科技法學評論，4 卷 2 期，頁 97（2007）

科法新論

無線射頻辨識系統（RFID）之應用對隱私法制之影響*

王郁琦**

摘　要

無線射頻系統（RFID）可被視爲現今最具潛力的無線感應設備，由於其獨有的特點，相較於紅外線感應系統，更能突破許多物理上的限制，而基於研發與生產方式的進步，得持續降低使用成本，也因此不論政府或是商業團體都計劃將此種科技運用於辨識個人或是物品。一如許多先進科技所帶來的便利，其同時也對現行法制產生相當衝擊；本文將著眼於 RFID 對個人資訊隱私權的影響，進行法理上的探究，除了對 RFID 的發展做簡要的介紹外，亦將分析 RFID 所可能產生的隱私權侵害，另透過資訊隱私權理論的延展，針對 RFID 進一步提出其受管制的可能性與模型，以期在促進科技使用、便利與個人權利保護兩者之間，取得適當的平衡點。

關鍵字：無線射頻辨識系統、RFID、資訊隱私權、公平資訊運作原則

---

* 本文為國科會委託專題研究案之成果（計畫編號：NSC 94-2414-H-128-007）。本研究案之研究助理為世新大學法研所宋佩珊同學。宋同學於本案執行上認真負責，對研究成果之產出具有重大之貢獻，作者特此表示謝意。

** 世新大學法律學系副教授。

投稿日：2007 年 7 月 16 日；採用日：2007 年 9 月 2 日

Cite as: 4 Tech. L. Rev., Oct. 2007, at 97.

The Impact of RFID Applications on Privacy Laws

Yu-Chi Wang

Abstract

Radio frequency identification system (RFID) seems to be the radio device with most potential in contemporary society. Factors like advanced features and mass production result in the continuing reduction of its cost. Both the public and private sectors plan to employ this technology on individual identification and product logistics. As much as the use of many other technologies, RFID not only makes our lives more convenient, but also raises many privacy concerns. This essay analyzes the privacy issues raised by RFID technology after a brief introduction of its various applications. Different models of privacy regulation will be discussed and an adequate one will be subsequently proposed to strike a better balance between efficiency and convenience of the use of this technology and a need to provide acceptable privacy protection.

Keywords: radio frequency identification system, RFID, information privacy, fair information practice

1. 前言

編碼的型態隨著時代的演進有不同的型態，由於電腦庫存系統的興起，近代較爲普遍使用的就是「條碼」（bar-code），其不但增加了商品存貨紀錄的正確，同時也增加了商業行爲活絡。現在，無線射頻系統（Radio Frequency Identification, RFID）的建立，爲編碼開啓了新的紀元；RFID 微型晶片具有良好且限制較少的傳輸能力，同時擁有較佳的儲存能力。隨著技術的進步，RFID 製造成本一直在降低，因而 RFID 成爲編碼世界的主流，並且突破了傳統條碼式編碼的侷限——同種編碼物識別程度低。因爲 RFID 晶片可儲存獨一無二的編碼，簡單而言，即是給予商品「身分識別碼」，就算是一模一樣的商品，也可以從編碼中加以區分，對於品管、倉儲管理都有很大的幫助，同時其也衍生了使用 RFID 的另一個功能——防僞，所以各國都對 RFID 的引進投入相當的資源，不論是商品或是個人的識別，都可與 RFID 進行結合。但另一方面，RFID 也引發一些隱私權上的疑義，本文將從 RFID 的介紹，進而討論 RFID 所產生的隱私權威脅，並對這些威脅提出管制模型的探討，以期尋求科技發展與隱私權保護的平衡點。

2. RFID 的應用

2.1 RFID 的發展與種類

RFID 晶片是無線射頻系統的核心，視標籤的技術而定，這一片 2 公厘見方的標籤，能儲存獨一無二編碼序號，甚至是簡單的資料訊息。目前廣爲區分主動式（active）RFID 與被動式（passive）RFID，依其是否具有獨立電源而發送訊號而定[1]，茲分述如下：

1　渡邊桂三，「從基礎面了解 RFID」，日經 BP RFID 編輯部編，周湘琪譯，RFID 技術與應用，頁 28（2005）。

2.1.1 主動式（active）RFID 標籤

主動式 RFID 標籤具有內建的電源系統，亦可稱爲「內建電池的標籤」[2]，可在收到讀取器的訊號時而執行回應，接收範圍可達 1 英里，儲存記憶容量一般爲 128KB，特殊技術可使其提升到 4MB[3]，並且可以對儲存資料進行修改與刪除，具有長距離無線通訊、位置偵測與大容量記憶體的優點，但是也因爲其自有電源，同時有電池壽命與成本高等缺點[4]，故目前多用於維修紀錄、兒童定位之運用[5]。

2.1.2 被動式（passive）RFID 標籤

被動式 RFID 標籤相較於主動式 RFID 標籤，並不具有內建的電源，因而感應距離必須限制在幾公尺內[6]，記憶容量不若主動式 RFID 標籤來得大，無法進行長距離通訊與位置偵測等應用，但是因爲其結構較爲簡單，成本低廉，多用來進行物流的管理，透過標籤內所儲存的獨一無二編碼來連結中央資料庫進行倉儲的控制，許多知名大型連鎖店皆在積極導入此種技術，如美國的 Wal-mart、英國的 Tesco[7]；此外，許多電子扣款系統也採取此種被動式標籤來紀錄消費，如由智慧卡中心發行的悠遊卡即是一例。

而 RFID 標籤共同的特性在於，因爲其係透過無線電頻率進行傳輸，相較於紅外線感應系統（如條碼的讀取即是一例），其不需以特別角度進行讀

---

2 同前註，頁 28。

3 CHRIS GARDNER, AUTOMOTIVE AFTERMARKET RFID: MEMA INFORMATION SERVICES COUNCIL WHITE PAPER 2004, at 5 (2004), *available at* http://www.miscouncil.org/Automotive% 20Aftermarket%20RFID.pdf.

4 渡邊桂三，前揭註 1，頁 29。

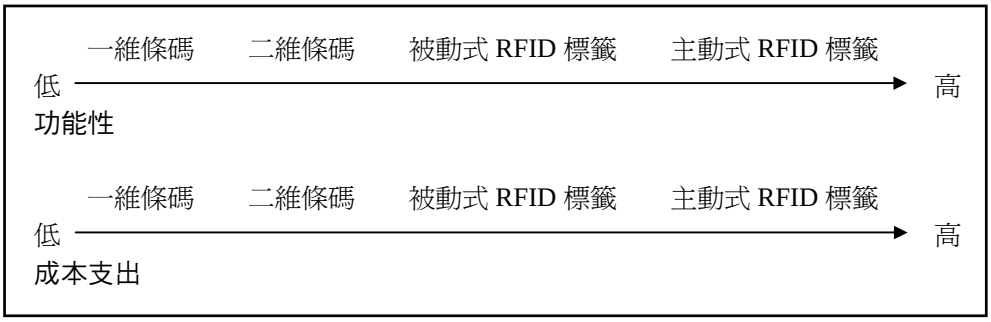
5 Mary Catherine O'Connor, *RFID Keeps Objects, Kids from Going Astray*, RFID J., Mar. 20, 2006, *available at* http://www.rfidjournal.com/article/articleview/2209/1/1/.

6 GARDNER, *supra* note 3, at 5.

7 Jonathan Collins, *Tesco Revises RFID Plans*, RFID J., Apr. 7, 2006, *available at* http://www.rfidjournal.com/article/articleview/2243/1/1/.

取，而且可同時大量進行訊息收發，節省許多感應時間，對於高速的感應也較紅外線感應系統來得強，所以可節省物流的成本，不過 RFID 標籤仍受限於一些物理因素的影響，例如：金屬物的障礙會影響讀取成功率，但是其所具有的優點仍使得政府與企業投注相當高的注意。

一般來說，目前被動式 RFID 標籤因爲成本的考量，在使用上的比例要較主動式 RFID 來得高；但是受限於其記憶容量的大小，被動式 RFID 標籤無法如主動式 RFID 標籤一樣記錄許多相關資訊，但其記憶體容量可形成的數列變化，卻要較傳統的一維條碼與二維條碼來得多，因此得產生獨一無二的編碼系統，也使其在物流上的使用更爲廣泛。



圖一　識別技術功能與成本的比較

資料來源：本研究整理

2.2　RFID 運用於物品與個人

目前 RFID 標籤運用在識別物品的討論上論述頗爲驚人，但是嚴格來說，RFID 標籤運用在識別個人的討論也不容小覷，兩者都是著眼於 RFID 晶片的小巧便利與獨一無二識別碼儲存，對於不論是物品或是個人資訊的管理上都帶來實質的助益，同時更精準地掌握資料客體的狀態與歷程，以下茲就

RFID 標籤在物品與個人兩者之應用進行介紹[8]。

2.2.1 應用於識別物品

以產品的編號來看，如果透過傳統一維或二維條碼的呈現，在倉儲管理系統上，可看出是商品的品名、顏色，甚至於出產時間等資訊，但是因爲 RFID 記憶體容量可容許較多的數列變化，即可透過此種特性對商品進行細目化編碼（item-level），因而即使是相同的產品，編號也不會有所重複，形成獨一無二的編碼，而成爲產品的 ID。之後，透過中央資料庫的建置，當讀取機讀取標籤內獨一無二的編碼時，即可透過網路的建置得知該產品的相關資訊，並進一步利用所得資訊來進行更有效的運作。

目前關於 RFID 應用於物品之上，最爲廣泛討論並且由政府所主導者，就是美國正在進行立法討論的「減少僞造與仿冒藥品法（Reducing Fraudulent and Imitation Drugs Act）」草案；有鑑於藥品僞造的情況日趨嚴重，參議員 Vitter 提出了因應此種現象的草案，其中規定許多與藥品附加 RFID 微晶片等內容，另外也包括許多藥品包裝的細節，例如：僅能使用塑膠密封包裝，而不能使用較不嚴密的瓶裝；其主要是爲了監控藥品的流程，以防止僞造；目前該草案在國會的能源與商業委員會裡被擱置，因此正在進行重新討論，但是美國食品藥物管理局（FDA）對於就藥物附加 RFID 晶片的計畫似乎是勢在必行[9]。

2.2.2 應用於識別個人

以目前 RFID 用來識別個人的形式，約可分爲將標籤植入於體內者、置

---

8 RFID 的應用日新月異，本文僅就其中做概略的介紹，更多的相關應用可參考以下書籍：日經 BP RFID 編輯部編，周湘琪譯，RFID 技術與應用（2005）；刁建成，RFID 原理與應用（2005）；NTT Data Ubiquitous 研究會，荒川弘熙編，葉珠娟等譯，RFID 是啥？：實現「無遠弗屆社會」的 RFID 技術（2005）。

9 Beth Bacheldor, *GAO Issues Drug Report, Senator Sponsors Bill*, RFID J., May 10, 2006, *available at* http://www.rfidjournal.com/article/articleprint/2327/-1/1/.

於個人貼身物品者與附加於識別個人之證件者。將 RFID 晶片注射於體內者，因爲其所引發的隱私權爭議過高，在商業上的運用甚少，多使用於性犯罪者的監控爲多。

將 RFID 晶片附加於識別個人證件的部分，政府與商業團體都有計劃的進行推廣。在商業的部分，瑞士一家連鎖電影院就在會員卡上附加 RFID 晶片，使會員得以利用該卡進行訂票與購買產品[10]；在政府的部分，多國皆在推行 e-passport 的計劃，美國在 2005 年 1 月於舊金山國際機場開始進行測試[11]，日本也於 2006 年 3 月開始進行測試[12]，兩者皆計劃在測試結束評估後進行全面的換發。但是值得注意的是，e-passport 附加 RFID 晶片的目的與儲存生物辨識相關資訊的目的並不相同，RFID 晶片的附加是爲了快速通關等便利性考量，而生物辨識則是在避免犯罪[13]，但兩者皆具有防止僞造的功用。

而將 RFID 標籤置於個人貼身物品的型態，多以手環的方式來呈現，許多遊樂園區透過讓遊客在入園時戴上此類 RFID 標籤而進行服務的提供，出園時再行取下，屬於短暫識別的效用[14]。至於長時間的識別，目前較廣泛討論者爲美國醫療科技資訊機構 Verichip 對於植入性 RFID 晶片的發展；該公司最主要的行銷商品，是一種植入型的 RFID 晶片，裡面紀錄病人的醫療資

---

10 Jonathan Collins, *Swiss Moviegoers Use RFID to Buy Tickets*, RFID J., Mar. 30, 2005, *available at* http://www.rfidjournal.com/article/articleview/2230/1/1/.

11 Mary Catherine O'Connor, *DHS Completes E-Passport Test at SFO*, RFID J., Apr. 18, 2006, *available at* http://www.rfidjournal.com/article/articleview/2274/1/1/.

12 Jonathan Collins, *Japan Issues E-Passports*, RFID J., Mar. 28, 2006, *available at* http://www.rfidjournal.com/article/articleview/2224/1/1/.

13 Laurie Sullivan, *RFID Passport Tests to Begin at San Francisco Airport*, TECHWEB NEWS, Dec. 30, 2005, *available at* http://www.informationweek.com/story/showArticle.jhtml?articleID=175800183.

14 Maija Palmer, *Theme Park Tags on to ID Chip Expansion*, FINANCIAL TIMES (London, England), Apr. 15, 2006, at 3, *available at* http://www.ft.com/cms/s/0/ff6d7f30-cc1c-11da-a7bf-0000779e2340.html.

訊，當病患無法陳述其醫療狀態時，醫院急救醫療人員可以透過掃描晶片獲取資訊，其原始的想法是鑑於美國在 911 時，大批的消防隊員進入現場救災時，因恐在救難過程中遭遇危難以致於救難人員因失去意識或受傷而難以辨識身分，要求消防隊員必須在胸前標明其徽章服務號碼，因此激發了 Verichip 公司推行植入性晶片的概念[15]，目前該 RFID 晶片植入計劃製造特殊的讀取機以及晶片予 66 所醫療院所，並且提供相關的教育訓練[16]，此科技的擁護者最有利的論點即在於該科技可運用於阿茲海默病人的身上，不但有助於患者病歷在醫療時的取得，同時也可減少醫療錯誤的發生。但是 Verichip 的應用也帶來了許多隱私權上的疑義，多因其涉及到醫療資訊敏感性的問題，本文亦將於後進行相關的討論。

RFID 的運用，其實增加許多時間與成本的節省，實質上帶來許多便利，但是 RFID 的應用更加大了資料的蒐集與儲存，更多的資訊將掌握在利益團體或政府的手中，在科技所帶來的正面影響之外，同時我們也無法忽視其對於個人隱私權的侵犯，所以 RFID 對於隱私權的影響勢必無法避而不談；針對這些相關的隱私權疑慮，本文將針對以下問題進行論述：

1.RFID 的應用對隱私權帶來什麼樣的影響？

2.法律是否應允許業者利用 RFID 進行資料蒐集？

3.對於 RFID 應用應透過法律或是市場自律的方式來管制？

4.RFID 的應用如果要以法律方式管制的話，管制應採取何種模式？

本文將就這些 RFID 應用所帶來的爭議與影響，分別闡述如後。

---

15 Verichip Corporation, http://www.verichipcorp.com/company.html (last visited Aug. 27, 2006).

16 Bert Hill, *Verichip Looks for $45.8M U.S. in IPO*, OTTAWA CITIZEN (Canada), Dec. 31, 2005, at H1.

3. RFID 所引起的隱私權爭議

3.1 透過 RFID 獨一無二的編碼來蒐集大量的消費者購買資訊，是否對個人的隱私權產生侵害？

由於 RFID 能儲存獨一無二的商品編碼，貨物或商品等於有了精確的識別碼，其與傳統條碼式的編號不同之處在於：物品的生產歷程、運輸供應，以至於到消費者手中的一切細節，皆可透過編碼連結中央資料庫來做紀錄建立與更新，使得公司能夠更精準地知道顧客的消費習慣，例如：可得知顧客在條件式折扣或是有特別贈禮的時候購買，有效的分析消費者個人購買習慣[17]，也因此顧客就無法確保其隱私。一般來說，學者普遍認爲使用 RFID 來附加於商品之上，會助長私人公司追蹤顧客的消費資訊[18]。John M. Eden 認爲這裡所涉及的消費者購買資訊蒐集，以美國的法律體系來看，在個人隱私權保護與促進商業的發展之中，由於現行的廣告主張效用，所以常透過購買模式的預測來進行鎖定式行銷，而憲法中的言論自由支持商業言論，因而導致現行的隱私權法理普遍支持商業性言論；而從 RFID 的利用來看，其是爲了廣告行銷有效的應用，所以藉由 RFID 的使用來獲得消費者購買資訊不會受隱私權法理的阻礙[19]。

現代社會下隱私權所應具有的功能包括：對於個人生活的自我決定、培養一個活潑有創造力的個人，作爲社會的安全閥以及給犯錯者自新的機

---

17 John M. Eden, *When Big Brother Privatizes: Commercial Surveillance, the Privacy Act of 1974, and the Future of RFID*, 2005 DUKE L. & TECH. REV. 20, ¶ 12, *available at* http://www.law.duke.edu/journals/dltr/articles/PDF/2005DLTR0020.pdf.

18 *See id.* ¶¶ 5-6; *see also* Harry A. Valetk, *Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies*, 2004 STAN. TECH. L. REV. 2, ¶ 93, *available at* http://stlr.stanford.edu/STLR/Articles/04_STLR_2/fsarticle.htm.

19 *See id.* ¶ 18.

會[20]。而從隱私權的功能爲原點來探討個人購買資料蒐集的影響，首先，這樣的資訊蒐集在進一步分析後，將會在某種層面形成個人側寫，因而對個人在社會群體中的地位與外在評價產生影響，故縱使其並非高度敏感之資訊，但是一旦此類資訊公開，仍有對個人生活產生侵擾，並且就個人產生不一樣的人格側寫，進而阻礙活潑有創造力的人格建立。再者，基於購買資訊所建構的「鎖定式行銷（targeted-advertising）」大大提升了行銷的成功率，但是從另一面來看，當業者醉心於此中行銷方式所帶來的效益，是否有可能更執著於加強個人行銷，因而造成個人生活更多的侵擾？對個人不受干擾的生活產生嚴重威脅。由上所述，消費購買資訊的蒐集或許不應該被全面禁止，但是該類資訊對個人隱私權來說，仍能造成一定的危險，影響個人的社會生活，而加上 RFID 的應用，此類資訊將會快速大量的累積，故更應認真看待之。

3.2 攜帶 RFID 標籤的個人在通過 RFID 讀取機時，是否因為位置資訊的揭露而對個人隱私權造成威脅？

在某些情形下，消費者團體憂慮在 RFID 裡儲存這些獨特的識別資料來識別商品進而銷售給顧客，此後即可透過機器的讀取而用來追蹤個人[21]，甚至可利用 RFID 晶片監控顧客的攜帶物[22]；除此之外，當 RFID 是用來識別個人時，獨一無二的編碼與個人之連結更爲緊密，目前 RFID 透過讀取機定點的接收訊號能得知其附加主體「經過」地點，但是在 2003 年 5 月，ADS（Applied Digital Solution 公司）成功測試了植入式全球定位（GPS）設備，

---

20 王郁琦，「工作場合中電子郵件隱私權之研究」，資訊、電信與法律，頁 90-91（2004）。

21 Reuven R. Levary, David Thompson, Kristen Kot & Julie Brothers, *Radio Frequency Identification: Legal Aspects*, 12 RICH. J.L. & TECH. 6, para. 10 (2005), *available at* http://law.richmond.edu/jolt/v12i2/article6.pdf.

22 Valetk, *supra* note 18, ¶ 93.

更精確取得個人的位置資訊[23]。目前隱私權理論的建構，傳統上從「隱私的期待」爲出發點，法理上並不保護公共場所位置資訊的蒐集，以美國聯邦最高法院在 United States v. Knotts 一案中的論證，政府將無線追蹤設備附加於化學製品的罐子上，之後以其來追蹤被告；最後法院認爲個人在公開大道騎乘摩托車，並無法對其移動具有隱私的期待；法院指出慣例的隱私權期待，並不涵蓋於在公開場合移動，並且能以視覺觀察得知的監視行爲[24]，但是，以 Katz v. United States 案[25]來看，電話亭原本是一個公開的場合，但是談話人一把電話亭的門關起來就變成了私密的場合，所以一旦進入了私密的場合，個人的行爲就成爲憲法所保障的隱私範圍。所以位置隱私一般來說就難受到憲法所承認的原因在於其是公開場合的行爲，又一般隱私權的法理在於不受干擾權利，進入公開場合屬於自願的放棄不受干擾的權利，不受憲法隱私權的保護。因此，個人在公共場合的位置資訊無法置於資訊隱私權的保護傘之下，透過 RFID 所獲得的位置資訊蒐集也並不違反憲法基本權的保護。

然而，縱使是公共位置資訊的揭露，對於個人來說仍具有一定程度的影響；首先，如在公寓大廈的大門口設置監視錄影機，其雖被認係公開場合，但其牽涉到個人進出私密領域的資訊，如仍將其視爲非隱私權所保障的範圍，不無疑問。不過，如果從隱私權的法理是個人資料自主權利的論點出發，而非以「隱私的合理期待」作爲論述的原點，則在公開場合的位置隱私就有思考的空間，因爲這樣的一個資訊蒐集，對個人的資訊自主產生很大的威脅，因爲如此一來，個人對其資訊的掌控就產生了動搖，所以如果認爲隱私就是個人資訊的自主權，位置隱私的保障似就可認爲係憲法隱私權所保障的範圍，目前我國大法官釋字第 603 號解釋裡也納入資訊自主權的概念，並且闡釋資訊自主權的內涵包括「保障人民決定是否揭露其個人資料、及在何

---

23 Margarett Driscoll, *This Girl's Parents Want to Keep Track of Her by Microchip: Paranoia or Wise Precaution?*, SUNDAY TIMES (London), Sept. 8, 2002, at 24.

24 United States v. Knotts, 460 U.S. 276, 281 (1983).

25 Katz v. United States, 389 U.S. 347 (1967).

種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權。」但是其也敘明資訊自主權並非讓資訊主體得漫無目的擴張使用，國家仍可在符合憲法第 23 條之情形下，就其限制之[26]。

再者，如果一個家庭決定安裝無線感應系統，在各個房間的入口地板上裝設自動感應的 RFID 讀取機，每一個家庭成員皆在其鞋子上裝設主動式標籤。如此一來，這些移動資訊與個人識別資料相連，就可以得知家庭成員在房內的移動模式。因此，一個裝配 RFID 的房間是否仍被視爲僅個人所掌控的私人空間[27]？此皆突顯位置資訊並非不具有隱私權上的爭議，同時也威脅到個人隱私權所具有之功能；最後，即使是公共場所，個人仍可在某種程度上期待匿名移動，而 RFID 與個人識別資料結合後，監視的型態從公眾移動轉變爲個人的移動[28]，難謂沒有影響現行個人資訊隱私權的運作與範圍認知。雖然在憲法的層次無法確立位置隱私的保障，但是並不代表在法律的層次不能就位置隱私進行保障。故由 RFID 所蒐集的個人位置資訊，其妥適性應進行討論並且思量其管制的模式，尋求維護隱私權核心價值與促進科技發展的最適平衡點。

3.3 利用 RFID 蒐集大量醫療資訊是否對資訊主體之隱私權產生更大的侵害？

醫療資訊在個人資訊裡屬於敏感資訊，其對資訊主體影響甚遠。目前美國在醫療產業所研發的 Verichip，其特色爲將晶片植入於人類皮膚之下，在

---

26 司法院釋字第 603 號解釋，解釋理由書。

27 Timothy P. Terrell & Anne R. Jacobs, *Privacy, Technology, and Terrorism: Bartnicki, Kyllo, and the Normative Struggle Behind Competing Claims to Solitude and Security*, 51 EMORY L.J. 1469, 1504 (2002).

28 Gary T. Marx, *Seeing Hazily (But Not Darkly) Through the Lens: Some Recent Empirical Studies of Surveillance Technologies*, 30 LAW & SOC. INQUIRY 339, 393 (2005).

醫院配備特殊掃描儀器的情況下，只需要透過一個掃描器進行掃描，即可獲得病人的醫療病史以及紀錄[29]。本產品設計目前的主要目的在於幫助急診部門減少診療錯誤與增加部門效率[30]。但是，目前已經有隱私權團體針對此項科技提出質疑，對於 RFID 植入的醫療安全性、未經授權連結該系統的可能性，以及缺少有效的法律在廣泛植入應用前進行規制，易增加資料被侵入的風險、違反匿名性及侵害其他個人隱私權的可能性[31]。也就是說，被視爲敏感性的資料，是否可透過和 RFID 結合來進行資訊傳遞，已經引起高度爭議。

3.4 執法人員透過 RFID 進行非接觸式感應進行無法院命令之搜索，是否侵害個人隱私權？

刑事搜索隨著科技的進步，其在概念上也一直有所改變，一般概念上符合正當法律程序的搜索指的是執法人員必須取得法院所簽發之搜索票，否則不得無理由對人民進行搜索或扣押；早期，美國聯邦最高法院於在 Olmstead v. United States 案中，一個私酒販者主張政府的監聽違反第 4 與第 15 憲法增補條款，所以應該受到節制[32]。但是以 Taft 法官爲首的最高法院並不同意這個論點，因爲第 4 增補條款的搜索與強行進入的保護並不適用於政府的監聽行爲，主要認爲監聽的行爲並不構成實質上的入侵，同時也尚未有明確的證據或資料因監聽而獲得，法院同時拒絕了原告對於第 15 增補條款的主張，因爲原告並不是被強迫去使用電話來提供有罪的證明[33]。後來，在 Katz v.

---

29 Waseem Karim, *The Privacy Implications of Personal Locators: Why You Should Think Twice Before Voluntarily Availing Yourself to GPS Monitoring*, 14 WASH. U. J.L. & POL'Y 485, 491 (2004).

30 VeriChip: Privacy Policy, http://www.verichipcorp.com/content/company/privacy (last visited Aug. 27, 2006).

31 Eden, *supra* note 17, ¶ 13.

32 Olmstead v. United States, 277 U.S. 438, 466 (1928).

33 *See id.* at 462.

United States 案，最高法院主張使用電子設備來規避直接進入當事人居住環境的結果，其並不具任何合憲上的意義[34]，法院提出新的隱私權期待定義，其內涵爲個人展現主觀的隱私權期待，以及這個期待是被社會認爲合理的[35]。

而到最近，美國聯邦最高法院於 Kyllo v. United States 一案中表明，在屋外使用熱感應系統來探視大麻的栽種，已經構成美國憲法第 4 增補條款的搜索，屋內的空間是所有科技的禁區，不論該科技是否具侵入性，都應取得法院的搜索票使得進行屋內資訊的蒐集[36]；但是，如果 RFID 的接收讀取器已經成爲「一般大眾使用」之儀器時，其隱私的期待將會受到限縮，因而利用感應設備來讀取 RFID 晶片的違憲性亦將受到重新評價[37]。但以現階段而言，執法人員仍無法利用 RFID 的非接觸感應特性，在無搜索票的情形之下，取得其所需之相關資訊，如此一來才能保障人民的基本權利。

4. RFID 管制的妥適性

4.1 從隱私的觀點是否允許 RFID 應用於資料蒐集？

4.1.1 用來識別商品的 RFID

基於 RFID 將聚集龐大的資訊，所以同時必須建立大量的資料庫，如果此種資料庫與個人識別資料庫有了連結，則物品即可代表個人。最後，在缺少個人同意之下，對個人進行側寫，對隱私權將產生一定的衝擊[38]。而在 2003 年 11 月，35 個隱私團體發表了一份聯合的聲明書[39]，該份聲明所主張

---

34 Katz v. United States, *supra* note 25, at 353.

35 *See id.* at 361 (Harlan, J., concurring).

36 Kyllo v. United States, 533 U.S. 27 (2001).

37 王郁琦，「生物辨識技術對隱私權的影響」，2005 全國科技法律研討會論文集，頁 304（2005）。

38 Katherine Albrecht, *Supermarket Cards: The Tip of the Retail Surveillance Iceberg*, 79 DENV. U. L. REV. 534, 560-62 (2002); *see also* Valetk, *supra* note 18, ¶¶ 92-94.

39 Consumers Against Supermarket Privacy Invasion and Numbering et al., RFID Position

的論點，後來成爲最常被引用來批評 RFID 的論點。首先，由於 RFID 擁有較佳的隱藏能力，所以當其附加在物體或資料上時，個人將缺少這一方面的認知，也就是無從知悉 RFID 的存在；再來，因爲隱藏的讀取機設定，將會使得個人在無所知覺的情形下，被讀取所攜之商品資訊；最後，一旦獨一無二的 RFID 編碼序號與個人識別資訊做連結後，將會依據 RFID 之編碼對個人進行資料的蒐集，更有甚者，一旦 RFID 的標準統一後，任何一個讀取機皆可自行讀取所有的商品，則將會對個人隱私權產生莫大的影響[40]。

透過 RFID 來進行資料蒐集，尤其是如果採行了「細目化（item-level）」的編碼方式，就業者而言，在倉儲管理、蒐集顧客相關資訊就更爲詳細與精準，但是也如前所述產生了許多隱私權上的疑慮，那是否因此就禁止利用 RFID 來就商品進行標示呢？自從電腦與網路興起後，資訊大量聚集因而對個人資訊隱私權產生威脅；從某種層面來看，科技發展所造就的新型態資料蒐集與儲存，對於資訊隱私權產生了威脅性，今日所面對的問題是，我們應該爲了保護個人隱私權而限制科技的發展嗎？如果要探討這樣的問題，其核心的關鍵應該爲，這樣的新科技是否造成了新的資訊隱私權利侵害，或是加強了原受法律所保護的資訊隱私權之侵害；在 RFID 科技應用於資料蒐集上，以顧客購買資訊的蒐集爲例，在現實世界中，顧客消費資訊的儲存與使用已經比比皆是，全球最大的網路書店 Amazon[41]，大量處理、紀錄並且使用顧客消費紀錄，法律也並不禁止此種的資料探勘（data mining），故透過 RFID 來蒐集顧客購買資訊，也僅是「加強」資訊的蒐集；另外，有關 RFID 所產生的公開位置資訊問題，其可與全球定位（GPS）系統的討論

Statement of Consumer Privacy and Civil Liberties Organizations, *available at* http://www.privacyrights.org/ar/RFIDposition.htm (last visited Sept. 22, 2006).

40 Jerry Brito, Relex, Don't Do It: Why RFID Concerns Are Exaggerated and Legislation Is Premature 17, *available at* http://www.lawtechjournal.com/articles/2004/05_041220_brito.pdf (last visited Sept. 22, 2006).

41 *See id.* at 18.

相似，兩個隱私權侵害的疑慮因爲其並未造成新的隱私權侵害，或是對法律現行所保護的隱私權產生侵害，故不應禁止之。惟雖然 RFID 科技不應禁止，此尚不代表 RFID 應用於資訊的蒐集不可進行適度的規範；而這樣的規範應透過法律層次的介入，或是應用市場機制來達到保護資訊隱私權的目的，茲分述如後。

4.1.2 用來識別個人的 RFID

如果說用來識別物品的 RFID，會在商品資料庫與個人識別資料有了連結後，造成物品編號即可用來代表個人的情況，進而產生侵害隱私權的疑慮，則用來識別個人的 RFID 將會引起更大隱私權爭議。目前利用 RFID 來進行個人識別身分的應用主要有公領域的身分證、護照、健保卡等個人識別，出入管制，員工證，會員卡以及儲值卡等，茲分別就其情形論述之。

首先，有關醫療識別的部分。在 2004 年 12 月，美國食品藥物管理局（FDA）依據聯邦食品、藥物及化妝品法（Federal Food, Drug, and Cosmetic Act）將這項醫療植入晶片計劃，歸類爲該法的第二級人類植入設備[42]，因爲其可透過對 Verichip 的進行「特別控管（special controls）」[43]來執行該晶片的應用，也就是說提供履行標準的公布、行銷後的監控、病患登記、指導方針的發布以及適當行動以確保特別控管的執行。其原因在於 Verichip 的晶片植入計劃雖然不須經由 FDA 核准後始能進行市場行銷，但是其仍具有一些潛在的風險需要注意，例如：身體組織的不良反應、植入設備的體內移動、資訊安全的威脅、植入失敗、電子掃描錯誤、電子干擾、核磁共振造影的互

42 Classification of Implantable Radiofrequency Transponder System for Patient Identification and Health Information, 69 Fed. Reg. 71,702, 71,703 (Dec. 10, 2004) (to be codified at 21 C.F.R. pt.880), *available at* http://www.fda.gov/ohrms/dockets/98fr/ch0466.pdf (last visited Sept. 23, 2006).

43 21 U.S.C. § 360c(a) (2000 & Supp. Ⅳ 2004).

斥等[44]，其中關於資訊安全的威脅的問題，FDA 在 2004 年 12 月 10 日所發布的「第二級特別控管指導方針文件：病患識別與醫療資訊之植入性無線頻率傳輸系統（Guidance for Industry and FDA Staff Class Ⅱ Special Controls Guidance Document: Implantable Radiofrequency Transponder System for Patient Identification and Health Information）」[45]指出，此類透過晶片所得之醫療資訊，必須符合四個資訊安全的要件：機密性（Confidentiality）、完整性（Integrity）、有效性（Availability）以及有責性（Accountability）[46]，故 Verichip 的使用只要符合特定的控管方法，仍得應用於醫療之上。

再者，以公領域的身分證、護照、健保卡等個人識別應用而言，其目的主要是在於防僞以及增強行政效率，由於 RFID 晶片的感應便利性與儲存容量等優點，能夠使得國家在人民資料庫管理上更有效率，並且減少僞造證件的流通，對政府來說能夠減少國家安全以及犯罪行爲的防治成本，對人民來說也可減少行政流程上的時間花費；目前美國[47]、日本[48]等皆已在推行電子護照（e-passport），以達到護照防僞以及加速通關速度的目的，如果基於目的之使用以觀，其係爲促進公共利益，難謂有應全面禁止之理由，身分證與

---

44 Classification of Implantable Radiofrequency Transponder System for Patient Identification and Health Information, 69 Fed. Reg. 71,703.

45 CENTER FOR DEVICES & RADIOLOGICAL HEALTH, U.S. DEP'T OF HEALTH & HUMAN SERVICES, CLASS Ⅱ SPECIAL CONTROLS GUIDANCE DOCUMENT: IMPLANTABLE RADIOFREQUENCY TRANSPONDER SYSTEM FOR PATIENT IDENTIFICATION AND HEALTH INFORMATION (Dec. 10, 2004), *available at* http://www.fda.gov/cdrh/ode/guidance/1541.pdf (last visited Sept. 23, 2006) [hereinafter GUIDANCE DOCUMENT].

46 此資訊安全的四個要件將於第五部分進行說明。

47 Laurie Sullivan, *RFID Passport Tests to Begin at San Francisco Airport*, TECHWEB NEWS, Dec. 30, 2005, *available at* http://www.informationweek.com/story/showArticle.jhtml?articleID=175800183.

48 Jonathan Collins, *Japan Issues E-Passports*, RFID J., Mar. 28, 2006, *available at* http://www.rfidjournal.com/article/articleview/2224/1/1/.

健保卡等應用亦同[49]。

最後，出入管制功能的 RFID 應用，工作場合的識別應用、商業行爲中所廣泛運用的會員卡制度以及儲值卡的 RFID 使用（如悠遊卡的使用），其主要目的通常在於一時的辨識，透過自動比對系統來控管個人，RFID 晶片擁有多角度的感應功能，比傳統的紅外線感應系統要容易讀取，且其儲存容量可以容納獨一無二的編號，能排除以往容易盜拷複製單一識別號碼的缺點，因此只要有助於該系統合法使用目的之達成，基於管理效能的考量，誠難認其有應禁止的理由。

由上可知，RFID 的功能與應用主要集中於「防止僞造」與「加速行政與管理效率」，因此在符合特定資安標準的情形下，不應完全禁止其使用與發展，只是應該就其所蒐集資料的特性進行不同程度與方式的控管，也因此，接下來的問題在於 RFID 的運作，應該使用何種方式來管制，本文將分述如後。

4.2 RFID 資料蒐集的管制應透過市場機制或是法律介入？

在 2004 年期間，聯邦貿易委員會（Federal Trade Commission, FTC）舉辦一場名爲「RFID：應用與受牽連的消費者」研討會，與會人士包括政府、

---

49 但是英國政府為減低民眾疑慮，其內政部澄清，該國即將發行之身分識別卡將不會加裝 RFID 晶片，但是會另外挑選其他無線頻譜裝備來達到非接觸感應的效果，同時會選擇特殊的讀取機，將感應範圍限縮到幾英吋。Philip Johnston, *ID Cards Will Track Where People Go*, THE DAILY TELEGRAPH (London), Jan. 28, 2006, at 4, *available at* http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2006/01/28/nid28.xml&sSheet=/news/2006/01/28/ixhome.html. 我國過去也有類似之健保 IC 卡爭議，但爭議重點並非在於健保卡可否 IC 化，而是 IC 健保卡中記載之資訊種類應否加以限定。可參閱王鍾渝，健保 IC 卡書面質詢，立法院全球資訊網：http://www.ly.gov.tw/ly/01_introduce/0103_leg/leg_main/leg_news/leg_news_02.jsp?ItemNO=01030700&tableid=1215&tablename=cw_ly1500&stage=5&lgno=00008（最後點閱日期：2007 年 7 月 14 日）。

業界與學術界，共同達成「RFID 使用者應該自律」的結論；產業界代表成功的說服 FTC 的律師將 RFID 視爲與其他蒐集個人資訊科技所相當之應用[50]。但是，觀察現行資訊隱私權運作的情形來看，具有以下幾種現象：

4.2.1 透明度的缺乏造成資訊不對稱[51]

資訊一向是有效市場機制的重要元素，如果資訊沒有公平的揭露，就會產生不公平的市場運作，內線交易即是一例。在個人資訊使用的範疇裡，因爲業者對於資料掌控的透明度過低，造成資料主體也就是消費者難以得知其資料使用、儲存以及使用期限等問題，故無法透過消費者有效的監督促使企業合理的應用其掌握之資訊，因而產生資訊不對稱的情況，使得大眾無法依據產業間的自律規則，來獲得產業使用資訊的妥適性，從而讓市場機制的運作難以達到資訊保護的目標。

4.2.2 資料的聚集與交換的簡易性造成評估的可能性降低[52]

由於資訊電子化後，不論是資料的蒐集或是交換都大大減少了難度與成本的支出，所以造成大量資訊被頻繁的運用，外界也難以得知個人資訊會何時被銷毀以及如何使用、如何與其他資料相結合與流通，因爲電子化所帶來的便利性提升，使得資訊一旦流出或是流出後監控失敗，其所相關的風險將會很難估算[53]，舉例來說，一旦銀行發生資安的問題，其所流出的大量個人金融與識別資訊，因爲複製資訊的金錢與時間成本大幅減低，所以擴散與使用的層面將難以估計，從而造成風險管理的難度升高。

---

50 Laura Hildner, *Defusing the Threat of RFID: Protecting Consumer Privacy Through Technology-Specific Legislation at the State Level*, 41 HARV. C.R.-C.L. L. REV. 133, 151 (2006).

51 James P. Nehf, *Incomparability and the Passive Virtues of Ad Hoc Privacy Policy*, 76 U. COLO. L. REV. 1, 20 (2005).

52 *See id.* at 21.

53 *See id.* at 21-22.

4.2.3 警示機制尚未具有效性[54]

資安警示的影響深度可分爲現時與往後，在現時的影響可讓資訊主體做出立即的資訊控制，例如：更改密碼等，而往後的影響可建立消費者對業者資安的評價，讓業者提高資安的自我要求，發展警示機制可以幫助人們評估許多商業活動的隱私運作，也可使得資料主體在資料外洩時進行一些風險的控制，並且利用公眾的印象，促使企業主重視資訊安全的問題，同時也可讓產業受到相關單位的監督，保護資料主體的權益。

4.2.4 科技的解決方案影響力極小[55]

對於科技所產生的侵害，一般來說亦希望能透過科技的方式，來保護消費者的權益，但是，消費者使用科技來防止隱私權的侵害，如果缺少法律的保護，握有經濟實力的業者將會發展更佳的資料蒐集模式來抵抗之，在資源掌握懸殊的情形下，消費者往往無法對抗業者的新進科技，故無法透過科技的方式來有效杜絕隱私權的侵害。

4.2.5 隱私權的侵害因為沒有公開而無法進行責任歸屬的討論[56]

此種現象與前述現象有所關連，可認爲是前述現象所導出；由於隱私權被侵害的時候，資料主體鮮少知悉，同時個人很難去追蹤責任的歸屬，因而造成業者在資料流出造成侵害時，消費者無法得知其權利受損，亦無從請求賠償，往往要經過一段時間後，才能察知資料外洩的事實，但在法律缺少相關規定的情況下，難以個人之力對抗企業。

綜上所述，由於資料管理的成本大幅降低，企業對於個人資訊的運用更有彈性，但是也因爲個人與企業對資訊掌控的能力大不相同，加上企業對於個人資訊的運作常有隱匿的情勢發生，而畢竟使用資訊揭露的對稱才能產生

54 *See id.* at 23.
55 *See id.* at 25.
56 *See id.* at 27.

公平的市場機制[57]，因此現實資訊隱私權的運作，難謂可透過完全放任的市場機制來進行[58]；縱然普遍認爲政府一旦利用管制的方式介入新科技，將會對該科技的發展帶來一定的影響，但是「禁止使用」與「合理管制」係不同之概念，本文認爲，RFID 爲物流與現代生活所帶來的便利性不容忽視，同時其既非造成新的隱私權侵害態樣，亦非對原本受法律所保護的隱私權造成侵害，自難有具說服力的論點來禁止 RFID 的應用，惟 RFID 的使用仍對個人隱私產生一定的影響，故仍應以資訊隱私權所建立之原則爲基礎，就其使用進行法律上的規範，以在消費者個人資訊的保護，與支持新科技發展間取得平衡點。

5. RFID 管制型態之探究

5.1 商品識別 RFID 之使用管制模式

承上所述，資訊隱私的保護在現行商業運作下，似乎無法利用自律來達到保護的目的，在這樣的情況下，法律的適時介入成爲必要，也因此法律管制的程度就成爲首要思考的問題。有關 RFID 應用的完全放任與完全禁止使用，於前已分別論析其窒礙難行之處，故 RFID 的使用必須在折衷的管制模式下進行，以下茲就公平資訊使用原則、EPCglobal 隱私指導方針與嚴格的 RFID 隱私權保護機制進行討論，以求在科技發展與隱私保護中取得適當的平衡點。

---

57 *See generally* Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869 (1996).

58 林宏達，「你看廣告我付錢」，商業周刊，第 958 期，頁 54（2006）。亦可見商業周刊網站：http://www.businessweekly.com.tw/article.php?id=22314。

5.1.1 公平資訊使用原則

5.1.1.1 公平資訊使用原則之概述

「公平資訊使用原則」最早在 1973 年由美國的健康教育以及福利部（Department of Health, Education & Welfare）所提出，主要內容包含幾個個人資訊隱私的基本原則：資料庫公開原則、個人參與原則、責任歸屬原則、使用限制原則與目的明確原則[59]；之後，經濟合作暨發展組織（Organization for Economic Co-operation and Development, OECD）在 1980 年也提出了個人資料保護的指導方針，其中在第二部分，由蒐集限制爲中心，提出幾項保護個人資料的原則，茲分述如下：

1.蒐集限制原則

任何個人或是相關資料的蒐集應該受到限制，而且此類的蒐集手段應該立基於合法與公平的意義之上，也就是資料主體必須適度的同意、認知該資料蒐集的主題[60]。

2.資料品質原則

個人資料的使用必須合乎蒐集的目的，並且爲目的所必須之使用，該資料同時應維持精準、完整以及最新資訊的狀態[61]。

3.目的明確原則

個人資料蒐集的目的應該在資料蒐集前即確定，不得在資料蒐集後或是經常使用後始確立目的，同時資料使用僅限於滿足蒐集目的之達成，不得進行於蒐集目的不相容或是逕行更改目的後之使用[62]。

---

59 FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS 7 (1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf (last visited Sept. 24, 2006).

60 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, ¶ 4, *available at* http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1, 00.html (last visited Aug. 27, 2006).

61 *See id.* ¶ 8.

62 *See id.* ¶ 9.

4.使用限制

蒐集的個人資料不得被揭露，或是進行與「目的明確原則」相違背之使用，除非基於當事人的同意或是法律的授權[63]。

5.安全防護

個人資料必須使用合理的安全防護以抵擋遺失的風險或是未經授權的接取、破壞、使用、修改以及揭露[64]。

6.資料庫公開

資料庫所有關於個人資料的發展、使用以及政策應秉持公開的原則。個人資料的使用方式，也就是個人資料的存在與種類、使用的主要目的以及資料控制者的常駐與身分，應可讓資料主體使用簡便的方式取得其相關資訊[65]。

7.個人參與原則

資料主體應該具有以下的權利：

(1)獲得來自資料管理員或是其他相似之工作者之信息，用以確認資料管理者是否擁有與資料主體相關之資料。

(2)資料主體可以在以下之條件下，要求資料管理員以容易理解的形式，通知資料主體與之相關資料的訊息：

①合理存在的期限內

②合理的收費

③使用合理的方法

(3)資料管理員如果拒絕資料主體 1.、2.之要求，應給予資料主體理由，並且資料主體得就該理由進行申訴。

(4)資料主體可就其所相關資料進行申訴，如果申訴成功，資料主體可就

63 *See id.* ¶ 10.

64 *See id.* ¶ 11.

65 *See id.* ¶ 12.

其資料進行消除、更正、增加完整性與增補[66]。

8.責任歸屬

資料管理員應該遵行有效符合前述原則的規範，並且負起相關責任[67]。

5.1.1.2 小結

以上幾個原則成爲近代資訊隱私權保護制度的基石，但是其所規範者爲一般的資料蒐集，鑑於各式資料蒐集科技的應用，「公平資訊使用原則」似乎難以完善保護資料主體的權利，以 RFID 的使用爲例，其缺少告知消費者晶片存在以及銷毀等資訊，將使消費者缺少此一方面之認知，導致隱私權上的侵害；故目前最大的 RFID 推行組織 EPCglobal 針對 RFID 的應用，在現行的隱私權規制架構上，就 RFID 應用的特性進行管制，提出較適合 RFID 隱私權保護模式的指導方針，茲分述如下：

5.1.2 EPCglobal 隱私指導方針

5.1.2.1 EPCglobal 隱私指導方針之概述

EPCglobal 是一個規劃電子產品編碼（EPC：Electronic Product Code），並與 RFID 相結合，進而串聯世界所有物品編碼資訊爲主的組織[68]，由國際條碼總會（EAN International）和統一編碼委員會（UCC）所共同成立的非營利組織[69]，係目前全球推行 RFID 的主要單位之一；目前 EPC 的編碼系統受限於 RFID 晶片的容量，多爲 96bits 的編碼，日後亦會隨著 RFID 容量的增大，逐步發展更細目的編碼系統[70]，也就是說關於商品的編碼描述會越來越

66 *See id.* ¶ 13.

67 *See id.* ¶ 14.

68 企業指南，EPCGlobal Taiwan 網站：http://www.epcglobal.org.tw/epcg/jsp/a41.htm（最後點閱日期：2006 年 8 月 3 日）。

69 EPCGlobal 組織，EPCGlobal Taiwan 網站：http://www.epcglobal.org.tw/epcg/jsp/a121.htm#01（最後點閱日期：2006 年 8 月 3 日）。

70 EPC 編碼，EPCGlobal Taiwan 網站：http://www.epcglobal.org.tw/epcg/jsp/a21.htm#（最後點閱日期：2006 年 8 月 3 日）。

詳盡。基於在使用電子產品編碼後，將會聚集大量的資訊，所以 EPCglobal 也制定了 RFID 相關的隱私權指導方針，該指導方針因爲係對於 RFID 特性所做的管制，普遍爲業界所接受，其相關內容爲：

1.消費者標示（Consumer Notice）

消費者應該被清楚的告知商品或是包裹有 EPC 科技的使用。這些警告標示應該附有 EPC 的 logo 或是可從商品包裝上識別。

2.消費者選擇（Consumer Choice）

消費者必須被告知其可就購買物品上的 EPC 標籤進行移除、毀壞。

3.消費者教育（Consumer Education）

消費者必須有機會得到 EPC 發展的資訊，以及該科技的提升程度。當公司使用 EPC 時，必須採取適當的方法來使消費者熟悉該項科技，並且幫助消費者瞭解該科技與其所帶來的利益。EPCglobal 將會對於公司與消費者提供論壇，以讓雙方在符合本指導方針的情況下學習並且使用此項科技。

4.紀錄之使用、保存與安全性（Record Use, Retention and Security）

EPC 並不包含、蒐集或是儲存個人識別資訊。如同傳統的條碼科技，與 EPC 相關的資料蒐集、使用、維護以及保護，將由 EPC 的會員公司依據相關法律來執行。公司會依據相關法律發布個人識別資料保存、使用與保護的政策[71]。

5.1.2.2　小結

由於 EPCglobal 隱私指導方針未能對消費者提供更完善的保護，尤其是普遍使用所造成的威脅、缺乏選擇加入機制的控制以及透過商業運作來進行價格誘導，使得消費者出賣其部分隱私權，在在讓消費者的權益受到威脅，也因此爲隱私權團體所抨擊，認爲保護密度不夠，無法有效保障消費者資訊隱私，故有學者提出對消費者保護更爲完善的原則，茲分述如後：

71　EPCglobal Guidelines on EPC for Consumer Products, *available at* http://www.epcglobalinc.org/public/ppsc_guide/ (last visited Sept. 17, 2007).

5.1.3 嚴格的 RFID 隱私權保護管制機制

5.1.3.1 嚴格的 RFID 隱私權保護管制機制概述

此種型態的管制模型，除了原本所廣爲應用的資訊隱私權保護原則外，尙增加三項主要的原則，分別爲：

1.資料最小化原則

將資料蒐集的數量降到最低並且盡可能維持個人資料匿名性[72]。此原則的適用將會使得資料蒐集是否爲最小化受到檢驗，因此能使業者的資料蒐集謹慎爲之，另外資料匿名性的使用，資料內容與資料主體的連結產生障礙，也將使得資料因爲不當侵入或外洩所產生的隱私威脅大幅降低。

2.選擇加入（opt-in）原則

一般來說，選擇退出（opt-out）機制對於資料蒐集者來說，其負擔的成本較低，而選擇加入原則與事前同意原則在某種層面上具有相同的意義，同時採取選擇加入（opt-in）原則的成本將會使公司使用 RFID 的成本增加，因爲需花費時間與成本取得消費者的同意[73]。

3.反差別待遇原則

私人公司不得差別對待拒絕其個人資訊透過 RFID 或是相似科技進行蒐集的客戶，例如：折扣或是優惠[74]。

5.1.3.2 小結

透過嚴格的隱私權保護機制，消費者的保護會更爲完善，RFID 使用對隱私權的影響將會降到最低點，但是相對也影響了商業運作。首先，資料最小化原則難以衡量，尤其是匿名性的要求主要使用在敏感性資料，並且用於統計觀察時才有意義，如果要求商業機構貫徹匿名性要求，對商業運作將會產生窒礙，削減了 RFID 所應帶來的便利，反而扼殺了 RFID 的發展。再

---

72 Eden, *supra* note 17, ¶ 30.

73 *See id.* ¶ 31.

74 *See id.* ¶ 32.

者，反差別待遇違反了商業運作的原則，因爲透過使用 RFID 以獲得個人資訊，如果是在合法的情況下蒐集，並以提供折扣作爲誘因，並非讓消費者毫無購物選擇，同時該原則也會剝奪私人公司蒐集自願提供的個人資訊權利。最後，如果在商品使用 RFID 的情況下，實行選擇加入機制，應聚焦在獨一無二識別編號與個人識別資訊結合之情形，如果單純使用 RFID 編碼來追蹤商品，而無與個人識別資訊連結之虞時，則不需與選擇加入機制相結合，如果一併實施選擇加入機制，廠商若未獲得消費者的事前同意，則不得使用 RFID 來追蹤製造產品，實妨礙 RFID 的發展，一旦貿然採取將會阻礙 RFID 的推行，因此這些原則完全使用的話，相形之下將引起很大的爭議。

5.1.4　平衡的 RFID 隱私權保護機制

5.1.4.1　平衡的 RFID 隱私權保護機制概述

綜觀以上的管制模型與機制，其各有存在的理論與依據，但是也有缺憾與不足之處：「公平資訊使用原則」雖然確立了近代資訊運用的最基本要求，但是其無法就 RFID 應用的特性提供適切的管制；「EPCglobal 隱私指導方針」雖然針對 RFID 的特性提供了相關的隱私指導方針，但是對於讓消費者認知相關資訊的部分卻相當薄弱；而「嚴格的 RFID 隱私權保護管制機制」雖然對於消費者的保護相當完善，但是完全以消費者立場出發的論點與保護機制，對於業者無疑是沉重的負擔，容易讓新科技在萌芽之初即受到嚴格限制，最終無法讓 RFID 的應用對人類生活產生貢獻。本文在此就 RFID 之特性、衡量隱私權與商業運作之間的平衡，對 RFID 的管制提出適當的模式，其應包含以下原則：

1.OECD 公平資訊運作原則

透過公平運作原則的運作，可以使得資料的蒐集獲得較爲完善的管制，一方面適度保護了資料主體的隱私權，另一方面也可讓業者利用合法蒐集的資料進行有效的商業運作，不論是對商業運作或是個人權利的行使，都能獲得妥適的管制與保護，因此公平資訊運作原則應作爲資訊隱私保護原則所遵

守的基礎規範，故透過 RFID 所蒐集的資料，自應當遵守該原則所揭示的規範爲妥。

2.充分告知機制

由於 RFID 晶片的小體積特性，大幅減低了使用的成本，但也因此增加了消費者察知其存在的可能性，因此特別需適用充分告知機制的建立，讓消費者能夠從選購商品時就得知 RFID 晶片的存在，同時亦須明確標示晶片所在之位置，以使消費者能獲得完整的 RFID 資訊，縱使因爲其他原因無法由業者在銷售點毀壞 RFID 的傳輸能力，亦可由消費者自行取出或損毀。

3.消費者選擇

在購物結帳時，業者應主動詢問消費者是否欲消除 RFID 晶片的傳送能力，讓消費者可以選擇其將物品攜出後，商品是否具有與感應器傳輸的能力，藉以保障其購買後的資訊隱私權。縱使消費者願意讓業者取得其購買資訊，也僅止於購買程序完結前，消費者可選擇是否交出比約定更多的資訊。

4.選擇加入（opt-in）機制

由於 RFID 晶片更爲詳盡的編碼，因而使每一個商品都具有了獨一無二的編碼，一旦與個人識別資訊結合後，其所紀錄的消費資訊將更爲深入，因而在利用 RFID 所得到之資料，與個人識別資料要進行連結時，必須透過選擇加入機制的建立，讓消費者重新檢視其所提供的隱私權內容與影響，建立合理的隱私權期待爲妥[75]。

5.1.4.2 小結

從消費者保護的觀點來看，此種模式仍讓經濟上優勢的業者大量掌握消費者的資訊，依據現行市場運作的情形，有關消費者識別資訊的運作，仍無法提高透明度，同時消費者對資訊隱私權的認知薄弱，因此平衡之隱私權保

75 在此特別強調者為，選擇加入機制的重點在於透過 RFID 所蒐集的資訊，與個人識別資料連結的情形，如果業者僅適用於倉儲管理，即不需採用選擇加入機制，不然會呈現荒謬的局面。

護機制所能達到的效能，仍有待觀察。但是平衡之 RFID 隱私權保護機制得以讓 RFID 有效推廣，但是同時也能適度的保障消費者資訊隱私權，讓 RFID 能夠增加倉儲管理的功能被廣泛運用，減低商業成本促進商業運作，並且也能兼顧消費者權益的保護，應爲目前較佳的 RFID 管制模式。

弱 ⟶ 強

不管制	公平資訊使用原則（FIPs：Fair information practuce）	EPCglobal 隱私指導方針	平衡之 RFID 隱私權保護機制	嚴格的 RFID 隱私權保護機制	完全禁止
	1.蒐集限制 2.資料品質 3.目的明確 4.使用限制 5.安全防護 6.資料庫公開 7.個人參與 8.責任歸屬	1.消費者標示 2.消費者選擇 3.消費者教育 4.紀錄之使用、保存與安全性蒐集限制。（FIPs 原則）	1.FIPs 原則 2.充分告知機制 3.消費者選擇 4.選擇加入機制	1.FIPs 原則 2.資料最小化 3.選擇加入 4.反差別待遇	

圖一　商品識別 RFID 之使用管制模式強弱圖

資料來源：本研究整理

5.2　個人識別 RFID 之管制型態

個人識別 RFID 的管制型態，應以商品識別的管制型態作爲基礎來討論，因爲識別個人的管制型態會因其所蒐集資訊的特性，產生不同程度的管制，但是不論是商品或是個人的識別，其所立基的管制模式應爲相同，只是尚須就其應用的方式進行不同的程度增改，因此在此爲避免複述前所論及之模式，故直接對個人識別所應考慮的要件進行討論。一般來說，進行個人識別的 RFID 應用皆應符合以下共通要件：

1.用於識別個人

RFID 晶片的存在目的應該爲識別個人，而非物品或商品，因爲兩者對於隱私權的侵害程度不一；一般來說因爲商品或物品有流轉的可能，與個人的連結性不若直接識別個人那麼強，在處理上也應有所不同，再者，直接識別個人，其所相關的資訊種類甚多，與商品識別所引起的隱私權疑慮也有所不同。

2.RFID 晶片儲存獨一無二的序號或編碼

正因爲 RFID 具有強大的儲存能力，因此其特點即爲可儲存獨一無二的序號或編碼，如此一來即可透過這種編碼或序號，將個人從數列中特定出來，達到精確識別的功用，如果缺乏此種獨一無二編碼的儲存，即喪失 RFID 晶片的價值，並且喪失識別的功效。

3.得與可識別之個人資料直接與間接連結

通常在 RFID 晶片中所儲存者爲序號，利用此組序號，即可進入資料庫進行個人資訊的搜尋或處理等應用，因此序號或編碼的價值在於資料庫的連結，透過與個人識別資訊的結合，對於隱私權的影響即大爲擴張，因此 RFID 序號必須得與個人可識別資料進行連結，才具有使用與討論的價值。

以上所述爲識別個人的 RFID 應用所共通具備的要件，但是因爲個人識別的範圍甚廣，依據其應用性質的不同，對於個人基本權利所產生的影響也有所不同，一般來說，因爲個人帶著獨一無二的編碼或序號在感應器之間穿梭，個人的位置資訊將無所遁形，這將隨著感應器分布的密度產生不同程度的影響，但是無疑所有識別個人的 RFID 應用，都將對個人位置資訊有所牽涉，本文依序將說明目前普遍的個人識別 RFID 應用，並依據其應用目的的不同，羅列其另需符合的要件與所產生的隱私權疑慮，進行隱私權相關議題的討論與探究。

5.2.1 醫療識別

醫療資訊一向被視爲敏感性資訊，與個人隱私權和社會生活有很大的關

連，因此在處理涉及此類的資訊時，必須賦予持有者更高的安全標準，來防止醫療資訊的濫用與外洩。RFID 晶片特有的技術與優勢，也被醫療產業所看中，由業者計劃導入來幫助醫療資訊的處理，以增加效率與降低醫療過失的發生，除了共通要件之外，其應用應尚須符合「作爲醫療識別」的要件，此種個人辨識的目的是爲了醫療資訊的連結，對於個人進行醫療相關服務的提供，涉及大量敏感性資訊，因此其管制程度自當與其他應用有所區隔；同時，透過 RFID 來識別個人，用以連結個人醫療資訊，除了共通的位置資訊問題外，尚涉及醫療隱私權的問題。

美國食品藥物管理局（FDA）在 2004 年 12 月 10 日所發布的「第二級特別控管指導方針文件：病患識別與醫療資訊之植入性無線頻率傳輸系統」[76]中提到，此類透過晶片所得之醫療資訊，必須符合四個資訊安全的要件：機密性（Confidentiality）、完整性（Integrity）、有效性（Availability）以及有責性（Accountability），茲就其內容分述如下[77]：

1.機密性（Confidentiality）

資料與資訊僅向資料主體所授權的人士揭露，擁有該資訊的單位，以及相關的資料處理，必須符合資訊主體所授權的使用事項，並且於其授權的時間內進行；此亦代表必須確保未授權者不得接近此類資訊。

2.完整性（Integrity）

資料與資訊必須保持其正確與完整性，也就是必須確保不適當資料修改的禁止。

3.有效性（Availability）

資料、資訊與資料庫在其目的所需以及有效時間存續內，必須保持可接近性以及實用性，也就是資訊在需要時具有實質的效益。

76　GUIDANCE DOCUMENT, *supra* note 45.

77　*See id.* at 4.

4.有責性（Accountability）

透過合法資料使用授權者的識別與證明，以確保接近處理資訊的合法性。

Verichip 作爲世界上最有規模的醫療植入式 RFID 晶片計劃，以機密性（Confidentiality）、完整性（Integrity）、有效性（Availability）以及有責性（Accountability）作爲基礎，依據 FDA 的要求，發布該公司的隱私權政策，作爲醫療資訊「特別控管」的標準，其主要的內容如下：

1.病人隱私權的部分

(1)病人的資訊，包括識別號碼皆屬於機密。

(2)醫療院所不得以任何理由使用病患的資訊，除非是對病患爲之。

(3)沒有病患事前的書面同意或是聯邦法規、州法所允許的情況，醫療院所不得向任何人或團體就病患的資訊進行揭露；醫療院所必須同意依據聯邦法或是州法以保護病患資訊的隱私與機密。

(4)醫療院所使用本系統所提供的資訊必須遵守 1996 年的醫療保險可攜與責任法案（Health Insurance Portability and Accountability Act, HIPAA）。

2.隱私權聲明

(1)病人擁有主控權：不論是資料庫裡的內容或是有資格接取資料庫的人員，都由病人自行控制。

(2)資訊接近與修改權。

(3)資訊使用終止權。

(4)申訴管道的建立[78]。

以上隱私權政策的揭露，最特別之處在於其將病人的識別號碼亦視爲機密，因此與其識別個人的應用相較之下，其資訊隱私權的防護也較完全。由於醫療資訊被視爲敏感資訊，因此任何連結都應該經過嚴格的限制，除了必須是法律授權以及經合法程序核准的情形，除非經當事人同意之外，概不得

78 VeriChip: Privacy Policy, *supra* note 30.

向其他第三人揭露相關資訊；而在 RFID 使用的情形，因爲無線傳遞，則增加了攔截資訊的機會，從而對隱私保護產生危害。也因此，Verichip 將識別號碼視爲機密資訊，對病人的保護來看，是更進一步；但是，僅是將識別號碼視爲機密，仍難防止訊號攔截的行爲，一旦獲得病人的 RFID 識別號碼，即可藉入侵資料庫或是其他接近資料庫的手段，獲得病人的醫療資訊。因此，從使用方式以觀，將識別號碼視爲機密尚須搭配「傳送資料加密」的手段爲妥，如此才能保障病人在傳送識別號碼時的機密性[79]。

5.2.2　身分證、護照、健保卡等公領域身分識別

基本上在國家所發給的證件上附加 RFID 晶片，功用主要是防止僞造與加速行政效率，因此除了共通要件外，尚包含「使用公領域之編碼系統進行編碼」的要件，其雖爲公領域的編碼系統，但是對於私領域的經濟活動有強大的作用，因此其與私領域的編碼系統有截然不同的影響力，進一步來說，公領域的編碼模式具有統一性、全國性的特點，並且有推定可信的效果，縱使以全國性大型企業所進行的編碼系統來看，其也不具有公領域編碼的效果，簡單來說，辦信用卡需要國民身分證號碼，但是不會有銀行要求申請人提供家樂福會員卡的卡號。也因此，除了涉及個人位置資訊隱私權的問題，此類的應用尚涉及個人公領域識別資訊的隱私權問題。

雖然此種技術的應用與在證件運作系統中儲存生物辨識檔案的使用目的不同，因爲生物辨識系統使用的目的是在於加強個人辨識與防止犯罪[80]。但是基於兩者都是用來識別公領域身分的目的，兩者所涉及的隱私權問題在某種程度上是可以互相涵蓋的，而由於生物辨識技術對於隱私權所涉及的個人資訊隱私權層面更爲廣泛，相較之下其相關的隱私權議題討論也更爲活絡。

79　現行已有速度較快，並且耗費較低能量的加密技術，並可適用於主動式 RFID 晶片。Mary Catherine O'Connor, *SecureRF Creates New Encryption Method*, RFID J., Nov. 9, 2005, *available at* http://www.rfidjournal.com/article/articleview/1973/1/1/.

80　Sullivan, *supra* note 47.

以歐盟、英國、加拿大、澳洲等國爲例，其針對生物辨識技術皆做出相關的指令規範，本文在此整理相關規定，以適用於 RFID 個人識別管制模型之上，茲分述如下：

5.2.2.1 監督機制的建立

任何公領域個人識別資料庫的建立，必須由獨立的單位來監督管理其儲存、使用、更改與消除等流程，並且秉持透明運作的原則，讓個人識別資料能在穩定、安全的環境中控管，以英國爲例，即爲該國所推行的生物辨識身分卡，由國務大臣指派成立國家身分計劃委員會（National Identity Scheme Commissioner）負責監督行政單位的運作。

5.2.2.2 資料庫接近的資格限制

就個人識別資料庫的使用人員進行管理與嚴格的資格限制，除非有法律授權或是經合法程序所取得之允許進入權，否則不得接近資料庫之內容，以維護資料庫安全與外洩風險的減低，藉以保障個人資訊隱私權。

5.2.2.3 資料庫連結的限制

除非有法律授權、當事人同意或是經合法程序的批准，否則應該禁止各單位的個人識別資料庫進行連結，以避免藉由職權透過單一識別號碼在各資料庫進行遊走，對個人資訊隱私權產生嚴重危害，並且擴大資料庫外洩的風險。

5.2.2.4 唯一識別原則之排除

RFID 運作與個人身分確認的強度雖不若生物識別技術對於個人的連結性強，惟在適用 RFID 晶片適用後個人證件的可性度增高，難謂不會將之是同個人的依賴性升高，故仍應避免將 RFID 證件視爲唯一的識別方式爲妥[81]。

---

81 王郁琦，「生物辨識技術對隱私權的影響」，科技法學評論，第 3 卷第 2 期，頁 80-93（2006）。

5.2.3　會員卡

在會員卡的部分，其識別功能通常與其購買資訊蒐集做結合，除了提供折價優惠外，亦用以實施「鎖定式行銷（targeted-advertising）」，因此本類型的 RFID 應用，除了應符合共通要件外，亦需符合「以商業運作爲目的」的要件，透過該要件的適用，其所需的管制亦有所不同，同時此種應用除了涉及位置資訊的隱私權問題外，尚涉及顧客消費資訊的隱私權。此種以商業行爲作爲使用 RFID 進行個人識別的使用，在現行法律規範之下係屬對隱私權合理的侵擾，惟在進行該項行銷時必須遵守資訊隱私權相關的規定，從學理上來說，就必須遵守「公平資訊使用原則」。

惟在會員卡的部分，尚須特別說明的部分爲「資訊主體同意原則」的部分；理論上來說，同意原則並未定於事前，也就是未結合「選擇加入原則」，將使消費者的保護蒙上陰影，因此爲了保護消費者隱私權，應該在此適用「選擇加入原則」，使得業者在發行 RFID 會員卡之前，必須先獲得消費者的同意，提供明確的隱私權聲明，並且合於目的之使用爲宜。

5.2.4　通行管制、工作場合的使用

通行管制與工作場合的 RFID 識別使用，通常建立於僱傭或是契約關係之上，因此部分隱私權將因契約關係有某些程度的退讓，只要該退讓並不侵害隱私權的核心意義即可，因此除了需符合共通要件外，尚須符合「以管制作爲目的」的要件，此種管制除了出入管制外，尚包括使用管制，主要爲增加控管的效率。但是，以門禁管制的生物辨識科技來看，其主要的重點在於「目的使用的限制」，也就是生物辨識科技的使用目的必須合理並且合法，而不得超出其目的之使用[82]，故以功能相當的 RFID 識別應用來看，其使用目的與生物辨識科技相當，故亦應遵守其主要管制核心內容，始能達到科技應用與隱私保護的平衡點。

82　同前註，頁 96-99。

5.2.5 儲值卡

儲值卡的 RFID 應用可以分爲與識別資料連結和不與識別資料連結兩種。與識別資料連結的 RFID 應用與會員卡應用相當，只是其增加了金額的資料，故其管制的密度與模型，應與會員卡的管制相當；而不與識別資料連結的儲值卡 RFID 應用，因其不涉及資料主體辨識的問題，故對隱私權的侵害相對降低許多，因而其針對隱私權的管制保護，應採取開放的型態爲佳。

5.3 RFID 系統運用所產生的隱私權侵害態樣

5.3.1 位置資訊

RFID 系統的無線感應能力加上感應器的設置，將在無形之中記錄個人的位置訊息，在某種程度上對個人產生了社會側寫，影響個人社會生活的活動，也成爲 RFID 系統在使用上最普遍的隱私權問題，尤其在個人缺乏告知訊息的情形下，此種情況將更爲嚴重。因此，在使用 RFID 系統時，業者或是資料蒐集者應採取更周詳的訊息告知，讓消費者能在資訊充分的情況下選擇加入或是避免此類資訊的大量蒐集爲妥。

5.3.2 醫療資訊

當 RFID 系統的運用與醫療進行結合時，就成爲醫療資訊鏈的一環，因此亦應受到更高程度的管制。一般來說，醫療資訊被視爲敏感性資訊，其對於個人社會生活的影響至深至遠，並非一般識別性資訊所能比擬，故其本非適用一般的資訊安全檢驗標準。而一旦 RFID 系統加入資訊鏈的一環，其使用上的優勢成爲隱私權的隱憂，對於醫療資訊的保護將產生衝擊，使用者勢必應採取更詳盡的保護管制，除了應適用嚴格的隱私權保護機制外，尚應加入機密性的要求爲宜。

5.3.3 公領域識別資訊

公領域識別資訊最常見者爲政府機構所訂之全國性編碼，一般來說就是

身分證號碼與護照號碼等，利用此種編號即可接近使用政府各機構的資料庫，就個人的識別資料而言有舉足輕重的地位，但是學說上對於公領域識別編碼是否爲受保護的隱私資訊尚有爭議，但是其對個人隱私權之影響卻是不可否認的，因此公部門欲使用 RFID 系統來增進行政效率時，應審慎爲之。

5.3.4　消費紀錄資訊

一般來說，商業進行最主要的目的是爲了能夠增加行銷成功率，因此個人消費資訊的蒐集就顯得相當重要，使用 RFID 系統將使得此類資訊的蒐集更爲精確，有助於商業運作，但是個人消費紀錄的蒐集透過分析使用後，將對個人產生一種側寫，有妨礙個人健全發展的可能，同時加上 RFID 系統識別商品的龐大資訊網，對個人隱私權有一定的衝擊，並不得任意爲之，故業者在使用 RFID 系統來識別個人時，仍應在商業運作與個人隱私權保護中取得平衡點爲宜。

5.4　小結

針對不同的 RFID 個人識別應用，應該有不同程度的管制，畢竟不同的使用對於個人隱私權的侵害程度與範圍不相當，不可一體適用同一標準，此已如前所述，針對各種不同的應用，應有不同的管制程度，茲就前述討論整理如下：

不管制	公平資訊使用原則	契約限制之隱私權保護機制（通行管制、工作場合）	EPCglobal 隱私指導方針	平衡之 RFID 隱私權保護機制（會員卡、商品識別、儲值卡、信用卡）	嚴格的 RFID 隱私權保護機制（醫療識別／敏感性資訊）	完全禁止
	1.蒐集限制 2.資料品質 3.目的明確 4.使用限制 5.安全防護 6.資料庫公開 7.個人參與 8.責任歸屬 （即 FIPs：Fair information practuce）	1.FIPs 原則 2. 充分告知機制	1.紀錄之使用、保存與安全性蒐集限制。（FIPs 原則） 2.消費者標示 3.消費者選擇 4.消費者教育	1.FIPs 原則 2.充分告知機制 3.消費者選擇 4.選擇加入機制	1.FIPs 原則 2.資料最小化 3.選擇加入 4.反差別待遇 5.機密性	

6. 我國電腦處理個人資料保護法與 RFID 管制模式之分析

6.1 RFID 應用適用我國電腦處理個人資料法之情形

有關個人隱私權的保護，在我國法律架構之下可分見於許多不同類型的法律之下，刑法的妨害秘密罪、民法的侵權行爲與醫事法的醫師保密義務，都對於隱私權的侵害提供了保護，但是對個人資訊隱私權最直接相關的法律爲「電腦處理個人資料保護法」（以下簡稱「個資法」），該法於 1995 年 8 月 11 日公布，對於個人識別資料做了專門的規範，因此一般在討論個人資訊隱私權時，即以本法作爲主要的討論依據；本文因探討 RFID 應用對於個人資訊隱私權的影響，故主要以個資法爲討論的重心，茲分述如後。

6.1.1　商品識別 RFID 之使用管制

6.1.1.1　透過 RFID 所得之資料類別與適用主體

單純將 RFID 使用於識別商品以供存貨清點，其本身不涉及個人識別時，原則上非屬個資法規制的範圍內，惟當其與個人識別資料結合後（最通常的情形就是與會員折扣制度結合後，藉以記錄購買者消費習慣），即應視爲可識別個人之社會活動紀錄[83]，故其使用應遵守個資法相關規定；而 RFID 進行商品識別者爲經濟行爲之實體，個資法將資訊使用主體分爲公務機關與非公務機關，公務機關指的是依法行使公權力之中央或地方機關[84]，而非公務機關指的是公務機關以外，法律所規定或是經由相關主管單位指定之事業、團體或個人者而言[85]，由於進行商品附加 RFID 晶片的單位多非依法行使公權力之中央或地方機關，因此可以推論主要商品識別的使用管制主體應爲非公務機關，從而適用非公務機關之相關規定。

6.1.1.2　個資法與 RFID 相關之規定概述

個資法在第 18 條規定非公務機關蒐集個人資料必須先向相關主管機關取得執照，始得進行個人資料的蒐集與運用，而同時第 19 條之規定，非公務機關蒐集個人資料必須擇一符合以下之條件：

1.經當事人書面同意者。

2.與當事人有契約或是類似契約之關係而對當事人權益無侵害之虞者。

3.已獲公開且無害於當事人之重大利益者。

83　電腦處理個人資料保護法第 3 條第 1 款：「個人資料：指自然人之姓名、出生年月日、身分證統一編號、特徵、指紋、婚姻、家庭、教育、職業、健康、病歷、財務情況、社會活動及其他足資識別該個人之資料。」

84　電腦處理個人資料保護法第 3 條第 6 款：「公務機關：指依法行使公權力之中央或地方機關。」

85　電腦處理個人資料保護法第 3 條第 7 款：「(一)徵信業及以蒐集或電腦處理個人資料為主要業務之團體或個人。(二)醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業。(三)其他經法務部會同中央目的事業主管機關指定之事業、團體或個人。」

4.為學術研究而有必要且無害於當事人之重大利益者。

5.其他相關法規所授權者。

故若不符合其條件限制或是違反申請登記事項之記載未更正，而擅自以 RFID 進行資料蒐集，則將遭致主管單位進行罰緩。

在蒐集資訊主體的識別資料後，其使用必須合於蒐集之目的，個資法第 23 條規定：「非公務機關對個人資料之利用，應於蒐集之特定目的必要範圍之內為之。」因此除非有但書之情形，餘皆不得違背蒐集目的之使用。

6.1.2 個人識別 RFID 之使用管制

我國將個人資料蒐集利用的主體以公務機關與非公務機關作為區分，並以此進行不同之管制，茲就個人識別 RFID 所面臨的管制概述如後：

6.1.2.1 公務機關

從個資法的規定來看，公務機關進行個人識別資料的蒐集使用，必須有特定目的，也就是符合目的明確原則的適用，並且同時必須是經當事人同意，或是法律規定，或是對當事人權利沒有侵害之虞者始得為之[86]；但是其同時在第 8 條規定目的外使用的條件，作為使用限制的例外[87]。另外，如果公務機關要進行個人識別資料的蒐集或使用時，必須進行公告[88]，以免有秘

---

86 電腦處理個人資料保護法第 7 條：「公務機關對個人資料之蒐集或電腦處理，非有特定目的，並符合左列情形之一者，不得為之：一、於法令規定職掌必要範圍內者。二、經當事人書面同意者。三、對當事人權益無侵害之虞者。」

87 電腦處理個人資料保護法第 8 條：「公務機關對個人資料之利用，應於法令職掌必要範圍內為之，並與蒐集之特定目的相符。但有左列情形之一者，得為特定目的外之利用：一、法令明文規定者。二、有正當理由而僅供內部使用者。三、為維護國家安全者。四、為增進公共利益者。五、為免除當事人之生命、身體、自由或財產上之急迫危險者。六、為防止他人權益之重大危害而有必要者。七、為學術研究而有必要且無害於當事人之重大利益者。八、有利於當事人權益者。九、當事人書面同意者。」

88 電腦處理個人資料保護法第 10 條：「公務機關保有個人資料檔案者，應在政府公報或以其他適當方式公告左列事項；其有變更者，亦同：一、個人資料檔案名稱。

密資料庫的存在，以符合資料庫公開原則。而同時爲了維護個人資料的正確以及讓資料主體參與個人資料維護，個資法在第 12、13 條規定了個人參與以及資料品質維護的相關規定[89]，以期保護資料主體之權利。

6.1.2.2　非公務機關

附加 RFID 會員卡之使用，與公部門發給公民所使用的身分證明皆爲識別個人的文件，但會員卡之使用僅用於商業行爲運作之相關資訊蒐集，其在個資法上的適用於商品識別資訊與個人識別資訊進行連結時，應遵守相同的規定。

6.2　個資法暨修正草案從 RFID 應用觀點之評析

目前個資法的蒐集限制雖然已有概括性的規定，但是在適用於 RFID 的應用時，卻不免引起若干疑義；首先，非公務機關需取得執照始能就個人資料進行蒐集的制度，並且必須填具申請書，一旦蒐集手段有所變更，又必須進行申報更改或是重新申請，不僅花費大量行政成本，且以目前主管機關所

二、保有機關名稱。三、個人資料檔案利用機關名稱。四、個人資料檔案保有之依據及特定目的。五、個人資料之類別。六、個人資料之範圍。七、個人資料之蒐集方法。八、個人資料通常傳遞之處所及收受者。九、國際傳遞個人資料之直接收受者。一〇、受理查詢、更正或閱覽等申請之機關名稱及地址。前項第五款之個人資料之類別，由法務部會同中央目的事業主管機關定之。」

89 電腦處理個人資料保護法第 12 條：「公務機關應依當事人之請求，就其保有之個人資料檔案，答覆查詢、提供閱覽或製給複製本。但有左列情形之一者，不在此限：一、依前條不予公告者。二、有妨害公務執行之虞者。三、有妨害第三人之重大利益之虞者。」電腦處理個人資料保護法第 13 條：「公務機關應維護個人資料之正確，並應依職權或當事人之請求適時更正或補充之。個人資料正確性有爭議者，公務機關應依職權或當事人之請求停止電腦處理及利用。但因執行職務所必需並註明其爭議或經當事人書面同意者，不在此限。個人資料電腦處理之特定目的消失或期限屆滿時，公務機關應依職權或當事人之請求，刪除或停止電腦處理及利用該資料。但因執行職務所必需或經依本法規定變更目的或經當事人書面同意者，不在此限。」

核准之行業幾乎已包含所有業者，故於非公務機關再行分類可蒐集個人資料之業者，尚難窺其實益。再者，以學術爲目的之資料蒐集，並未配合要求匿名或是去名化（de-identification）制度，縱使特別規定須無害於當事人之重大利益，惟學術研究之範圍過廣，爲恐業者以該條件逕行蒐集利用，而涉及敏感資訊之外洩或是風險提高，應配合匿名制度之使用爲妥。

由於現行個資法面對龐大的資訊難以因應種種挑戰，法務部草擬本法的修正草案，針對諸多規定加以修正，其中將非公務機關需申請核准使得蒐集個人資料的條件刪除，將非公務機關定義爲公務機關以外者[90]，同時草案並明文規定業者應告知資料主體之事項[91]，如有違反將處以罰鍰[92]，並且增加了學術研究匿名統計的機制[93]，也因此相較於現行個資法，其對於隱私權的保障較爲適切。

其次，從身分識別 RFID 適用個資法中有關公務機關之規定而言，現行的個資法並未就個人資料的本質進行區分，也就是敏感性資料的保護與一般識別資料適用相同規定，對於例如醫療相關資訊等敏感性資料的保護顯有不足；再者，現行公務機關與非公務機關之區分，對於行政法人之歸屬產生了難以區分的情形，無法清楚適用易生疑義。同時，其對於學術研究匿名化規定的闕漏，亦使個人資訊隱私權產生威脅。最後，縱使個資法中要求公務機關主動告知資料蒐集的相關事項，以符合資料庫公開原則之適用，但由於缺少對民眾的告知，大眾對於其資料的處理將難以瞭解，並且在缺少相關認知的情形下同意公務機關進行資料蒐集，對於隱私期待的建立也將有所落差。

以個資法修正草案之規定以觀，針對現行法所產生的疑慮，修正草案首

90 「個人資料保護法」修正草案第 2 條第 8 款：「指前款以外之自然人、法人或其他團體。」法務部網站：http://www.moj.gov.tw/public/Attachment/62228524321.pdf （最後點閱日期：2006 年 8 月 27 日）。

91 同前註，第 8 條第 1 項。

92 同前註，第 47 條第 1 款。

93 同前註，第 19 條第 4 款。

先在第 6 條就敏感性資訊，如醫療、基因、性生活、健康檢查及犯罪前科等個人資料明文禁止蒐集，除非符合但書之規定，否則即屬違法之個人資料蒐集[94]。再者，有關公務機關是否包含行政法人之部分，修正草案第 2 條第 7 項規定：「公務機關：指依法行使公權力之中央或地方機關或行政法人。」因此解決了行政法人之爭議。而本次修正草案將學術使用資料匿名化原則引進，也適度解決了原先的隱私權疑慮，最後，修正草案在第 8 條增訂公務機關與非公務機關的告知義務[95]，提供資料主體更多關於其個人資料處理的相關資訊，以便建立資料主體之隱私權期待。

最後，有關私部門利用 RFID 應用來識別個人時，雖然其並非全國性統一編碼，對於個人識別的連結性與可靠性較低，保護尚不需若公部門所發放之識別證件嚴密，但在使用 RFID 會員卡時，我國並未就其編碼型態進行規定，但是如果業者以公部門識別號碼作爲會員卡編碼，透過 RFID 晶片進行發送，則將使得會員卡成爲個人隱私權保護最大的漏洞。再者，會員編碼並非可直接識別個人之資料，因此是否成爲個資法所規定之個人資料，尚有疑

---

94 「個人資料保護法」修正草案第 6 條：「有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：一、法律明文規定。二、法律未明文禁止蒐集、處理或利用，且經當事人書面同意者。三、公務機關執行法定職務或非公務機關履行法定義務所必要。四、當事人自行公開或其他已合法公開之個人資料。五、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究為必要，請資料經過處理後或依其揭露方式無從識別特定當事人。」法務部網站：http://www.moj.gov.tw/public/Attachment/62228524321.pdf （最後點閱日期：2006 年 8 月 27 日）。

95 「個人資料保護法」修正草案第 8 條第 1 項：「公務機關或非公務機關依第十五條或第十九條規定向當事蒐集個人資料時，應明確告知當事人下列事項：一、公務機關或非公務機關名稱。二、蒐集之目的。三、個人資料之類別。四、個人資料利用之期間、地區、對象及方式。五、當事人依第三條規定得行使之權利及方式。六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。」法務部網站：http://www.moj.gov.tw/public/Attachment/62228524321.pdf（最後點閱日期：2006 年 8 月 27 日）。

義，惟個資法修正草案將「直接、間接」識別個人之資訊，皆納入個人資料的保護之內，應可消弭爭議。

6.3 本文建議

6.3.1 商品識別 RFID 之使用管制

對於商品識別 RFID 之管制，雖透過修正草案的增補，對隱私的保障更爲完善，但是其仍屬一般性的規定，關於 RFID 應用所引發的特有爭議，仍有保護不足之處，本文在此提出幾點建議，可供未來擬定 RFID 應用之管制規範參考：

6.3.1.1 消費者選擇

由於 RFID 較佳的傳輸能力，使得消費者相關的隱私資訊將受到威脅，因此應該在消費者消費行爲結束時，由業者主動銷毀晶片之傳輸能力，也就是當晶片編碼失去其原有目的後，即取消其能力，不再四處跟隨消費者，並且傳送其他資訊給感應器，讓消費者能選擇其提供資訊的終點。

6.3.1.2 充分資訊告知

由於 RFID 晶片體積微小，一般人難以察覺，因此在購物環境之中，即應該以明顯的標示告知消費者商品內含 RFID 晶片，而在商品上亦須標示其 RFID 晶片存放之處，當 RFID 晶片銷毀時也應告知消費者，甚而提供檢視 RFID 晶片是否已被消除傳送能力的設備，讓消費者在消費行爲開始到結束，都能完整獲知有關 RFID 晶片的存在與銷毀，不但可保障消費者的資訊隱私，亦可免除大眾對 RFID 晶片的不必要恐懼。

6.3.3.3 自律的運作

從之前的討論來看，資訊隱私權的保護因爲相關環境因素，並無法以自律的方式來達到目的，因而必須透過法律的管制；而 RFID 的適用，由於透過其所蒐集資料得以透過一般性的法律來保護，但是基於 RFID 特性所衍生的保護機制，例如：消費者選擇，應由自律來達成抑或是透過政府的力量？從 RFID 在商品的使用來看，其係全球性的編碼系統，因此跨國商品的來往

透過全球性的組織以自律的方式維持，跨越各國法律的屏障，似能達到較佳的管制效果，故在管制 RFID 附加於商品的部分，應以自律作爲先行的管制方式，日後若自律未能達到其所欲達之目的，再以法律介入管制爲妥。

6.3.2 個人識別 RFID 之使用管制

6.3.2.1 特定使用之 RFID 訊號傳送加密

個人識別號碼存於 RFID 晶片之中，將因其發送能力而使個人識別號碼洩漏於無形之中，因此對於涉及敏感性資訊或是具有廣泛證明個人身分功能之編碼，利用加密技術來保障其能安全傳輸，以防有心人士之擷取，始能將隱私權侵害的風險降到最低。

6.3.2.2 充分資訊告知

關於使用 RFID 晶片的任何訊息皆應告知資料主體，不論是晶片存在的位置，或是感應器的位置都應有明顯的標示，以讓資料主體能夠擁有相關的認知，並且建立資料主體的隱私權期待。

6.3.2.3 監督機制的建立

不論是公部門或是私部門對於 RFID 晶片身分識別卡的應用，都應該受到獨立監督機制來管理，以負責申訴等問題的處理，並且強化資料庫接近資格的限定，讓資料主體資訊的保護更爲完善。

6.3.2.4 醫療植入使用最小化原則

醫療植入涉及身體侵入性的問題，主要使用目的在於醫療錯誤的減少，對於失去意識或是阿茲海默症等患者，具有快速識別的功能。惟當患者意識清楚或是尚能辨識身分時，適用植入性醫療 RFID 晶片的必要性將受到質疑，故應將醫療植入 RFID 晶片的適用降到最低，除了當事人同意外，尚須符合必要性的條件，將醫療植入使用最小化。

6.3.2.5 私部門的編碼應與公部門身分識別碼區別

因爲私部門所蒐集之資訊多屬商業運作的資訊，其編碼不具有證明個人身分之功能，原不需受到特殊加密技術的保護，但是一旦業者將消費者之公

部門編碼直接作爲會員編碼，透過 RFID 晶片進行傳輸，則等於其將個人的身分編碼昭告世人，因此在 RFID 晶片使用的情況之下，私部門的個人編碼應避免使用公部門之身分識別編碼，以資區別，方可提供個人隱私更充分的保障。

7. 結語

多角度且低干擾的無線感應功能，讓 RFID 擁有強大的經濟效益，但是相對也讓使用者的隱私權產生威脅。本文從 RFID 對我們生活的改變來探討其對隱私保護所產生的衝擊，首先，RFID 應用確實對我們的隱私權產生了某種程度的威脅，透過其資料蒐集的特性產生了程度不一的衝擊。針對 RFID 在應用上的特性所進行之管理，本文認爲應先以業者自律的方式進行；再者，本文提出平衡的 RFID 使用管制模型，希冀能在科技應用與隱私保護間得到最適的管制；最後，針對我國隱私法制的適用不足部分，提出相關建議，以期建立良好的使用規則。

RFID 的應用，在隱私權的領域代表了一個重要的意義——科技的發展將越來越模糊公與私的界線。而隨著 RFID 應用的擴大，個人所能掌控的隱私範圍將越來越小。試想若我們不願在購買商品時暴露個人的識別資訊，我們可以選擇利用現金進行支付；但是如果政府決定利用 RFID 標籤植入現鈔的方式來防止僞造，則個人在購買商品保持匿名性的期待，將會隨著現金流的易於追蹤而逐漸落空。人們在享受科技所帶來的便利時，是不是一定要以其隱私權作爲交換？這些問題不斷出現在科技發展與隱私保護的爭論之中。當全球定位系統（GPS）的應用使我們旅途的導向更爲精確，但同時個人所在的位置卻也陷入更易於讓他人追蹤的境地。科技發展與隱私保護的論戰將持續下去，但科技法制研究者的使命，就是在一次又一次的挑戰中盡力尋找出最適的平衡。

參考文獻

中文書籍

NTT Data Ubiquitous 研究會，《RFID 是啥？：實現「無遠弗屆社會」的 RFID 技術》，荒川弘熙編，葉珠娟、江佳純譯，向上出版，台北（2005）。

《RFID 技術與應用》，日經 BP RFID 編輯部編，周湘琪譯，旗標出版，台北（2005）。

刁建成，《RFID 原理與應用》，全華出版，台北（2005）。

中文期刊

王郁琦，〈生物辨識技術對隱私權的影響〉，《科技法學評論》，第 3 卷第 2 期，頁 49-106，2006 年 10 月。

林宏達，〈你看廣告　我付錢〉，《商業周刊》，第 958 期，頁 54-56，2006 年 4 月 3 日。亦可見商業周刊網站：http://www.businessweekly.com.tw/article.php?id=22314。

中文論文集

王郁琦，〈工作場合中電子郵件隱私權之研究〉，《資訊、電信與法律》，頁 71-106，元照出版，台北（2004）。

王郁琦，〈生物辨識技術對隱私權的影響〉，《2005 全國科技法律研討會論文集》，頁 287-317，交通大學科技法律研究所出版，新竹（2005）。

其他中文參考文獻

〈EPC 編碼〉，EPCGlobal Taiwan 網站：http://www.epcglobal.org.tw/epcg/jsp/a21.htm#（最後點閱時間：2006 年 8 月 3 日）。

〈EPCGlobal 組織〉，EPCGlobal Taiwan 網站：http://www.epcglobal.org.tw/epcg/jsp/a121.htm#01（最後點閱時間：2006 年 8 月 3 日）。

王鍾渝，〈健保 IC 卡書面質詢〉，立法院全球資訊網：http://www.ly.gov.tw/ly/01_introduce/0103_leg/leg_main/leg_news/leg_news_02.jsp?ItemNO=01030700&tableid=1215&tablename=cw_ly1500&stage=5&lgno=00008（最後點閱時間：2007 年 7 月 14 日）。

〈企業指南〉，EPCGlobal Taiwan 網站：http://www.epcglobal.org.tw/epcg/jsp/a41.htm（最後點閱時間：2006 年 8 月 3 日）。

英文書籍

CENTER FOR DEVICES & RADIOLOGICAL HEALTH, U.S. DEP'T OF HEALTH & HUMAN SERVICES, CLASS II SPECIAL CONTROLS GUIDANCE DOCUMENT: IMPLANTABLE RADIOFREQUENCY TRANSPONDER SYSTEM FOR PATIENT IDENTIFICATION AND HEALTH INFORMATION (2004), *available at* http://www.fda.gov/cdrh/ode/guidance/1541.pdf (last visited Sept. 23, 2006).

FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS (1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf (last visited Sept. 24, 2006).

GARDNER, CHRIS, AUTOMOTIVE AFTERMARKET RFID: MEMA INFORMATION SERVICES COUNCIL WHITE PAPER 2004 (2004), *available at* http://www.miscouncil.org/Automotive%20Aftermarket%20RFID.pdf.

英文期刊

Albrecht, Katherine, *Supermarket Cards: The Tip of the Retail Surveillance Iceberg*, 79 DENV. U. L. REV. 534 (2002).

Eden, John M., *When Big Brother Privatizes: Commercial Surveillance, the Privacy Act of 1974, and the Future of RFID*, 2005 DUKE L. & TECH. REV. 20, *available at* http://www.law.duke.edu/journals/dltr/articles/PDF/2005DLTR0020.pdf.

Hildner, Laura, *Defusing the Threat of RFID: Protecting Consumer Privacy Through Technology-Specific Legislation at the State Level*, 41 HARV. C.R.-C.L. L. REV. 133 (2006).

Karim, Waseem, *The Privacy Implications of Personal Locators: Why You Should Think Twice Before Voluntarily Availing Yourself to GPS Monitoring*, 14 WASH. U. J.L. & POL'Y 485 (2004).

Lessig, Lawrence, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869 (1996).

Levary, Reuven R., Thompson, David, Kot, Kristen & Brothers, Julie, *Radio Frequency Identification: Legal Aspects*, 12 RICH. J.L. & TECH. 6 (2005), *available at* http://law.Richmond.edu/jolt/v12i2/article6.pdf.

Marx, Gary T., *Seeing Hazily (But Not Darkly) Through the Lens: Some Recent Empirical Studies of Surveillance Technologies*, 30 LAW & SOC. INQUIRY 339 (2005).

Nehf, James P., *Incomparability and the Passive Virtues of Ad Hoc Privacy Policy*, 76 U. COLO. L. REV. 1 (2005).

Terrell, Timothy P. & Jacobs, Anne R., *Privacy, Technology, and Terrorism: Bartnicki, Kyllo, and the Normative Struggle Behind Competing Claims to Solitude and Security*, 51 EMORY L.J. 1469 (2002).

Valetk, Harry A., *Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies*, 2004 STAN. TECH. L. REV. 2, *available at* http://stlr.stanford.edu/STLR/Articles/04_STLR_2/fsarticle.htm.

其他英文參考文獻

Bacheldor, Beth, *GAO Issues Drug Report, Senator Sponsors Bill*, RFID J., May 10, 2006, http://www.rfidjournal.com/article/articleprint/2327/-1/1/.

Brito, Jerry, Relex, Don't Do It: Why RFID Concerns Are Exaggerated and Legislation Is Premature, http://www.lawtechjournal.com/articles/2004/05_041220_brito.pdf (last visited Sept. 22, 2006).

Classification of Implantable Radiofrequency Transponder System for Patient Identification and Health Information, 69 Fed. Reg. 71,702 (Dec. 10, 2004) (to be codified at 21 C.F.R. pt.880), *available at* http://www.fda.gov/ohrms/dockets/98fr/ch0466.pdf (last visited Sept. 23, 2006).

Collins, Jonathan, *Swiss Moviegoers Use RFID to Buy Tickets*, RFID J., Mar. 30, 2005, http://www.rfidjournal.com/article/articleview/2230/1/1/.

Collins, Jonathan, *Japan Issues E-Passports*, RFID J., Mar. 28, 2006, http://www.rfidjournal.com/article/articleview/2224/1/1/.

Collins, Jonathan, *Tesco Revises RFID Plans*, RFID J., Apr. 7, 2006, http://www.rfidjournal.com/article/articleview/2243/1/1/.

Consumers Against Supermarket Privacy Invasion and Numbering et al., RFID Position Statement of Consumer Privacy and Civil Liberties Organizations, *available at* http://www.privacyrights.org/ar/RFIDposition.htm (last visited Sept. 22, 2006).

Driscoll, Margarett, *This Girl's Parents Want to Keep Track of Her by Microchip: Paranoia or Wise Precaution?*, SUNDAY TIMES, Sept. 8, 2002, at 24.

EPCglobal Guidelines on EPC for Consumer Products, *available at* http://www.epcglobalinc.org/public/ppsc_guide/ (last visited Sept. 17, 2007).

Hill, Bert, *Verichip Looks for $45.8M U.S. in IPO*, OTTAWA CITIZEN, Dec. 31, 2005, at H1.

Johnston, Philip, *ID Cards Will Track Where People Go*, THE DAILY TELEGRAPH, Jan. 28, 2006, at 4, *available at* http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2006/01/28/nid28.xml&sSheet=/news/2006/01/28/ixhome.html.

O'Connor, Mary Catherine, *SecureRF Creates New Encryption Method*, RFID J., Nov. 9, 2005, http://www.rfidjournal.com/article/articleview/1973/2/1/.

O'Connor, Mary Catherine, *RFID Keeps Objects, Kids from Going Astray*, RFID J., Mar. 20, 2006, http://www.rfidjournal.com/article/articleview/2209/1/1/.

O'Connor, Mary Catherine, *DHS Completes E-Passport Test at SFO*, RFID J., Apr. 18, 2006, http://www.rfidjournal.com/article/articleview/2274/1/1/.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, *available at* http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (last visited Aug. 27, 2006).

Palmer, Maija, *Theme Park Tags on to ID Chip Expansion*, FINANCIAL TIMES, Apr. 15, 2006, at 3, *available at* http://www.ft.com/cms/s/0/ff6d7f30-cc1c-11da-a7bf-0000779e2340.html.

Sullivan, Laurie, *RFID Passport Tests to Begin at San Francisco Airport*, TECHWEB NEWS, Dec. 30, 2005, http://www.informationweek.com/story/showArticle.jhtml?articleID=175800183.

VeriChip Corporation, http://www.verichipcorp.com/company.html (last visited Aug. 27. 2006).

VeriChip: Privacy Policy, http://www.verichipcorp.com/content/company/privacy (last visited Aug. 27, 2006).