this standard shall lead to possible RFID technological convergence towards pre-emptive technical regulation. It is hoped that governments and standard bodies should make a genuine effort to cooperate producing a global standard; see also EPC Global, "Communications Commission sets the stage for the EU to realise benefits of applications based on EPCglobal standards" Retrievable online: http://www.epcglobalinc.org/about/media_centre/press_rel/Press_Release_Commission_Communication_on_RFID_070314.pdf, accessed 20 February, 2007; see generally: <http://en.wikipedia.org/wiki/EPCglobal>, accessed 20 February, 2007.
- ⁷Hodges and Horrison (2007).
- ⁸Hodges and Horrison (2007, p.9).
- ⁹See JISC Technology and Standards Watch, May 2006 at pp.4, 5.
- ¹⁰See JISC Technology and Standards Watch, May 2006 at p.9.
- ¹¹See en 16 above, at pp.4, 5.
- ¹²See en 16 above, at p.9.
- ¹³See en 18 above, at pp.4, 5.
- ¹⁴See generally http://ec.europa.eu/information_society/policy/rfid/index_en.htm, accessed 2 May, 2007.
- ¹⁵See generally http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm; see also <http://www.edri.org/edriagram/number3.3/consultation>, and http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf respectively, accessed 22 March, 2007.
- ¹⁶See Pitkanen and Niemela (2007).
- ¹⁷See Pitkanen and Niemela (2007) see en 17 above, at pp.1, 2.

¹⁸The data should be processed fairly and lawfully; collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; adequate, relevant and not excessive in relation to the purposes; accurate and, where necessary, kept up to date. For restrictions, see http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf, accessed 22 March, 2007.

¹⁹See http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/radio_frequency_identification_tech_guidance.pdf; see also http://www.ico.gov.uk/global/search_results.aspx?search=RFID, accessed 22 March, 2007.

²⁰See http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/radio_frequency_identification_tech_guidance.pdf; see also http://www.ico.gov.uk/global/search_results.aspx?search=RFID, accessed 22 March, 2007, see en 18 above, at pp.3, 4.

²¹The concerns include ‘skimming’, ‘hacking’, ‘rogue RFID tag readers’, ‘skimmers’ ‘cloned EFID chip’, ‘blocker tags’ and ‘clipped tags’. For more detailed explanation, see the guidance at pp.5–7; see also http://www.ico.gov.uk/upload/documents/library/data_protection/introductory/radio_frequency_identification_tags.pdf, accessed 23 March, 2007.

²²As the bulk report remains an authoritative and guidance to data controller, it is suggested that the substance of the report should be inferred within the context of data protection strategy and management of the data controller. See http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf, accessed 23 March, 2007; see also the appendices of the report: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_appendices_06.pdf, accessed 23 March, 2007; see the summary of the report: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_summary_06.pdf, accessed 23 March, 2007.

²³See generally http://www.itu.int/osg/spu/ni/ubiquitous/Presentations/4_poon_RFID.pdf, accessed 2 May, 2007; see also <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN018240.pdf>, accessed 2 May 2007.

²⁴See generally <http://www.rfidjournal.com/article/articleview/1024/1/1/>, accessed 2 May, 2007.

²⁵With government help, RFID technology provider Tunity Technologies is developing EPC-compliant multifrequency RFID tags that operate in three different RF bands.

²⁶See generally <http://www.american.edu/carmel/ag0466a/Doc13.htm>, accessed 2 May, 2007.

²⁷See generally <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN012665.pdf>, accessed 2 May, 2007; see also <http://www.infowar-monitor.net/modules.php?op=modload&name=News&file=article&sid=1319>, accessed 2 May, 2007.

²⁸See http://www.theedgedaily.com/cms/content.jsp?id=com.tms.cms.article.Article_d2cc4b98-cb73c03a-29d65b00-cd5c3a50, accessed 20 February, 2007; see also http://morerfid.com/details.php?subdetail=Report&action=details&report_id=1032&display=RFID, accessed 20 February, 2007. In the Malaysia RFID 2006–2010 Forecast and Analysis, it predicted the state of the market for RFID solutions implementation in Malaysia, historical development, and prediction for the future. It also presents an end user’s RFID case study and write-up on key players that offer RFID solutions in Malaysia. Based on the study, hardware comprises largest portion of the total commercial RFID spending in 2005 at 60%, driven primarily by the purchases of readers and tags, followed by software and services which take up the remaining 40% of the RFID spending.

“Based on the IDC’s definitions, software revenue captured in this forecast is limited to RFID middleware, reader firmware, and additional enterprise middleware directly related to integrating data from the RFID layer with the enterprise application layer. It does not incorporate spending on enterprise applications and upgrades beyond middleware to accommodate and take advantage of the influx of data from RFID tags. Services included in this forecast are business process consulting, installation, systems integration, and ongoing support services. Software and services would pose more growth potential, with CAGR of 48% and 51%, respectively.”

- ²⁹The owner of the car should be nearby if the police officials want to check the driver's identity. The system will be implemented next year. The new cars would have such plates followed by the older ones. The risk what I see is that in case the RFID system of your car breaks down, then you might be pulled from your car by the cops thinking that you are a thief. See generally http://www.iht.com/articles/ap/2006/12/09/asia/AS_GEN_Malaysia_Car_Thefts.php, accessed 22 February, 2007.
- ³⁰See <http://www.hitachi.co.jp/Prod/mu-chip/index.html>, accessed 22 February, 2007.
- ³¹The Prime Minister, Datuk Seri Abdullah Ahmad Badawi, who launched the microchip yesterday, said the chip with its identification serial number, could help to counter the forgery of government documents; currency notes; halal certificates; medical products and compact discs, among others. Besides, some applications currently being developed would further assist to improve the public service delivery system. See <http://www.mida.gov.my/beta/view.php?cat=14&scat=1552>, accessed 22 February, 2007; see also <http://en.qschina.com/html/tradeinfo/html/2007/3/13/9088.html>, accessed 22 February, 2007.
- ³²See Azmi (2002).
- ³³See Azmi (2007); see also Islamy (2007).
- ³⁴Ritikos *et al.* (2007).
- ³⁵See generally http://en.wikipedia.org/wiki/Technological_convergence, accessed 22 March, 2007.
- ³⁶See generally <http://www.boycotttesco.com/>, accessed 2 May, 2007; see also <http://news.bbc.co.uk/1/hi/business/4209545.stm>, accessed 2 May, 2007.
- ³⁷See <http://www.out-law.com/page-3812>, accessed 2 May, 2007 see also <http://www.boycottgillette.com/>, accessed 2 May, 2007.
- ³⁸See <http://www.boycottbenetton.com/> accessed 2 May, 2007; see also <http://www.rfidjournal.com/article/articleview/344/1/1/>, accessed 2 May, 2007 see generally <http://www.out-law.com/page-3465>, accessed 2 May, 2007.
- ³⁹See generally <http://www.ipc.on.ca/images/Resources/up-rfidtips.pdf>, accessed 3 May, 2007.
- ⁴⁰See generally http://en.wikipedia.org/wiki/Enterprise_Risk_Management, accessed 24 March, 2007.
- ⁴¹Globally, the preferred risk management module is enterprise risk management. See generally http://en.wikipedia.org/wiki/Enterprise_Risk_Management, accessed 24 March, 2007.
- ⁴²See generally <http://www.admin.ox.ac.uk/riskmgmt/overview.shtml>, accessed 24 March, 2007.
- ⁴³Thiesse (2006); see Atkinson (2004); see also Cavoukian (2004).
- ⁴⁴RFID risk manual can only be established once organisations or companies have undergone the levels of risk management exercise. See also an example of risk management checklist: http://www.lms.ca/@pdf/Risk_Management_Checklist.pdf, accessed 24 March, 2007.
- ⁴⁵See generally <http://cyber.law.harvard.edu/ecommerce/privacyaudit.html>, accessed 24 March, 2007; see also <http://www.itcinstitute.com/display.aspx?id=2499>, accessed 24 March, 2007.
- ⁴⁶See <http://csrc.lse.ac.uk/asp/aspecis/20050060.pdf>, accessed 3 May, 2007.