科技法學評論，3 卷，頁 49（2006）

科法新論

生物辨識技術之運用對隱私權的影響*

王郁琦**

摘　要

在美國發生 911 事件之後，世界各國紛紛尋求科技的幫助，希望能夠加強安全管制，避免悲劇再次發生。由於生物辨識技術是透過電腦，以人類的生物特徵辨識個人的身分，因此，如果能夠成功運用於機場或其他公共場所的進出管制，對於減少身分偽造或冒用，避免再一次的恐怖攻擊將會有莫大的助益。對於私人住家與企業而言，生物辨識技術用於門禁管制亦可加強安全維護。但是，由於生物辨識技術的運用，涉及了對個人指紋、虹膜或其他相關資訊的蒐集，因此必須對個人資訊隱私有完善的保護，以防資訊外洩或遭到濫用。此外，由於生物特徵無法更改，將可能用來連結各個資料庫，使得個人的一切作爲都在政府的監督之下。本文除了希望透過對生物辨識技術以及隱私權概念深入的研究，以釐清生物辨識技術是否會對個人隱私造成侵害。在生物辨識科技不可避免的將被廣泛運用的情況下，應該如何妥善使用生物辨識技術，一方面可以避免個人身分在任何情況下被冒用或偽造，同時也應該透過良好的監督機制，儘量避免可能的隱私權侵害。

關鍵字：生物辨識、資訊隱私權、身分盜用

---

* 本文為國科會委託計畫「生物辨識技術對隱私權影響之研究」之研究成果，研究助理為世新大學法研所碩士吳佩諭小姐。吳小姐於執行研究計畫過程中認真負責，作者特此致謝。另外，審稿委員對本文提出多處指正，作者亦衷心感謝。

** 世新大學法律學系副教授，資策會科法中心主任；美國印第安那大學法學博士（S.J.D.）。

投稿日：2006 年 7 月 15 日；採用日：2006 年 8 月 28 日

Cite as: 3 Tech. L. Rev. 49 (2006)

The Impact on Privacy from the Application of Biometrics

Yu-Chi Wang

Abstract

After the 911 attack on the U.S., governments all over the world look for help of technology to enforce the airport surveillance and to avoid terrorist attacks. Biometrics compares the physiological or behavioral characteristics by computers to identify a person. The use of biometrics in the control of public places and airports can reduce the problem of identity theft. In private houses and companies, the application of biometrics can accrue safety. Because the application of biometrics requires the collections of fingerprints, irises or other personal information alike, it's important to protect personal information from disclosure or abuse. In addition, the biometrics information can be used as an identifier because it is difficult to change, the government may therefore use it to surveillance people's behavior through cross-linking all databases the government owns. In addition to researching on the development of the biometrics technology and its impact on privacy, this article argues that the use of biometrics is inevitable and the government should assess the impact on privacy and set up the mechanism of supervision to avoid possible abuses.

Keywords: biometrics, information privacy, identity theft

1. 生物辨識之介紹

生物辨識技術是指利用每個人特有的生物或行爲特徵以辨識或確認其身分之方式[1]。生物辨識技術最早起源於 19 世紀之法國，當時法國巴黎的一位人類學者 Alphonse Bertillion 測量罪犯之頭圍、中指長度等資料，並加以建檔，以辨識罪犯[2]。現代生物辨識技術之發達始於 1990 年代初期，美國國防部投入大筆資金研究使用演算法辨識人類臉孔的可能性[3]，而今日，生物辨識技術的應用早已充斥在我們的日常生活中。尤其在美國 911 事件發生後，生物辨識技術更成爲世界各國政府積極發展的身分辨識方式，期望可以透過生物辨識技術在恐怖份子試圖進入國界之際，便成功的加以辨識、逮捕。

生物辨識技術發展至今，幾乎人類所有特徵均可以透過演算法，將該特徵轉變爲模組（template），用以作爲身分辨識之方式。生物辨識技術大致上可以分成生理特徵以及行爲特徵兩大類，生理特徵包括基因、手掌、眼睛、臉部、指紋、耳朵、氣味等，行爲特徵則包含簽名、聲紋、敲擊鍵盤節奏、步伐等，均可用以作爲辨識身分之個人特徵[4]，常見的生物辨識技術主要爲下列幾種：

1.1 簽名

簽名辨識在過去大多以肉眼辨識兩個簽名之間是否相符，以作爲確認

---

1 ERIK BOWMAN, EVERYTHING YOU NEED TO KNOW ABOUT BIOMETRICS 1, http://www.ibia.org/EverythingAboutBiometrics.PDF (last visited on Sept. 8, 2005).

2 Alexander T. Nguyen, *Here's Looking at You, Kid: Has Face-Recognition Technology Completely Outflanked the Fourth Amendment?*, 7 VA. J.L. & TECH. 2 (2002).

3 Julia Scheeres, *Smile, You're on Scan Camera*, http://www.wired.com/news/print/0,1294,42317,00.html (last visited on Sept. 8, 2005).

4 BOWMAN, *supra* note 1, at 2-3.

本人身分的方式。但是生物辨識技術對於簽名之辨識方式並不是以外觀上是否相似作爲辨識之方式，而是透過電腦，比對簽名的筆順（stroke order）、速度（speed）以及書寫壓力（pressure），藉以分辨兩者是否爲同一人所書寫之簽名[5]。雖然將簽名電子化之後，將會使得個人簽名之複製更爲容易，但是由於每個人隨著每次書寫狀態的不同，簽名亦或多或少會有差距，因此一般認爲並沒有完全相同的簽名，故而百分之百相同的簽名，反而可能會被認爲是經由複製之簽名，而非本人實際簽名[6]。

1.2 指紋

指紋辨識作爲犯罪偵察之方式由來已久，但生物辨識技術擺脫傳統以油墨複印當事人指紋的方式，而改以光學、矽晶或者超音波的方式對指紋進行掃瞄，其中光學技術爲目前最常用的掃瞄方式，而超音波技術則是三種當中最準確的掃瞄方式[7]。

指紋辨識的精確度高，即使是雙胞胎，擁有相同指紋的機率也低於一兆分之一[8]，加上指紋辨識使用之掃描器體積小，容易與其他設備整合且價格低廉[9]，使得指紋辨識成爲最廣爲使用的生物辨識方式之一，就使用者的角度而言，指紋辨識更是既方便、簡易又值得信任的一種生物辨識方式[10]。

---

5 INTERNATIONAL BIOMETRICS GROUP, SIGNATURE VERIFICATION: HOW IT WORKS, http://www.biometricgroup.com/reports/public/reports/signature-scan_tech.html (last visited on Sept. 8, 2005).

6 Robyn Moo-Young, *"Eyeing" the Future: Surviving the Criticisms of Biometric Authentication*, 5 N.C. BANKING INST. 421, 436 (2001).

7 INTERNATIONAL BIOMETRICS GROUP, OPTICAL—SILICON—ULTRASOUND, http://www.biometricgroup.com/reports/public/reports/finger-scan_optsilult.html (last visited on Sept. 8, 2005).

8 BOWMAN, *supra* note 1, at 4.

9 findBIOMETRICS.com, *About Fingerprint Scanning*, http://www.findbiometrics.com/Pages/fingerprint_articles/fingerprint_1.html (last visited on Sept. 8, 2005).

10 findBIOMETRICS.com, *Fingerprint Authentication—The Time Has Finally Arrived*,

雖然指紋辨識可能受到手指長繭、受傷、髒污或者環境的過度乾燥或潮濕之影響而辨識失敗[11]，實務上，年長者、從事手工業者來說，在登入指紋辨識系統上可能會有困難[12]，即便透過外科手術以酸性溶液腐蝕指紋，但手指復原之後，新長出的指紋仍舊會和過去相同[13]。另外，在進行指紋辨識的同時，亦可以進行皮膚溫度、血液含氧量、血壓以及皮膚導電率之偵測，以防止有心人士以斷指的方式試圖欺騙指紋辨識儀器[14]。

1.3　臉型

臉型辨識雖然同樣都是以攝影機捕捉個人的臉部影像之後，再加以比對以辨識身分，但是其辨識方式卻有所不同。有些臉部辨識系統以嘴巴、鼻子、眼窩、顴骨等特徵彼此之間的距離進行辨識，亦有些臉部辨識系統以臉部特徵的分布之分析作爲辨識的方式[15]。

臉部辨識系統可以結合閉路電視監視系統，用以監督各種場所進出的每一個人，因此，隨著閉路電視監視系統的廣泛運用，臉部辨識系統的使用也越來越普遍。就使用者的觀點而言，由於臉部辨識系統在辨識過程中，僅需要求受辨識者以正面面對攝影機，甚至可能在受辨識者未察覺之下進行辨

---

http://www.findbiometrics.com/Pages/fingerprint_articles/fingerprint_2.html (last visited on Sept. 8, 2005).

11 findBIOMETRICS.com, *supra* note 9.

12 INTERNATIONAL BIOMETRICS GROUP, FINGERPRINT GROWTH INHIBITORS, http://www.biometricgroup.com/reports/public/reports/growth_inhibitors.html (last visited on Sept. 8, 2005).

13 DAN FINGERMAN, STATIC MEASUREMENTS AND MOVING TARGETS: PRIVACY, BIOMETRICS AND THE CONSUMER-BANK RELATIONSHIP 8, http://www.danfingerman.com/papers/Biometrics_paper.pdf (last visited on Sept. 8, 2005).

14 findBIOMETRICS.com, *supra* note 9.

15 INTERNATIONAL BIOMETRICS GROUP, PRIMARY FACIAL RECOGNITION TECHNOLOGIES, http://www.biometricgroup.com/reports/public/reports/facial-scan_primary.html (last visited on Sept. 8, 2005).

識，侵入性較低，因此，大多數人均認爲臉部辨識系統爲較舒適之生物辨識方式[16]，然而臉部辨識系統可能因爲資料的年代久遠、環境燈光或者受辨識者的僞裝而影響辨識，甚至只要在攝影機前放置照片便可能通過臉部辨識系統，爲此某些臉部辨識系統除了針對臉部特徵進行辨識之外，同時亦將觀察或記錄受辨識者之眨眼或眼球轉動等特徵，以確認所辨識者確實爲人類之臉龐[17]。

1.4 掌型

掌型辨識過程是由受辨識者將手掌平放於掃描器上，將拇指、食指以及中指放置於正確的位置後，掃描器將掃瞄手指之長度、寬度、厚度以及手掌和手指之輪廓等資料，以作爲辨識之特徵[18]。掌型辨識雖然準確度較指紋辨識低，且辨識儀器之價格較高，但是因爲其優點在於使用容易、不易造假以及接受程度高等[19]，因此亦爲一種廣爲使用之生物辨識方式，美國 90%的核子設施均以掌型比對管制進出人員[20]。

1.5 虹膜

虹膜位於眼球表面，虹膜的中心便是瞳孔。虹膜上可供辨識的特徵爲指紋辨識的 10 倍，而且虹膜特徵永遠不會改變，即便是同一個人的左眼與右眼之虹膜亦不會相同[21]。虹膜辨識是由被辨識者靜止於攝影機前，以攝影

---

16 INTERNATIONAL BIOMETRICS GROUP, USER PERCEPTIONS, http://www.biometricgroup.com/reports/public/reports/facial-scan_perceptions.html (last visited on Sept. 8, 2005).

17 Joris Evers, *Biometrics Firms Seeks to Foil Fraudsters*, http://news.com.com/Biometrics+firm+seeks+to+foil+fraudsters/2100-7348_3-5905230.html (last visited on Jan. 8, 2006).

18 INTERNATIONAL BIOMETRICS GROUP, *supra* note 5.

19 *Id*.

20 Robin Feldman, *Considerations on the Emerging Implementation of Biometric Technology*, 25 HASTINGS COMM. & ENT. L.J. 653, 660 (2003).

21 FINGERMAN, *supra* note 13, at 15.

機拍攝虹膜上分布之斑點與線條，藉由這些斑點與線條分布的位置作爲辨識之特徵[22]。

虹膜辨識之過程當中雖然並不會侵入人體，但是在辨識的過程中，被辨識者必須靜止不動，方能成功捕捉到虹膜特徵，即便過程十分短暫，仍可能造成部分使用者對虹膜辨識系統的不適應[23]。

1.6 聲紋

聲紋辨識是以每個人聲音之不同作爲辨識身分的方式，由於聲紋辨識僅需要透過收音器將聲音傳輸至辨識端，即可進行辨識，因此不論是電話或者電腦之麥克風均可以作爲辨識之工具，但是隨著收音器的收音品質不同，亦可能會影響聲紋辨識之準確度[24]。

由於聲紋辨識使用方便，因此使用者對聲紋辨識技術的接受度頗高，而雖然聲音可以被模仿，但是由於機器辨識聲紋過程中，其注重之處與人類聽覺注意之處並不相同，故而對於模仿之聲音亦可能加以成功辨識[25]。但是聲紋辨識並不適合作爲主要的生物辨識方式，因爲聲紋辨識會受到收音麥克風品質、背景噪音的音量或者受辨識者喉嚨不適等的身體狀況而影響[26]。

---

22 DEPARTMENT OF COMMUNICATIONS, INFORMATION TECHNOLOGY AND THE ARTS, BIOMETRICS: AN AUSTRALIAN GOVERNMENT PERSPECTIVE 8, http://www.dcita.gov.au/__data/assets/pdf_file/23467/Biometrics_-_An_Australian_Government_perspective.pdf (last visited on Sept. 8, 2005).

23 INTERNATIONAL BIOMETRICS GROUP, IRIS RECOGNITION ISSUES, http://www.biometricgroup.com/reports/public/reports/iris-scan_issues.html (last visited on Sept. 8, 2005).

24 INTERNATIONAL BIOMETRICS GROUP, *supra* note 5.

25 BOWMAN, *supra* note 1, at 6-7.

26 ELECTRONIC FRONTIER FOUNDATION, BIOMETRICS WHO'S WATCHING YOU?, http://www.eff.org/Privacy/Surveillance/biometrics/ (last visited on Sept. 8, 2005).

1.7 視網膜

視網膜位於眼球內層，視網膜辨識是以視網膜上之血管分布作爲身分辨識之特徵[27]，視網膜上可供辨識之特徵約爲指紋之 20 倍，爲所有生物辨識技術當中最多的一種[28]。

視網膜辨識過程當中，使用者必須將眼睛持續張開，放置於攝影機前，由光線穿入眼睛，捕捉視網膜上血管分布之特徵[29]。視網膜辨識技術的優點在於其辨識速度快、準確度高且用以儲存資料之模組小[30]。但是由於辨識過程可能會引發不適，且光線穿入眼睛具有侵入性，因此，對於使用者來說，較不舒適[31]。此外，視網膜上分布之血管在青春期之前仍可能會有所改變，另外，懷孕亦可能導致視網膜上的血管變化因而辨識失敗[32]。

1.8 其他

除了上述幾種比較常見的生物辨識技術之外，仍有許多不同的生物辨識技術，研究以不同的人體特徵辨識身分。美國國防部之進階防禦研究計劃署（Defense Advanced Research Project Agency, DARPA）已研發出以雷達脈衝辨別個人步伐、手臂以及腿部的運動，以在人群中辨識出特定身分者，並判斷對方與辨識機器之間的距離，目前該技術之辨識成功率約在 85-90%之間[33]。另外，日本富士通（Fujitsu）公司則研發出以紅外線掃瞄手掌的血管分布，以辨識身分之生物辨識技術，該技術之優點在於不需要接觸機器，便

---

27 BOWMAN, *supra* note 1, at 5.

28 FINGERMAN, *supra* note 13, at 11.

29 DEPARTMENT OF COMMUNICATIONS, *supra* note 22, at 8.

30 BOWMAN, *supra* note 1, at 5.

31 FINGERMAN, *supra* note 13, at 12.

32 Moo-Young, *supra* note 6, at 429.

33 Robert Lemos, *Researchers See Strides in Biometrics*, http://news.com.com/2100-1001-962734.html (last visited on Sept. 8, 2005).

可以進行身分辨識[34]。

除了可見之外觀特徵外，亦有發展出以超音波測量中指最長的骨頭之密度，以辨識使用者年齡的生物辨識技術，該技術可以用以防止兒童接觸不適宜之網路內容[35]。在使用電腦時，敲擊鍵盤之節奏亦可辨識個人身分，並且只要透過軟體安裝即可進行辨識，目前已有網路業者以此辨識客戶，以避免用戶數人共享同一個帳號、密碼[36]。

2. 生物辨識技術之應用與準確度

2.1 生物辨識技術之應用

一般而言，生物辨識技術用以辨識個人身分之方式大致可分爲兩種：「確認」（verify）以及「辨認」（identify）。「確認」是由使用者出示卡片或其他儲存生物辨識特徵之設備後，系統將卡片中所儲存之個人特徵與使用者之特徵進行比對，屬於一對一之比對方式；「辨認」指以使用者之特徵和資料庫當中所儲存之資料進行比對，爲一對多之比對方式[37]。若選擇以「辨認」的方式進行生物辨識，則首先必須建立生物辨識資訊資料庫，方得以進行辨認，但若以「確認」方式進行生物辨識，則由使用者自行攜帶存有其生物辨識資訊之設備，而不需建立資料庫。兩種方式各有其優缺點：兩者均可以達到辨識個人身分的目的，但「確認」方式，僅能確定卡片中儲存的生物辨識特徵爲持卡人所有，但卡片上記載的身分是否真的就是持卡人本

---

34 Dan Ilett, *Fujitsu Sees Biometric Future in Palms*, http://news.com.com/Fujitsu+sees+biometric+future+in+palms/2100-7355_3-5611477.html (last visited on Sept. 8, 2005).

35 Robert Lemos, *Hand Scan Could Limit Kids' Net Access*, http://news.com.com/Hand+scan+could+limit+kids+Net+access/2100-1029_3-5571671.html (last visited on Sept. 8, 2005).

36 ELECTRONIC FRONTIER FOUNDATION, *supra* note 26.

37 GAO, CHALLENGES IN USING BIOMETRIC TECHNOLOGIES 2-3, http://www.gao.gov/new.items/d04785t.pdf (last visited on Sept. 8, 2005).

人，則有賴製作卡片之防僞造以及其他安全維護機制的配合，方能減少此機制之風險；而「辨認」方式的風險則存在於建置生物辨識資訊資料庫本身，例如：駭客入侵、身分資訊輸入資料庫產生錯誤，或者該資訊在當事人不知情的情況下遭資料庫管理者誤用或濫用等。當然，兩種身分辨識方式亦可結合在一起，以提供更進一步的安全保障。

2.1.1 各國出入境管制

2.1.1.1 機場

冰島的凱夫拉維克（Keflavik）國際機場爲世界各國當中，第一個使用生物辨識技術之國際機場，美國波士頓機場[38]、澳洲雪梨國際機場[39]等亦正試驗臉部辨識系統，而德國法蘭克福（Frankfurt）機場[40]則是裝設虹膜辨識系統。

英國政府則是要求所有申請簽證者必須在抵達英國之機場時留下指紋資料，自 2004 年 12 月起，英國各機場亦進行電子通關系統（e-border system）之試驗，通關旅客可自願留下虹膜資料作爲辨識方式，並以虹膜辨識快速通關[41]。美國政府則是自 2004 年 1 月 12 日起，執行 US-VISIT 計劃，所有持非移民護照且從某些特定國家進入美國之旅客均必須留下照片以及指紋資料。另外，美國政府亦推動 Trusted Traveler 計劃，自願參加者可以獲

---

38 Thomas C. Greene, *Face Recognition Fails in Boston Airport*, http://www.theregister.co.uk/2002/07/20/face_recognition_fails_in_boston/ (last visited on Sept. 8, 2005).

39 The National Business Review, *Face Scan Technology Fails at Border-Update*, http://www.nbr.co.nz/home/column_article.asp?id=5293&cid=3&cname=Technology (last visited on Feb. 7, 2005).

40 Dinesh C. Sharma, *Iris Scanning to Begin at German Airport*, http://news.com.com/Iris+scanning+to+begin+at+German+airport/2100-7348_3-5158973.html (last visited on Sept. 8, 2005).

41 Jo Best, *Fingerprints, Iris Scans to Tighten U.K. Borders*, http://news.com.com/Fingerprints%2C+iris+scans+to+tighten+U.K.+borders/2100-1029_3-5566612.html (last visited on Sept. 8, 2005).

得一張智慧卡，儲存指紋或虹膜辨識資訊後，以該張智慧卡快速通關[42]。

2.1.1.2　生物辨識護照

除了在機場加裝生物辨識系統外，ICAO（International Civil Aviation Organization）自 1997 年開始推動電子護照（e-passport），並於 2002 年決議以臉部辨識、指紋辨識以及虹膜辨識作爲電子護照之生物辨識技術選項[43]。而美國國會則於 2002 年立法限期要求 27 個免簽證國家發行高科技護照[44]，各國若未能於 2006 年 10 月前在護照上附加數位照片，則該國國民將無法免簽證進入美國[45]。

目前計劃發行電子護照並將生物辨識技術納入之國家包括有美國、歐盟各國、澳洲、紐西蘭、加拿大、日本、韓國等[46]。其中美國政府計劃於 2006 年底完成換發儲存生物辨識資訊之電子護照的工作[47]。歐盟原先計劃於 2006 年開始發行電子護照，初期電子護照當中僅以 RFID 晶片儲存護照持有者之臉部辨識資訊，三年之後，再進一步於電子護照當中增加持有者之指

---

42 Eric P. Haas, *Back to the Future? The Use of Biometrics, It's Impact on Airport Security, and How This Technology Should Be Governed*, 69 J. AIR L. & COM. 459, 480 (2004).

43 Michael Kanellos, *E-passports to Put New Face on Old Documents*, http://news.com.com/E-passports+to+put+new+face+on+old+documents/2100-7337_3-5313650.html (last visited on Sept. 8, 2005).

44 Edward Alden & Sarah Laitner, *U.S. to Compromise on Biometric Passports*, http://www.msnbc.msn.com/id/8157125/&&CE=3032071 (last visited on Sept. 8, 2005).

45 Reuters, *U.S. Pushes Back Europe's E-passport Deadline*, http://news.cnet.co.uk/gadgets/0,39029672,39190098,00.htm (last visited on Sept. 8, 2005).

46 財團法人國家實驗研究院科技政策研究與資訊中心，「市場報導：全球生物辨識系統市場」，網站：http://cdnet.stic.gov.tw/techroom/market/ee/ee001.htm（最後點閱時間：2005 年 9 月 8 日）。

47 U.S. DEPARTMENT OF HOMELAND SECURITY, FACT SHEET: SECURE BORDERS AND OPEN DOORS IN THE INFORMATION AGE, http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0838.xml (last visited on July 9, 2006).

紋資訊[48]，不過由於技術上仍有未能克服之處，歐盟已經將在護照當中以晶片儲存生物辨識資訊之計劃撤銷[49]。英國雖然同爲歐盟會員國，但已決定在發行電子護照部分獨立作業，目前英國已於 2006 年第一季開始發行電子護照，初期電子護照當中僅儲存臉部辨識資訊，日後視情況再加入其他生物辨識資訊[50]。

2.1.2 進出管制

除了機場之外，仍有許多場所以生物辨識技術管制進出之人員，如美國之賭場以臉部辨識技術過濾進入之賭客是否列名不受歡迎名單[51]，而美國運通（American Express）則是於卡片中儲存員工之生物辨識資訊，作爲辦公室之門禁管制方式[52]。此外，美國政府則是在 2006 年編列了 6 百萬美元之預算發行 DAC（Department of Homeland Security Access Card）予 4 萬名國土安全部門之員工，在卡片中儲存持卡人之指紋辨識資訊，於持卡人進出政府單位時進行指紋辨識以確認身分，未來將以 DAC 爲聯邦、州以及各地方政府單位進出管制方式[53]。

---

48 Lars Pasveer, *Europe Likely to Opt for Biometric Passports*, http://news.com.com/Europe+likely+to+opt+for+biometric+passports/2100-1012_3-5429679.html (last visited on Sept. 8, 2005).

49 Statewatch, *EU: The Collision of Chips*, http://database.statewatch.org/unprotected/article.asp?aid=26996 (last visited on July 9, 2006).

50 Steve Ranger, *U.K. E-passports Start Their Travels*, http://news.com.com/U.K.+e-passports+start+ their+travels/2100-7348_3-6041491.html (last visited on July 8, 2006).

51 Scheeres, *supra* note 3.

52 REID Journal, *Amex Opts for Biometric RFID Card*, http://www.rfidjournal.com/article/view/309/1/1/(last visited on Sept. 8, 2005).

53 ELECTRONIC PRIVACY INFORMATION CENTER, SPOTLIGHT ON SURVEILLANCE, http://www.epic.org/privacy/surveillance/spotlight/0405/ (last visited on Sept. 8, 2005).

2.1.3　身分證明文件

英國目前正計劃於 2008 年發行存有生物辨識資訊之身分卡（ID card），未來凡是英國國民均領有身分卡，該身分卡將儲存持卡人之虹膜辨識、指紋辨識以及臉部辨識資訊[54]。除了英國之外，加拿大、美國各州以及部分歐洲國家以及中國大陸、馬來西亞等亞洲國家亦已發行儲存個人生物辨識資訊之駕照或身分卡，或者計劃在未來發行類似身分證明文件[55]。

2.1.4　治安維護

在治安維護方面，生物辨識資訊除了可以幫助刑事偵察外，亦可裝設於公共場所，以往來民眾之生物特徵與資料庫中之名單作比對，幫助警方發現危險人物。在 2002 年鹽湖城冬季奧運會時，美國聯邦調查局（FBI）便以臉部辨識系統掃瞄參與開幕儀式的 5 萬多名觀眾[56]。2001 年時，美國警方於超級盃比賽會場以臉部辨識系統對入場觀眾進行辨識，之後並在當地部分街道裝設監視攝影機對來往行人進行臉部辨識，將行人之臉部特徵與儲存通緝犯、蹺家少年以及性侵害犯罪者之資料庫進行比對，但是在該系統裝設的兩年期間，並未有任何比對成功之案例[57]。而以色列國防部亦以臉部辨識系統配合錄影監視掃瞄所有進出加薩走廊之民眾[58]。

54　Andy McCue, *Queen Gives Biometric ID Cards the Green Light*, http://news.com.com/Queen+gives+biometric+ID+cards+the+green+light/2100-7349_3-5464556.html?part=rss&tag=5464556&subj=news.7349.20 (last visited on Sept. 8, 2005).

55　Declan McCullagh, *National ID Cards on the Way*, http://news.com.com/National+ID+cards+on+the+way/2100-1028_3-5573414.html (last visited on Sept. 8, 2005).

56　Robert H. Thornburg, *Face Recognition Technology: The Potential Orwellian Implications and Constitutionality of Current Uses under the Fourth Amendment*, 20 J. MARSHALL J. COMPUTER & INFO. L. 321, 329 (2002).

57　Feldman, *supra* note 20, at 658.

58　Scheeres, *supra* note 3.

2.1.5 授權機制

生物辨識技術亦普遍使用於需要經由確認身分方可獲得授權進行之行爲，如自動提款機（ATM）之操作，便可以生物辨識取代提款卡，方便民眾不需要攜帶卡片便可以進行提款，美國、日本、南非和英國分別以臉部辨識、虹膜辨識或者拇指指紋辨識取代提款卡[59]，而澳洲則是在自動提款機裝設聲紋辨識以幫助老人或行動不便者操作提款機[60]。

另外，美國連鎖超市 Thriftway 在西雅圖地區裝設指紋辨識系統（Pay By Touch System），讓消費者通過指紋辨識後，透過已註冊的信用卡付款，試驗結果發現，許多消費者認爲不需要攜帶現金赴超市可以增加人身安全，因此十分樂意使用該系統[61]。

2.1.6 個人保密

生物辨識若結合生活用品，便可作爲個人生活保密之工具，但由於目前僅指紋辨識同時具有體積小以及價格低廉兩項優點，因此多數產品均以指紋辨識結合生活用品，如手機、電腦鍵盤[62]、隨身碟[63]等產品均可以生物辨識技術作爲加密方式，以防止個人隱私或商業機密外洩。

---

59 Scheeres, *supra* note 3; Roger Clarke, *Biometrics and Privacy*, http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html (last visited on Sept. 8, 2005).

60 Moo-Young, *supra* note 6, at 424.

61 Jo Best, *Supermarket: Let Your Fingers Do the Paying*, http://news.com.com/Supermarket+Let+your+fingers+do+the+paying/2100-1029_3-5559074.html (last visited on Sept. 8, 2005).

62 CNET, IBM LAPTOP FEATURES FINGERPRINT SCANNER, http://news.com.com/IBM+laptop+features+fingerprint+scanner/2100-1044_3-5395368.html (last visited on Sept. 8, 2005).

63 Dinesh C. Sharma, *SanDisk Flashes Biometric Storage Gizmo*, http://news.com.com/SanDisk+flashes+biometric+storage+gizmo/2100-1041_3-5608589.html (last visited on Sept. 8, 2005).

2.1.7　位置追蹤

生物辨識技術之普遍裝設，亦可以作爲記錄或追蹤個人行動、位置之工具，例如：在校園當中裝設指紋辨識系統，便可以追蹤、記錄學生到校時間以及在校園中之活動[64]，而以聲音辨識則可用以確認獲得假釋必須在家監禁者是否遵守假釋規定[65]。另外，臉部辨識系統配合閉路電視監視系統（CCTV）亦可以作爲追蹤個人行動之一種方式。

2.2　生物辨識技術之準確度

生物辨識技術之準確度以錯誤排斥率（false rejection rate, FRR）以及錯誤接受率（false acceptance rate, FAR）爲評估標準，所謂「錯誤排斥率」是指獲得授權之使用者被誤認爲不具資格者之機率，而「錯誤接受率」是指誤將盜用身分者辨識爲獲得授權者之機率。除了系統本身之設定外，針對使用者進行良好的訓練，使其在辨識過程中能夠正確使用生物辨識系統，亦可以明顯降低錯誤排斥率，一般使用而言，錯誤排斥率通常會在使用兩週後明顯下降[66]。

目前生物辨識技術的錯誤排斥率與錯誤接受率均可降低至 0.2%以下[67]，而在該範圍內，系統操作者可以自行決定錯誤排斥率與錯誤接受率之高低。若選擇降低錯誤排斥率，則可以避免合法使用者被誤判所引發之不便，然而選擇降低錯誤接受率則可以避免未經授權者通過辨識之機率，增加安全性。

就生物辨識技術之分類而言，生理特徵之生物辨識技術通常錯誤接受率較高，而行爲特徵之生物辨識技術通常錯誤排斥率較高，其中視網膜掃瞄幾乎是所有辨識技術當中準確度最高的一種，錯誤排斥率低，而錯誤接受率

64　Claudia Graziano, *Learning to Live with Biometrics*, http://www.wired.com/news/privacy/0,1848,60342,00.html (last visited on Sept. 8, 2005).

65　Moo-Young, *supra* note 6, at 427.

66　BOWMAN, *supra* note 1, at 3.

67　*Id*.

接近 0%[68]。但是由於視網膜掃瞄對使用者而言，侵入性較高且使用上較爲困難，因此，儘管辨識準確度高，仍未普遍使用。

目前計劃發行生物辨識護照或者生物辨識身分卡之國家，大多考慮使用指紋辨識、臉部辨識或虹膜辨識，但由於大多數生物辨識技術均未經大型資料庫測試，因此，對於生物辨識技術普遍應用於大規模辨識時之準確度仍有存疑。目前僅有英國以及美國政府對生物辨識系統進行大規模測試。

2.2.1 英國之測試

英國爲了決定身分卡中儲存之生物辨識特徵，在 2004 年 4 月至 12 月間，以 1 萬名自願者進行生物辨識試驗，所測試之生物辨識技術爲臉部辨識、指紋辨識以及虹膜辨識。其中臉部辨識技術之辨識準確率約爲 70%，爲三種生物辨識技術當中最低者，虹膜辨識最爲成功，辨識準確率可達 96%，指紋辨識則爲 81%[69]。在是否能夠成功取得其生物辨識特徵方面，以臉部辨識之成功率最高，接近 100%，在虹膜辨識方面，黑人以及 59 歲以上之民眾明顯較容易發生錯誤，而部分民眾亦在取得指紋過程中發生困難[70]。

2.2.2 美國之測試

美國政府針對各種不同之臉部辨識以及指紋辨識系統進行大規模測試，其之所以未進行虹膜測試的原因，在於目前缺乏足夠大的資料庫可以進行實驗[71]。美國商務部（Department of Commerce）之 FRVT 2002（Face Recognition Vendor Test 2002）便是針對臉部辨識系統所進行之測試，該測

---

68 *Id*. at 5.

69 ATOS ORIGIN, UK PASSPORT SERVICE BIOMETRICS ENROLMENT TRIAL REPORT 8, http://www.passport.gov.uk/downloads/UKPSBiometrics_Enrolment_Trial_Report.pdf (last visited on Sept. 8, 2005).

70 *Id*. at 7.

71 NATIONAL INSTITUTION OF STANDARDS AND TECHNOLOGY, SUMMARY OF NIST STANDARDS FOR BIOMETRIC ACCURACY, TAMPER RESISTANCE, AND INTEROPERABILITY 1, http://www.itl.nist.gov/iad/894.03/NISTAPP_Nov02.pdf (last visited on Sept. 8, 2005).

試以一個含有近 4 萬人之 12 萬張照片的資料庫進行辨識，結果發現可能影響臉部辨識系統之準確度的因素包括：

2.2.2.1　照片拍攝地點

以所有臉部辨識系統而言，表現最好之臉部辨識系統在對室內拍攝之照片進行辨識時，錯誤接受率爲 1%的情況下，辨識準確率爲 90%，但若以室外拍攝之照片進行辨識時，辨識準確率則降爲 50%[72]。

2.2.2.2　照片拍攝時間

若用以比對之照片並非當年度所拍攝之照片，則平均每經過一年，其辨識準確率下降 5%，亦即，若僅以臉部辨識作爲使用之生物辨識技術，則照片之更新有其必要[73]。

2.2.2.3　資料庫大小

當資料庫中僅有 800 人作爲比對之對象時，其辨識準確率爲 85%，而當資料庫增加爲 1 千 6 百人時，其辨識準確率下降至 83%，若資料庫增加爲 3 萬 7 千人以上時，辨識準確率僅爲 73%[74]。若是進行一對多之辨識，則測試名單爲 25 人時，錯誤接受率 1%之設定下，辨識準確率爲 77%，若測試名單多達 3 百人，則辨識準確率爲 69%[75]。

2.2.2.4　性別與年齡

男性與女性相較，男性之辨識成功率比女性高 6-9%。至於年齡部分，18-22 歲者辨識準確率爲 62%，38-42 歲者辨識準確率 74%，但超過 63 歲者，每增加 1 歲，臉部辨識系統之辨識準確率會提升 5%，亦即對臉部辨識系統年長者之辨識要比年輕人之辨識成功[76]。

72　P.J. PHILLIPS ET AL., FRVT 2002: OVERVIEW AND SUMMARY 2, http://www.frvt.org/DLs/FRVT_2002 _Overview_and_Summary.pdf (last visited on Sept. 8, 2005).

73　*Id.*

74　*Id.*

75　*Id.*

76　*Id.* at 5.

在指紋辨識部分，美國國家標準與技術研究院（National Institute of Standards and Technology）針對指紋辨識所進行之試驗發現，以 6 千個指紋的資料庫進行辨識，錯誤接受率設定爲 1%時，辨識準確率爲 90%，因此，若要將指紋辨識用於一個包含 4 千萬人之資料庫，則一個人必須提供至少 4 隻手指之指紋方能成功辨識[77]。

3. 生物辨識技術之隱私爭議

由於生物辨識技術具有辨識準確、使用便利以及加強安全等優點，但是，各種生物辨識技術所特有之優點，在生物辨識技術使用的同時亦可能帶來隱私權上的隱憂，而引發各種不同的爭議。

3.1 生物辨識資訊之蒐集

若欲使用生物辨識技術進行個人身分辨識，不可避免地必須先就個人之生物特徵進行蒐集，但生物辨識資訊之蒐集本身便可能存在法律上之爭議。由於個人之生物特徵不僅可以作爲辨識身分之用，同時亦可能涉及其他個人隱私的範圍，蒐集個人之生物特徵便可能引發重大爭議。以台灣近來之身分證換發爲例，政府欲將個人指紋資訊記載於身分證並建檔儲存之行爲，便引發社會重大爭議[78]。另外，冰島以基因和病歷建置資料庫，由於其目的在於進行基因之醫學研究，故其僅爲個人基因之蒐集以及基因資料庫之建立，但並不對個人身分加以辨識，所涉及者僅爲個人生物特徵之蒐集而無身分辨識之行爲，然亦因對於個人隱私之保障不足，而引發隱私權侵害之爭議[79]。

---

77 NATIONAL INSTITUTION OF STANDARDS AND TECHNOLOGY, *supra* note 71, at 2.

78 黃雅詩，「明年全面換身分證捺指紋」，請參閱下列網站：http://intermargins.net/Forum/2001% 20July-Dec/privacy/nation/na04.htm（最後點閱日：2006 年 9 月 9 日）。

79 Oksana Hlodan, *For Sale: Iceland's Genetic History*, http://www.actionbioscience.org/genomic/hlodan.html (last visited on Sept. 9, 2006).

3.2　獨特性與資料庫連結

3.2.1　生物辨識技術之獨特性

由於生物辨識技術進行身分辨識所依賴者爲個人之生物特徵，且所利用之生物特徵大多具有專屬個人之特性，即使雙胞胎亦不會擁有相同之生物特徵。同時，該生物特徵通常終身不變，不會因爲時間或者是受傷等其他因素而改變，因此使得生物辨識技術相較於其他身分辨識方法更具有可信度，常見的生物辨識技術當中。不論是指紋、虹膜、視網膜或者是血管分布均具有上述特性。

3.2.2　資料庫連結

由於生物辨識特徵具有人各不同之獨特性且不可變更，使得生物辨識資訊亦可能被用以連結各種不同的資料庫或者追蹤個人的各種交易行爲[80]，只要透過生物辨識技術的連結，加上電腦處理資料之能力，則可能建立關於個人日常生活所有私密細節的龐大資料庫，甚至以此對個人之各種私密活動或者性格進行詳細之側寫。以美國之社會安全號碼（social security number）爲例，該號碼原本僅用以配合社會福利系統，但 1943 年社會安全號碼被用來作爲永久帳號（permanent account），1961 年美國國稅局（Internal Revenue Service, IRS）將該號碼用以作爲納稅人之納稅辨識號碼（Taxpayer Identification Number, TIN），而後社會安全號碼更被作爲駕照、軍隊個人資料等的一部分，因此，只要得知個人之社會安全號碼，便可能進一步得知許多個人資訊[81]。同樣地，生物特徵的資訊原本僅作爲身分識別的用途，但由於生物特徵資訊用途的擴充，以及相關資料庫的交互連結，個人於社會上的生活狀況將可被有權力接近使用該等資訊者充分掌握。

80　George Tomko, *Biometrics as a Privacy—Enhancing Technology: Friend or Foe of Privacy*, http://www.dss.state.ct.us/digital/tomko.htm (last visited Sept. 8, 2005).

81　Nguyen, *supra* note 2.

3.3 資料庫建立與變更資料用途

3.3.1 資料庫建立之便利性

若銀行在提款機加裝生物辨識系統，且由用戶提供其生物辨識資訊建立資料庫，再以該資料庫和提款機進行連線，則用戶不需要攜帶提款卡，亦不需要記得任何密碼，便可以直接以其指紋或眼睛通過身分辨識，順利完成提款動作。以資料庫儲存生物辨識資訊，除了免去使用者持有任何卡片之負擔外，甚至可以直接透過網際網路進行身分辨識[82]。即便無生物辨識資料庫之建立，例如：在機場加裝生物辨識系統，雖然無法省去旅客攜帶護照之麻煩，但是，由於生物辨識系統操作過程快速，透過生物辨識技術確認旅客身分的方式，可以讓旅客更快速的通關。若要建立生物辨識資訊之資料庫，則以模組較小之生物辨識技術較爲適合，目前所有生物辨識技術當中，虹膜辨識、視網膜辨識以及指紋辨識均屬於模組較小之生物辨識技術，相對比較適合用以建立資料庫。

3.3.2 變更資料用途與資訊遺失之風險

然而，建立生物辨識資料庫固然可以爲使用者帶來諸多便利，但是一旦儲存生物辨識資訊之單位變更資料用途（function creep）時，則生物辨識資料庫所儲存之個人資訊便可能會被濫用或做目的外使用[83]。此時即便只有單一之生物辨識資料庫，然卻可能因爲儲存或使用該資料庫之單位變更資料庫用途之行爲，而產生對人權之侵害。在二次世界大戰期間，人口普查資料便遭到各國政府濫用，歐洲某些社會主義政府以人口普查資料辨別猶太人、同性戀者等不受歡迎人物；在美國，則以人口普查資料拘留日裔人士[84]。

---

82 Tomko, *supra* note 80.

83 Roger Clarke, *Biometrics and Privacy*, http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html (last visited on Sept. 8, 2005).

84 Solveig Singleton, *Privacy and Twenty-First Century Law Enforcement: Accountability for New Techniques*, 30 OHIO N.U. L. REV. 417, 435 (2004).

除了變更資料用途之外，一旦生物辨識資訊遺失，由於生物辨識特徵無法更改，因而可能會對當事人造成難以恢復之傷害，尤其若遺失之生物辨識資訊爲當事人生物特徵之原始圖檔時，只要使用同一個生物特徵之生物辨識系統，便可能會被有心人士冒用其身分。加以一般人相信生物辨識技術不會有誤，身分遭到盜用者在舉證上將會面臨困難[85]。即便遺失者爲當事人生物特徵經演算法轉換後之模組，而非原始圖檔，亦有可能會被以各種方式還原或轉換成其他生物辨識系統可辨識之模組而遭到身分盜用。

3.4　準確度與辨識錯誤

3.4.1　減少身分盜用

生物辨識技術之所以在近幾年受到世界各國政府重視，其主要原因之一在於生物辨識技術具有相當之準確度，目前各種常見之生物辨識技術均可將其錯誤接受率以及錯誤排斥率降低至 0.2%以下[86]。因此，若以生物辨識技術作爲身分辨識方式，相信可以減少許多身分盜用之問題，對政府取締非法移民或者銀行減少盜刷信用卡等各種身分犯罪之預防將會有莫大助益。

3.4.2　辨識錯誤之可能

然而，儘管生物辨識受到使用者高度的信賴，甚至被誤認爲絕對正確無誤，但是生物辨識技術畢竟並非百分之百準確無誤，因此，一旦生物辨識系統辨識錯誤卻未立即被發現，事後當事人要舉證生物辨識系統辨識錯誤將會十分困難。澳洲雪梨機場之臉部辨識系統便曾經錯誤辨識兩位交換護照之日本旅客，由於該日本旅客交換護照之目的僅爲測試臉部辨識系統，因此在事後通知雪梨機場該次錯誤事件。而儘管官方表示在過去 1 萬 6 千次辨識當

85　Roger Clarke, *Biometrics' Inadequacies and Threats, and the Need for Regulation*, http://www.anu.edu.au/people/Roger.Clarke/DV/BiomThreats.html (last visited on Sept. 8, 2005).

86　BOWMAN, *supra* note 1, at 3.

中，並無錯誤辨識的情況發生，但實際上若是有心人士成功矇騙生物辨識系統而進入澳洲，並不會主動通知相關單位，則雪梨機場可能會毫不知情[87]。

3.5 維持治安與寒蟬效應

3.5.1 維持治安

以閉路電視監視系統配合臉部辨識技術裝設於路口或重要公共場所，並建置含有通緝犯或逃家青少年等人之臉部辨識資訊的資料庫，一旦通緝犯或逃家青少年出現，該系統便會自動通知警方前往，可以幫助警方維持社區治安[88]。美國坦帕市（Tampa）警方在部分街道裝設閉路電視監視系統配合臉部辨識系統，捕捉所有過往行人的臉部辨識資訊，和一個含有 3 萬名通緝犯、翹家青少年以及性犯罪者之資料庫進行比對[89]。

裝設於公共場合用以辨識每位出入者的生物辨識技術，必須能夠在無使用者之配合下進行辨識，因此，臉部辨識技術爲最適合之方式，尤其目前世界各國大力推動閉路電視監視系統之架設，以閉路電視監視系統配合臉部辨識技術，不僅可以辨識每個經過的路人，甚至可以錄影，以便日後進行資料查詢。

3.5.2 寒蟬效應

對使用生物辨識技術之機構而言，生物辨識技術可以提高每個人行爲的透明度，且使用生物辨識技術的機構又可能與其他機構分享個人資訊。再者，隨著生物辨識資訊被用作各地點進出管制之方式，個人出現的時間、地點都可能會被儲存。因此，個人可能由於知道自己被觀察，因而進行「自我審查」，並造成寒蟬效應[90]。尤其是廣泛設置於各公共場所之閉路電視監視

87 The National Business Review, *supra* note 39.

88 Nguyen, *supra* note 2.

89 Feldman, *supra* note 20, at 658.

90 Clarke, *supra* note 85.

系統若配合臉部辨識系統，除了可以方便執法人員追蹤罪犯之外，亦可能作爲政府監督與追蹤異議份子行蹤之工具。中國裝設在天安門廣場用以控制交通的攝影機，在 1989 年時便被中國政府用以找尋與逮捕異議份子[91]。

然而一般人日常生活中於公共場所所進行之各種活動較難以主張隱私權之保護，若個人係參與政治聚會或社團等政治性活動，則或許可能主張言論自由的保障，但在政府維持社會治安的公共利益之下，除非有明顯濫用之證據，否則在主張上亦恐有困難[92]。

3.6　隱私保障與個人敏感資訊外洩

3.6.1　促進隱私保障

若是以生物辨識作爲個人資訊之加密方式，則可爲個人資訊帶來更高的保障。例如：以個人的指紋作爲私人的加密或者密碼鑰匙（coding key），以指紋爲個人的密碼加密，而資料庫當中僅儲存經過加密之密碼，辨識的過程中，使用者以其指紋爲儲存於卡片中之密碼解密之後，該密碼進入辨識系統通過身分辨識[93]。如此一來，使用者之指紋資訊不會被儲存在資料庫中，也不會在外流通，則不僅可以爲個人資訊增加一層安全防護，亦可以降低個人生物辨識資訊外洩的可能。

3.6.2　個人敏感資訊外洩

然而，即便以生物辨識技術作爲個人資訊之加密方式，可以降低個人生物辨識資訊外洩的可能性，但是，生物辨識的過程中，對個人生理特徵之細微觀察，不僅可捕捉個人之生物辨識資訊，亦可能獲知關於個人健康之敏感資訊。根據相關研究，指紋可能揭露與透納氏症候群（Turner’s syn-

---

91　Nguyen, *supra* note 2.

92　Roberto Iraola, *Light, Camera, Action! —Surveillance Cameras, Facial Recognition Systems and the Constitution*, 49 LOY. L. REV. 773, 800 (2003).

93　Tomko, *supra* note 80.

drome）、柯林菲特氏症（Klinefelter's syndrome）、唐氏症（Down's syndrome）、白血病、乳癌等疾病相關之個人健康資訊；虹膜掃瞄可能揭露當事人身體健康上懷孕、高血壓或者愛滋病、糖尿病、動脈硬化症之訊息；視網膜之掃瞄則可能得知個人糖尿病、動脈硬化症、高血壓或者靜脈注射毒品之疾病或行爲[94]。

3.7 小結

總結來看，不論是以掌型、臉部、指紋、視網膜、虹膜、聲紋或者個人簽名作爲生物辨識之方式，均可能產生資料庫不當連結以及辨識錯誤之危險。然在資料庫建立此一爭議上，由於指紋、視網膜以及虹膜此三種生物辨識資訊之模組較小，因此相較於其他生物辨識資訊，更適合用於建立資料庫。在此同時，此三種生物特徵用以辨識個人身分時，亦可能涉及洩露個人之健康資訊，因而有揭露個人敏感資訊之虞。

在寒蟬效應此一爭議上，由於臉孔乃是個人表現於外之生物特徵，爲所有生物特徵中較難以主張具有個人隱私保障之一種，且個人出入公共場合時，亦較可能在不知不覺中被他人以臉部特徵進行身分辨識，因而最可能被使用於公共場合之身分辨識，而產生寒蟬效應。至於聲紋雖然亦可能在個人不察覺之情況下遭他人用以辨識身分，然聲紋之辨識易受到外在環境之影響而錯誤，並不適合用於公共場合。至於指紋資訊雖然可能在當事人不知情的情況下加以蒐集，然若欲用於公共場合辨識當事人之身分，則必然需要當事人的配合方可能於當場辨識個人身分，因而引發寒蟬效應之可能性較低。本文以下以表格方式，列出各種生物辨識技術所可能引發的爭議：

---

94 Greg Star, *Airport Security Technology: Is the Use of Biometric Identification Technology Valid under the Fourth Amendment*, 20 TEMP. ENVTL. L. & TECH. J. 251, 254-256 (2002).

表 1　各種生物辨識技術與可能引發之爭議

	掌型	臉部	指紋	視網膜	虹膜	聲紋	簽名
資料庫連結	○	○	○	○	○	○	○
資料庫建立			○	○	○		
辨識錯誤	○	○	○	○	○	○	○
寒蟬效應		○					
敏感資訊			○	○	○		

4. 生物辨識技術與隱私

本文對生物辨識技術與隱私權之討論分成三個部分，首先將就公部門使用生物辨識技術之合憲性問題進行討論。然由於我國在資訊隱私權之憲法定位問題相關論述比較缺乏[95]，相較之下，美國之資訊隱私權理論發展較爲成熟，相關之最高法院判決亦比較豐富，加以我國大法官釋憲時，亦常以美國司法判決所建立之原則作爲參考，故本文將以美國最高法院與隱私權相關判決所建立之標準，討論公部門使用生物辨識技術是否有違憲之可能。其次，本文將針對其他國家關於公部門使用生物辨識技術之法律規範，包括建立全民身分卡系統以及生物辨識護照之發放進行分析，最後就其他國家對於私部門使用生物辨識技術之法律規範。透過上述三種不同層面的探討，針對生物辨識技術所涉及之隱私權議題進行討論。

95 雖然我國關於資訊隱私權之意義，於釋字第 585 號解釋中已有大法官加以分析，但是直至釋字第 603 號解釋關於戶籍法第 8 條強制按捺指紋一案，大法官才算是對資訊隱私權的議題有較為充分且全面性的討論。此外，我國關於資訊隱私權討論之期刊論文可參見劉靜怡，「資訊隱私保護的國際化爭議——從個人資料保護體制的規範協調到國際貿易規範的適用」，月旦法學雜誌，第 86 期，頁 195-205（2002)；陳起行，「資訊隱私權法理探討——以美國法為中心」，政大法學評論，第 64 期，頁 297-341（1990）；王郁琦，「資訊時代隱私權基礎理論初探」，世新法學，第 1 期，頁 283-305（2004）。

4.1 生物辨識技術之合憲性

生物辨識技術之合憲性議題，最主要牽涉到公部門對於生物辨識技術之使用，是否會侵犯人民之隱私權，而構成美國憲法第四增補條款所稱之搜索。

4.1.1 公共場合蒐集生物辨識資訊之合憲性

4.1.1.1 刑事搜索之合憲性

目前公部門對於生物辨識技術之使用，主要裝置於公共場合辨識個人身分，因此，一般個人在公共場合之合理隱私權期待（reasonable expectation of privacy）便成爲判斷政府部門使用生物辨識技術是否合憲之重要前提[96]。若個人得主張其具合理隱私權期待，亦即政府之搜索行爲，必須要有法院之搜索票（warrant）爲前提，否則便可能違反美國憲法第四增補條款。

根據美國聯邦最高法院在 *Katz v. United States* 案[97]當中所發展出之標準，判斷個人是否具有合理的隱私權期待，主要以當事人是否表現出主觀的隱私權期待，以及該隱私權期待在社會中是否會被視爲合理爲標準。若當事人確實具有合理的隱私權期待，則政府部門之行爲便構成美國憲法第四增補條款所欲規範之搜索行爲。透過上述標準之判斷，該案之當事人在公共電話亭撥打公共電話，儘管公共電話亭一般而言會被視爲公共場所，但因在話亭內撥打電話，當事人將門拉起來後即屬於私密空間，因此亦被認定爲具有合理之隱私權期待。由此可見，並非身處在公共場合時，個人便喪失合理之隱私權期待。在該案之判決當中，美國聯邦最高法院並強調美國憲法第四增補條款所保障者爲人而非場所，因此，不應以身處之場所爲判斷標準，而必須參酌當時之狀況[98]。

---

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

97 *Id.*

98 *Id.*

然而，就美國聯邦最高法院之後的判決來看，個人對於自己在公共場合之行動並無合理的隱私期待[99]，尤其是對於經常暴露於外的臉部和聲音，聯邦最高法院便曾明白宣示，個人並無合理隱私期待[100]。從這個角度看來，針對裝設於公共場合之生物辨識裝置，個人似乎很難主張其存在違反合理之隱私權期待，更遑論進一步推論生物辨識技術之使用違憲。

除了辨識過程中所使用之生理特徵外，在辨識過程中可能揭露之個人敏感資訊亦可能會影響生物辨識技術使用之合憲性問題。美國最高法院於 *Skinner v. Railway Labor Executives' Association* 案[101]之判決當中，認定呼吸、血液以及尿液檢驗構成美國憲法第四增補條款之搜索，其原因便在於該檢驗可能揭露個人健康方面的敏感資訊。因此，若生物辨識技術之使用過程當中，確實會揭露個人健康訊息，則個人亦可能主張合理隱私權期待之存在。在生物辨識過程當中，所儲存的如僅爲經演算法轉換後之「模組」，則或許可以降低揭露個人健康訊息之風險，但其所儲存者若爲個人生物特徵之「圖檔」時，則由於該圖檔極可能揭露個人健康訊息，個人可能主張合理隱私權期待之存在[102]。

就個別的生物辨識技術來看，雖然指紋之取得，過去被美國最高法院認爲並不構成搜索行爲[103]，但是若依 *Skinner* 案所建立的原則，在指紋可能揭露個人健康資訊的情況下，仍可能構成第四增補條款之搜索行爲，而虹膜辨識以及視網膜辨識亦可能因其揭露個人健康資訊而侵犯個人合理之隱私權期待。反之，如臉部辨識、掌型辨識、聲紋辨識等在辨識過程當中不會洩露

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

100 United States v. Dionisio, 410 U.S. 1 (1973).

101 Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602 (1989).

102 生物辨識特徵若是以模組方式儲存，由於將生物特徵經由演算法轉換為數字，因此不會透露個人之原始生物特徵。但若是以圖檔方式儲存生物辨識資訊，則是將個人生物特徵加以攝影儲存，因此個人之生物特徵在圖檔方式呈現下，除了可用以進行生物辨識之外，亦可能透露其他個人資訊。

103 Davis v. Mississippi, 394 U.S. 721 (1969).

個人健康資訊之生物辨識方式，若其裝設於公共場合用以辨識個人身分時，個人將難以主張其隱私權受到侵犯。

4.1.1.2 行政搜索之合憲性

行政部門使用生物辨識技術之方式主要爲在海關或邊境裝設生物辨識系統，以資料庫的方式，辨識被行政部門列入不受歡迎或可疑之恐怖份子，保障國家安全。行政部門使用生物辨識技術之合憲與否，除了前述考量因素之外，是否符合行政搜索（administrative search）之規定亦爲重要衡量因素之一。

所謂「行政搜索」是指政府單位爲了促成行政目的所做的管制的一部分，且非刑事偵察當中搜索犯罪證據的一部分[104]。行政搜索必須有實質的（substantial）政府利益存在、必須是管制計劃所需要採取之措施並且以法令取代搜索票授權[105]。因此，行政部門在海關或者邊境裝設生物辨識系統即便構成第四增補條款所謂之搜索行爲，在符合行政搜索必要之範圍的情況下，亦會被法院認定爲合憲之行政措施。

在政府利益部分之判斷，過去美國最高法院曾經表示沒有任何政府利益比國家安全更重大[106]，而且，在 *Katz* 案當中，多數意見亦在註解當中表示，若涉及國家安全，則該案之判決結果可能會有所改變[107]。且自美國 911 事件、英國倫敦大爆炸等重大恐怖份子攻擊事件接連發生，政府部門以保護國家邊境，避免可疑份子進入從事恐怖活動爲目的，在機場或海關裝設生物辨識系統之行爲，在法院進行衡量時，極可能傾向於認定爲具有重大政府利

104 Star, *supra* note 94, at 262.

105 Haas, *supra* note 42, at 487.

106 *Id*. at 464.

107 Kanya A. Bennett, *Can Facial Recognition Technology Be Used to Fight the New War against Terrorism? Examining the Constitutionality of Facial Recognition Surveillance Systems*, 3 N.C. J.L. & TECH. 151, 169 (2001).

益之行政措施[108]。

就海關的搜索行爲而言，在 2004 年時，於 *United States v. Manuel Flores-Montano* 案[109]當中，美國最高法院指出政府防止不受歡迎之人或物進入國境，最重要的一環便是在海關，且國會亦授權行政單位在不具有嫌疑或者搜索票的情況下，進行例行搜索和扣押，以避免違禁品進入本國。因此，在通過邊境時，海關人員進行的搜索並不需要嫌疑。而且在該判決當中，美國最高法院亦表示個人在通過海關時，其隱私期待比在國土內活動時低，因此標準亦不同。

儘管政府單位於邊境或海關裝設生物辨識系統之行爲可能會被認定爲確實具有重大政府利益存在，但前提爲國會之立法授權，並且在機場之行政搜索應僅限於爲了達成機場安全之目標所必須的手段以及範圍，不可以逾越保障機場安全所必須之程度，同時亦不可爲了與機場安全不相關之執法目的而進行搜索[110]。

4.1.2　生物辨識科技使用之合憲性

針對執法單位（law enforcement authority）使用各種科技是否侵犯人民隱私權，美國最高法院在 *Katz* 案之後，於 2002 年之 *United States. v. Kyllo* 案[111]當中提出了不同的標準檢驗警方所使用之科學儀器。在 *Kyllo* 案當中，警方以熱感應器偵測當事人之住家，透過不同溫度的反應進一步懷疑當事人種植大麻，並以此偵測圖片取得法院之搜索令。但是經過美國最高法院之審理，認定凡是住家當中之所有生活細節均屬於個人生活私密細節，加以警方所使用之儀器非一般大眾所能取得或使用之儀器，因此認定警方以熱感應器偵測當事人住家之行爲侵犯當事人之隱私權，並構成美國憲法第四增補

108 Star, *supra* note 94, at 265.
109 United States v. Manuel Flores-Montano, 541 U.S. 149 (2004).
110 Star, *supra* note 94, at 264.
111 Danny Lee Kyllo v. United States, 533 U.S. 27 (2001).

條款之搜索行爲。

由於 *Kyllo* 案所涉及之場合爲當事人之住宅，使得該判決結果是否將會普遍適用於所有場合仍有待美國最高法院其他判決之適用或解釋。雖然美國最高法院過去亦曾提及「一般大眾可取得」（available to the public）[112]，但是在該判決當中，美國最高法院首度以「一般大眾使用」（general public use）判斷當事人是否具有合理之隱私權期待，引起不小爭議。

在該判決之不同意見書中指出，該標準可能會在不同的時間點對同樣的技術做出不同之判斷。同時，該標準對警方而言太寬，以致於某些原先可能被認定合憲的儀器會被認定違憲，另外，不同意見書中亦提出第四增補條款所保護的是人，而非場所，因此多數意見不應以住宅爲判斷標準。亦有批評者認爲，若某項技術會侵害個人隱私，則該技術越廣泛適用所造成之侵害將越大，但是若根據該判決，則當該儀器非一般大眾使用時，大眾無法防範，因此構成搜索，若該儀器爲一般大眾所使用，則大眾應該自我保護[113]。

若以 *Katz* 案以及 *Kyllo* 案當中美國最高法院用以判斷執法單位是否侵犯當事人之隱私之標準，檢視生物辨識技術之使用是否合憲，則除了當事人是否表現出主觀的隱私權期待以及該隱私權期待在社會中是否會被認爲合理之外，生物辨識技術本身是否爲「一般大眾可使用」亦同樣可能成爲判斷標準。

就隱私權期待部分而言，由於生物辨識技術所使用之生物特徵大多爲個人顯露於外的生物特徵，因此，除了前述敏感資訊之取得，可能主張隱私權期待外，幾乎都難以主張隱私權期待之存在。但是亦有少數生物辨識技術使用之生物特徵並非明顯表露於外，例如：視網膜辨識技術之視網膜位於眼球後方，必須透過光線穿透眼球方能加以辨識，因此，仍有可能主張隱私權

112 Dow Chemical Co. v. United States, 476 U.S. 227 (1986).

113 Sean D. Thueson, *Fourth Amendment Search—Fuzzy Shades of Gray: The New "Bright-Line" Rule in Determining When the Use of Technology Constitutes a Search*, 2 WYO. L. REV. 169, 195-196 (2002).

之期待。

至於「一般大眾可使用」之標準若用以判斷生物辨識技術，則由於目前市面上已有不少結合生物辨識技術之電腦產品，以生物辨識技術作爲住宅或汽車之門鎖亦所在多有，甚至目前世界各國均紛紛研議發給人民具有生物辨識之身分證件，因此，生物辨識技術極有可能被認定爲一般大眾可取得或使用之技術。

另外，執法單位使用生物辨識技術時，除了進行個別身分辨識之外，亦可能以建立資料庫的方式，儲存通緝犯、失蹤人口等希望尋找之對象的生物辨識資訊，並裝置於公共場合，一旦有任何與資料庫符合之對象出現，則啓動警報，通知附近的執法人員前往。

美國最高法院於 *Illinois v. Roy I. Caballes* 案[114]之判決當中，由於認定緝毒犬只會發現違禁品，並不會揭露其他私人物品，因而判定執法人員無搜索令卻以緝毒犬偵測當事人一事並不侵害當事人之隱私。本文以爲，若依此精神判斷，一旦執法單位建立通緝犯或失蹤人口之資料庫，並用於公共場合比對來往行人之身分，則由於資料庫比對的使用方式只會比對、過濾出儲存於資料庫中之對象，亦即遭到列案之通緝犯或失蹤人口，一般無辜公民的身分並不會被揭露，亦可能會被美國最高法院認定爲並不影響當事人之隱私。但是由於美國最高法院在 *Hiibel v. Sixth Judicial Circuit of Nevada* 案[115]中判決個人在被警察逮捕之前，有權拒絕揭露自己的身分，因此，若執法單位以全民資料庫，一一辨識往來公共場合之行人，則可能會被認定爲違憲之行爲。

在各種生物辨識技術當中，以臉部辨識技術配合閉路電視監視系統最方便使用，因此，美國加州以及維吉尼亞州均針對執法單位使用臉部辨識系統訂立州法加以規範[116]。其中維吉尼亞州不僅規定執法單位必須獲得法院

---

114 Illinois v. Roy I. Caballes, 2005 U.S. LEXIS 769 (2005).

115 Hiibel v. Sixth Judicial Circuit of Nevada, 540 U.S. 965 (2003).

116 David McCormack, *Can Corporate America Secure Our Nation? An Analysis of the Identix Framework for the Regulation and Use of Facial Regulation Technology*, 9 B.U. J. SCI.

之授權方可裝設臉部辨識系統，並且限制僅能於可以提供與重罪、爲重罪通緝令所通緝之個人、恐怖份子或失蹤人口相關訊息時方可使用，同時對於裝設期間亦設有限制[117]。

4.1.3 小結

整體而言，若生物辨識技術所辨識之生物特徵爲明顯表露於外之生物特徵，則除非該生物特徵可能洩露個人健康或其他敏感資訊，否則個人將難以主張對該生物特徵具有合理之隱私權期待，進而拒絕該生物辨識技術之使用。其次，由於恐怖攻擊事件不斷，行政單位爲了保障國家安全，避免恐怖攻擊而使用生物辨識技術，極可能爲法院所認同。

然儘管由於個人在通過國境時，海關人員得在無嫌疑情形下對個人進行搜索，因此生物辨識技術使用於海關，同樣亦可能被認定爲合憲，但在護照上附加生物辨識特徵，以作爲通關檢查之用時，行政單位所蒐集或儲存之生物辨識特徵，仍應僅限於爲了保障國境安全之目的，原則上不得擅自進行任何目的外之使用，否則可能違反行政搜索之原則。

至於執法單位若於公共場所使用生物辨識技術，以辨識通緝犯或失蹤人口，則可能並不構成對一般人民之隱私權侵犯，但是若是使用於犯罪案件之偵辦過程中，則仍應獲得法院之授權，以避免執法單位在缺乏監督的情形下，濫用生物辨識技術而對隱私權保障有所影響。

4.2 公部門使用生物辨識技術之法律規範

4.2.1 生物辨識技術使用之建議

在推動生物辨識技術使用的同時，針對生物辨識技術與隱私之間的衡

& TECH. L. 128, 144 (2003); John J. Brogan, *Facing the Music: The Dubious Constitutionality of Facial Recognition Technology*, 25 HASTINGS COMM. & ENT. L.J. 65, 92 (2002).

117 Brogan, *supra* note 116, at 92-93.

平，亦有不少國家之隱私保護單位提出建議。其中，行政部門在推動生物辨識技術之使用之前，本應先建立完善的法律管制和隱私權保障制度，但是相關單位卻指出，事實上政府單位只是一味推動生物辨識技術之使用，卻完全忽略了法律規範和隱私權保障[118]。

歐盟資料保護工作小組（Data Protecting Working Party）所提出者主要爲生物辨識技術使用時應注意之事項，包括：

1.生物辨識技術之使用應有所限制[119]：如果生物辨識過度普遍的在日常生活中使用，則可能會使得人們對生物辨識資訊隱私的保障變得較不敏感或是較爲輕忽。例如：讓學童在學校圖書館使用生物辨識技術借還書，日後學童可能會較不注意生物辨識資料保護的風險和影響。因此，對於生物辨識技術之使用應謹慎評估，不可過度氾濫。

2.避免資料庫使用[120]：在生物辨識技術使用上，應避免以資料庫儲存大量生物辨識資訊，以避免大量生物辨識資訊外洩之風險，降低對資訊隱私權可能之侵害。

3.模組取代圖形[121]：除了對於生物辨識過程中所取得之不需要的資訊，應該儘速銷毀外，在儲存和辨識的過程中，應使用模組而非圖形，並且在以演算法轉換成模組之後，立即銷毀原始圖檔。

4.身分確認[122]：由於生物辨識資訊一旦建立，將會作爲當事人身分之表徵，並且受到相當之信任，因此，在建立生物辨識資訊和發放相關證件的過

---

118 GAO, SOME PROGRESS MADE, BUT MANY CHALLENGES REMAIN ON U.S. VISITOR AND IMMIGRANT STATUS INDICATOR TECHNOLOGY PROGRAM 11-12, http://www.gao.gov/new.items/d05202.pdf (last visited on Sept. 8, 2005).

119 Article 29 Data Protection Working Party (EU), *Working Document on Biometrics* 7, http://www.statewatch.org/news/2004/feb/biometric-wp80_en.pdf (last visited on Sept. 8, 2005).

120 *Id*.

121 *Id*. at 7-8.

122 *Id*. at 9.

程當中，對於當事人的身分應再三確認無誤，以確實避免身分盜用。

5.傳輸過程之安全性[123]：在生物辨識資訊傳輸過程當中，應該特別注意其安全性，避免透過網路傳輸，若透過網路傳輸時，則應更加注意。同時，應使模組無法還原成原始資料或圖檔，以降低生物辨識資訊遺失後可能之傷害。

澳洲之聯邦隱私委員會（Federal Privacy Commissioner）則針對生物辨識技術是否侵害個人隱私提出幾個評估方向，包括生物辨識資訊是否被儲存或用以連結許多個人資料庫、民眾是否有權選擇參與生物辨識與否、生物辨識技術是否用以秘密地蒐集資訊、當錯誤發生時，是否有適當的處理措施以及是否有內建機制防止變更資料用途[124]。另外，聯邦隱私委員會亦建議政府部門應針對生物辨識技術另立特別法，而非僅僅修改原先的法律[125]。至於如何評估生物辨識技術之使用是否適當，聯邦隱私委員會則認爲可以以下列準則判斷[126]：

1.分析（analysis）：仔細分析以確定所採取的行動爲必須、有效、符合比例以及對隱私侵害最小的措施，並且該措施應與大眾的期待相符。

2.授權（authority）根據該措施對隱私的影響不同，應有適當的授權，如對隱私有重大影響之措施，應有法律明文授權。

3.透明（accountability）：該措施之實行應透明、負責，並應建立獨立

123 *Id*.

124 OFFICE OF THE PRIVACY COMMISSIONER, GETTING ON IN THE ACT: THE REVIEW OF THE PRIVATE SECTOR PROVISIONS OF THE PRIVACY ACT 1988, 252, http://www.privacy.gov.au/act/review/revreport. pdf (last visited on Sept. 8, 2005).

125 *Id*. at 260.

126 E-mail from Hugh Clapin, Deputy Dir., Policy, Office of the Fed. Privacy 14. Comm'r, to John Carter, Sectional Comm. Sec'y, Joint Comm. of Pub. Accounts & Audit, Framework for Assessing and Implementing New Law Enforcement and National Security Powers 2, http://www.aph.gov.au/house/committee/jpaa/aviation_security/submissions/sub64.pdf (last visited on Sept. 8, 2005).

單位負責監督、報告、接受與處理申訴。

4.評估（appraisal）：應定期評估該措施之成本及利益。

而加拿大之資訊與隱私委員會（Information and Privacy Commissioner）曾經針對警方在賭場使用臉部辨識技術進行調查，除了確認警方並未濫用臉部辨識技術之外，亦要求警方必須明白告知所有進出賭場之賭客，警方於賭場裝設臉部辨識系統之事實[127]。至於社會福利單位使用生物辨識技術防止重複領取社會福利的部分，加拿大之資訊與隱私委員會則是建議[128]：

1.生物辨識資訊應轉換成模組後使用，而非以原始圖檔進行辨識，原始檔案並應在轉換爲模組之後，立即銷毀。

2.生物辨識資訊之使用應限於一對一之比對，確認當事人之資格，不可進行資料庫比對。

3.資料庫當中所儲存之指紋模組應無法重建，並且不得被用於進行其他目的之比對。

4.相關單位不能以指紋作爲確認身分的唯一方式。

5.對於接近、使用生物辨識資訊的工作人員應嚴格加以限制。

6.警方或政府若要接近、使用該資料庫，應先取得法院之命令。

7.生物辨識資訊不應和其他個人資訊共同儲存，同時該生物辨識資訊不得用以連結其他資料庫。

8.生物辨識資訊必須直接從當事人取得，不得以其他方式未經當事人同意或知悉取得。

---

127 INFORMATION AND PRIVACY COMMISSIONER, THE USE OF BIOMETRIC FACE RECOGNITION TECHNOLOGY IN ONTARIO CASINOS, http://www.accessandprivacy.gov.on.ca/english/pir/prov/pc010005.htm (last visited on Sept. 8, 2005).

128 INFORMATION AND PRIVACY COMMISSIONER, PRIVACY AND BIOMETRICS 4-6, http://www.ipc.on.ca /userfiles/page_attachments/pri-biom.pdf (last visited on Sept. 8, 2005).

4.2.2 英國之身分卡法案（Identity Cards Bill）

英國政府近來積極推動發行儲存有生物辨識特徵之身分卡，並且向國會提出了身分卡法案（Identity Cards Bill）。英國政府之計劃當中，身分卡將會儲存持有者之姓名、性別、出生時地、死亡日期、可供辨識之生理特徵等個人資訊[129]，由國務大臣（The Secretary of State）負責主導相關事務，但是身分卡內儲存之資訊內容以及儲存方式由身分卡法案明訂，除非經過國會同意，國務大臣不得自行更改[130]。身分卡法案當中其他關於隱私權的規定如下：

1.提供當事人資訊予第三人：經過當事人之授權或者同意，行政單位得提供當事人之基本資訊與第三人[131]。但若是當事人之生物辨識資訊、密碼等特殊敏感資訊，則必須另外取得當事人之單獨同意[132]。

2.當事人同意之例外：根據身分卡法案，在下列幾種情形，國務大臣不需要事先取得當事人之同意便可以提供當事人提供之資訊予政府單位。

(1)保安服務總監（the Director-General of the Security Service）、秘密情報服務之首領（the Chief of the Secret Intelligence Service）、政府通訊總部部長（the Director of the Government Communications Headquarters）、重大組織犯罪偵察局之局長（the Director General of the Serious Organised Crime Agency）爲了發揮該單位之功能所必須之資訊[133]。

(2)關於哪些個人資訊於何時提供給他人以及根據哪些法條等相關資料，若是爲了國家安全之利益、偵察或預防犯罪或其他由國務大臣所允許之目的，可以將其提供給警政首長[134]。

---

129 Identity Cards Bill, 2005, § 1(6) (Eng.).
130 *Id.* § 8(9).
131 *Id.* § 14(1).
132 *Id.* §§ 14(2)(g), 14(3).
133 *Id.* § 19(2).
134 *Id.* § 19(3).

(3)為了達成反恐、犯罪以及安全法（Anti-terrorism, Crime and Security Act 2001）第 17 條(2)(a)-(d)所訂定之目的，亦可以提供資訊給第三人[135]。

3.監督單位：由國務大臣指派之國家身分計劃委員會（National Identity Scheme Commissioner）負責監督相關行政單位之運作[136]，該委員會可監督國務大臣以及相關行政單位對於個人資訊之儲存及運用，以及身分卡之使用[137]等。但是，該委員會可監督之事項不包括行政處罰之上訴（appeals against civil penalties）、提供給保安服務總監、秘密情報服務之首領、政府通訊總部部長等單位之資訊及相關約定[138]。

英國之資料委員辦公室（Information Commissioner's Office）針對身分卡法案之內容，提出了幾點建議：

1.身分卡之用途：在身分卡法案當中，雖然已說明身分卡之用途，但仍過於廣泛，且若僅為建立可信之身分辨識系統，不需要建立資料庫，僅以卡片儲存持卡人之生物辨識資訊便可[139]。

2.儲存之資訊：國家註冊處（National Identity Register）所儲存的資料過於廣泛且會增加民眾更正個人資訊之負擔[140]，另外，政府計劃記錄民眾每一次出示、使用身分卡的時間、地點，並以資料庫儲存相關訊息，為不必要之措施[141]。

---

135 *Id.* § 20(2).

136 *Id.* § 24(1).

137 *Id.* § 24(2).

138 *Id.* § 24(3).

139 *See* INFORMATION COMMISSIONER'S OFFICE, THE IDENTITY CARDS BILL—THE INFORMATION COMMISSIONER'S PERSPECTIVE, http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/id_cards_bill_-_ico_perspective_dec_2004.pdf (last visited on Sept. 25, 2006).

140 *Id.* at 2.

141 *See* INFORMATION COMMISSIONER'S OFFICE, THE IDENTITY CARDS BILL—THE INFORMATION COMMISSIONER'S CONCERNS 2, http://www.ico.gov.uk/upload/documents/library/cor-

3.個人資訊之揭露：根據身分卡法案，可以接近使用該資料庫之政府單位過於廣泛[142]。

4.監督：由國務大臣所指定之國家身分計劃委員會負責監督相關行政單位之運作對民眾之保障不足，應允許資料委員監督該系統之運作[143]。

4.2.3 歐盟之生物辨識護照發放

在恐怖攻擊頻傳以及美國政府的壓力下，歐盟近幾年來亦積極規劃發行生物辨識護照，並針對歐盟國家發行生物辨識護照訂定相關規定。在歐盟針對生物辨識技術之使用所做的研究當中，建議在使用生物辨識技術的同時，應注意下列事項[144]：

1.清楚定義生物辨識技術應用的目的：避免相關單位變更資料用途並鼓勵使用者接受生物辨識技術之使用。

2.增進隱私保障：允許個人不需要揭露身分便可以進行確認，其方式是使用各種不同的生物辨識方式、分離個人資料，並發展各種保障隱私的措施和政策。

3.讓歐洲的生物辨識產業起飛：創造適當的隱私和資料保護機制，建立大眾對生物辨識技術的接受度，且建立開放、互容的標準，並透過新護照的發行，創造生物辨識技術的競爭市場，讓歐洲的生物辨識產業起飛。

4.保持彈性：在使用生物辨識技術的過程中，相關措施應保持彈性，以解決使用過程中可能發生的各種困難和錯誤。

5.進行研究：在重要領域進行更多的研究，多發展科技並根據實際配置的生物辨識系統累積經驗資料，在實際使用生物辨識技術之前，應該實施大

---

porate/detailed_specialist_guides/id_cards_bill_-_ico_concerns_october_2005.pdf (last visited on Sept. 25, 2006).

142 INFORMATION COMMISSIONER'S OFFICE, *supra* note 139, at 3.

143 *Id.*

144 OUT-LAW NEWS, BIOMETRICS INEVITABLE, BUT CHALLENGING, SAYS EU, http://www.out-law.com/page-5469 (last visited on Sept. 8, 2005).

規模的試驗。

在歐盟針對會員國之旅行文件或護照之安全以及生物辨識標準規則當中，明確規定會員國所發行之護照應包含臉部辨識以及指紋辨識資訊，且其儲存媒介應確保個人資料之相容性、可信度[145]。此外，會員國應該設立專屬機構負責旅行文件以及護照之發放[146]，並且文件持有人有權確認旅行文件或護照當中所儲存之個人資料，並得要求更正或刪除[147]。同時，該規則亦明訂儲存於護照或旅行文件當中之生物辨識資訊僅能用以確認該文件之真實性以及用以比對持有人和護照或旅行文件當中所儲存之生物辨識資訊是否相符[148]。

至於生物辨識護照詳細的規格，歐盟目前計劃以臉部辨識爲主要方式，雙手之食指指紋辨識爲次，若食指受傷或無法辨識，則在註明之後，以其他手指之指紋爲辨識，生物辨識資訊之儲存將以圖檔方式儲存，儲存媒介則爲 RFID 晶片[149]。

對於歐盟發行生物辨識護照之計劃，歐盟之資料保護工作小組也就個人隱私保障提出幾點意見：

1.生物辨識資訊之蒐集[150]：對於生物辨識資訊蒐集和處理之目的應有清楚的說明，並且在蒐集生物辨識資訊前應確認當事人確實爲其所宣稱之身

---

145 Council Regulation (EU) No. 2252/2004, Standards For Security and Biometrics In Passports and Travel Documents Issued By Member States, art. 1.2.

146 *Id.* art. 3.2.

147 *Id.* art. 4.1.

148 *Id.* art. 4.3.

149 *Working Document: EU-Passport Specification* 3-5, http://www.statewatch.org/news/2005/mar/biometric-implement.pdf (last visited on Sept. 8, 2005).

150 Article 29 Data Protection Working Party (EU) Opinion No. 7/2004, the Inclusion of Biometric Elements in Residence Permits and Visas Taking Account of the Establishment of the European Information System on Visas, at 4, http://www.statewatch.org/news/2004/sep/wp96.pdf (last visited on Sept. 8, 2005).

分。至於無法提供特定生物辨識資訊者，相關單位亦應加以保障，提供其他生物辨識方式。

2.降低錯誤排斥率[151]：使用生物辨識技術時，應盡可能降低錯誤排斥率，以避免生物辨識技術錯誤排斥合法持有文件者，造成當事人之不便與困擾。在通關過程中遭到拒絕者，應確保其獲知被拒絕的原因，並告知其可主張權利之方式且儘速澄清事實。

3.告知事項：個人資料之主體應被告知資料儲存期間、資料處理過程、申訴單位等相關資訊[152]。

4.個人資料保護[153]：儲存於晶片中的資料不可被發放護照單位以外之任何人更改，且該資訊不可在當事人無法察覺的情況下被讀取，而有權接近或使用該資訊者，應僅可接近、使用其執行職務所必須取得之資訊，所有登入使用、閱讀相關資料之紀錄應保存適當期間。

5.資料保存期間[154]：該生物辨識資訊之儲存期間最長應不可超過 5 年，若是短於 3 個月之簽證，其相關資訊不應保存超過 2 年。

4.2.4 台灣之釋字第 603 號釋憲案

2005 年修正之戶籍法第 8 條規定，年滿 14 歲之國民應請領國民身分證，且按捺並錄存其指紋，若不依規定按捺指紋者，則不發予國民身分證。此一強制全民按捺並錄存指紋之規定引發社會爭議，並進一步聲請解釋憲法，確認戶籍法第 8 條之規定是否違憲。司法院大法官於 2005 年 9 月做出

---

151 *Id*. at 6.

152 Article 29 Data Protection Working Party (EU), *Opinion on the 'Proposal for a Regulation of the European Parliament and of the Council Concerning the Visa Information System and the Exchange of Data between Member States on Short Stay-visas'* 14, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp110_en.pdf (last visited on Sept. 8, 2005).

153 Article 29 Data Protection Working Party (EU), *supra* note 150, at 6.

154 Article 29 Data Protection Working Party (EU), *supra* note 152, at 14.

釋字第 603 號解釋，認定戶籍法第 8 條之規定違反憲法第 22 條、第 23 條以及比例原則。

綜觀此次大法官所做出之釋憲，對於戶籍法第 8 條強制按捺指紋之規定的主要爭議有下列幾點：

1.指紋資訊之性質：由於指紋資訊具有觸碰留痕之特性，因此有大法官在不同意見當中主張指紋屬於中性之身分辨識工具，無涉於個人隱私[155]。亦有大法官提出指紋觸碰留痕之特性並不當然使得指紋成爲公開資訊，而即便爲公開資訊則亦可能在隱私權保障之範圍內[156]。在解釋理由書當中，多數意見認定指紋屬於具有高度人別辨識功能之個人資訊，若國家藉由身分確認而個人指紋資料並建檔管理，足使指紋形成得以監控個人之敏感資訊，因而認定指紋屬於相對敏感之個人資訊[157]。

2.違憲審查標準：由於對指紋資訊之性質有不同認定，因而大法官所主張適用之違憲審查標準亦有所不同，認定指紋資訊無涉於個人隱私者，主張應以無理由而不受理或者以美國之合理性標準審查[158]。然亦有大法官主張基於現代資訊科技的應用、指紋之特性、人別辨識功能與作爲開啓個人檔案之鑰的可能用途，應認定指紋資訊爲相當敏感之個人資訊，並採嚴格審查標準予以審查[159]。在解釋理由書當中，則是採折衷立場，將指紋資訊定位爲相對敏感之個人資訊，而以中度審查基準進行審查[160]。

3.立法目的：在審查的過程中，戶籍法第 8 條規定強制按捺指紋之立法目的亦引發諸多討論與爭議。有大法官主張透過對戶籍法第 8 條之修法動機

155 參見司法院釋字第 603 號解釋，余雪明大法官所提出之部分協同部分不同意見書。
156 參見司法院釋字第 603 號解釋，林子儀大法官所提出之協同意見書。
157 參見司法院釋字第 603 號解釋，解釋理由書。
158 前揭註 155。
159 前揭註 156。
160 前揭註 157。

與修法等立法史，可認定其立法目的包括治安之維持[161]，但是多數意見認爲防範犯罪顯然不在戶籍法立法目的所涵蓋範圍內，而不加以採納[162]，更有大法官進一步提出，若爲了刑事偵察犯罪之需要，可在缺乏合理懷疑或其他程序保障的前提下，要求全民指紋建檔，則當政府以同樣理由要求人民交出 DNA 資訊、虹膜紀錄等，又豈能拒絕[163]。

在此次大法官之釋憲過程中，多數意見採中度審查基準，認定指紋資訊爲個人資訊隱私權之一環，受到憲法第 22 條之保障，國家需基於明確之重要公共利益目的始得蒐集，且指紋資訊之蒐集並須爲與該公益目的之達成具備密切關聯之侵害較小手段，始符合憲法第 23 條比例原則之要求[164]。

而針對戶籍法第 8 條之立法目的，除了治安之維持爲多數意見所排除外，行政院所提出之加強新版國民身分證之防僞功能、防止冒領、冒用以及辨識迷途失智者、路倒病人、精神病患與無名屍體之身分等目的，亦爲多數意見認定不符合比例原則。就加強新版國民身分證之防僞功能而言，行政院之設計並無於身分證上設錄存指紋之欄位或提供指紋資料庫以供即時辨識之規劃，且新式身分證設置多項防僞措施，應足以達成防僞與防止冒用之目的。至於防止冒領以及冒用部分，此次換發身分證戶籍機關勢必透過其他戶籍資料交叉比對確認按捺指紋者之身分，由此可見透過其他資料之交叉比對亦可正確辨識身分，而不必然需要透過指紋比對辨識身分。最後則是迷途失智者、路倒病人、精神病患與無名屍體之身分辨識，多數意見認爲對於目前以身分不明、辨識困難者並無幫助，就未來而言，亦損益失衡、手段過當，不符合比例原則之要求[165]。基於上述推論，大法官認定戶籍法第 8 條第 2 項及第 3 項規定強制按捺並錄存指紋，以作爲核發身分證之要件，其目的爲

161 前揭註 155。
162 前揭註 157。
163 前揭註 156。
164 前揭註 157。
165 前揭註 157。

何，戶籍法並未明文規定，與憲法保障人民資訊隱私權之意旨不合。

除了對戶籍法第 8 條進行憲法解釋之外，大法官並提出，倘若未來國家大規模蒐集人民指紋並建立資料庫予以保管與應用，則其蒐集應與重大公益目的之達成相關並符合比例原則，且應明文禁止法定目的外之使用，並採取合時之科技技術及組織上與程序上之必要方式，以確保人民資訊隱私之安全[166]。並有大法官指出，目前我國之個人資訊保護法當中，雖然禁止對於個人資訊進行目的外利用，然個人資訊保護法第 8 條容許政府機關對個人資訊爲特定目的外之使用，且其要件極爲空泛、概括，實際上幾乎與空白授權無異，至於對於個人資訊隱私之保障，亦建議國家所採取組織保護措施應包括設置獨立、專業之資訊保護官，以幫助人民保護其個人資訊安全[167]。

釋字第 603 號解釋對於指紋資訊之討論，和其他國家針對生物辨識技術之使用與個人隱私保障所建立之法律規範之相同處，在於強調禁止法定目的外之使用，並強烈要求透過法律明訂蒐集個人生物辨識資訊之目的[168]。同時針對我國向來缺乏獨立、專業之個人資訊保護組織，代替人民監督政府對於個人資訊隱私之保護，亦有大法官在該解釋中提出政府應採取組織上以及程序上必要之防護措施，以符合憲法保障人民資訊隱私權之本旨。然釋字第 603 號解釋當中，並未對於政府建立指紋資料庫之必要性與風險進行討論，因爲就身分辨識之目的而言，單純的將指紋資訊儲存於個人身分證上便可進行個人身分辨識與確認，而不需要建立全民指紋資料庫，徒增大量指紋資訊遺失之風險。同時，由於生物辨識技術之準確度受到高度信任，因此在

166 前揭註 157。

167 參見司法院釋字第 603 號解釋，許宗力、曾有田大法官所提出之協同意見書。

168 目前已送進立法院待審議的「個人資料保護法」修正草案，其中第 6 條關於「敏感性資料」，亦即有關醫療、基因、性生活、健康檢查及犯罪前科等五類資料為特種資料，除符合法定要件外，原則上不得蒐集、處理或利用。當初草擬時係參考國外之立法例所制訂，但其精神應與釋字第 603 號解釋之意旨相符。不過指紋等生物辨識資訊是否屬於該草案之「敏感性資料」，恐有疑問。

建立生物辨識資訊資料庫前，對於個人身分確認之重要性便更不可輕忽，因爲一旦事前的身分確認有所錯誤，而造成個人身分與生物辨識資訊連結有所錯誤，將使得當事人難以舉證其身分遭到盜用，或者恢復其身分並更正錯誤之生物辨識資訊。

4.2.5 小結

由於生物辨識技術之使用可能產生資料庫連結、變更資料用途、辨識錯誤、寒蟬效應、個人敏感資訊外洩等問題之疑慮，因此，從上述討論當中不難發現，雖然每一個國家對於生物辨識技術之使用規範並不完全相同，然卻同樣重視前述可能產生之隱私權爭議，並加以規範。

1.避免資料庫建置：爲防止資料庫連結或其他因建置資料庫而導致對隱私權侵害之疑慮，原則上仍建議生物辨識技術之使用應儘量以一對一比對方式取代資料庫之建置。若建置資料庫，亦應當將生物辨識資訊單獨儲存，避免和其他個人資料有所連結。

2.禁止目的外利用：對於生物辨識技術之使用目的均強調應有所限制，不僅必須做清楚、明白之規定，並且應當告知當事人蒐集該生物辨識資訊之用途與目的，原則上禁止任何與原先蒐集生物資訊之目的不相關之使用或變更所蒐集之生物辨識資訊用途。

3.降低辨識錯誤之可能：除使用生物辨識技術時，應儘量降低錯誤辨識之機率外，生物辨識資訊亦應當有其儲存年限，定期更新，以避免因時間久遠而導致之辨識錯誤問題。另外，爲使當事人於辨識錯誤或其他意外狀況發生時，得以受到保護，在蒐集當事人之生物辨識資訊同時，應告知當事人申訴方式以及其他保障個人權益管道。

4.使用生物辨識資訊應公開、透明：若生物辨識技術之使用爲公開訊息而非秘密使用，且能事先告知當事人，並取得當事人之同意，則可避免寒蟬效應問題之產生。故多數國家均禁止秘密使用生物辨識技術，且不允許未經當事人同意或知悉之生物辨識資訊蒐集行爲。換言之，蒐集個人之生物辨識

資訊時，應事先告知當事人，並取得當事人之同意後爲之。

5.模組方式儲存生物辨識資訊：由於以圖檔方式儲存個人之生物辨識資訊所可能產生之疑慮遠大於模組，故多數國家均認爲應以模組方式儲存個人之生物辨識資訊，而非圖檔。如此可避免因圖檔外洩而洩露除生物辨識資訊外之任何個人敏感資訊。

6.建立監督機制：爲確實於使用生物辨識技術過程中，保障個人隱私，對於生物辨識技術之使用以及生物辨識資訊之儲存等相關事物應建立獨立之監督單位，以嚴格執行相關規範，防止任何侵害個人隱私之使用行爲發生。同時，對於接近、使用相關生物辨識資訊者亦應當嚴格管制，禁止任何非必要之工作人員接近使用生物辨識資訊。

4.3　私部門使用生物辨識技術之法律規範

在私部門使用生物辨識技術方面，除了用作個人或居家保全措施之外，金融機構亦積極使用生物辨識技術，希望能夠有效降低身分盜用所造成之損失。另外，爲了加強對進出人員的管制，有些公司也開始採用生物辨識技術作爲對員工進出管制之方式。有鑑於此，針對私部門使用生物辨識技術之規範亦日漸受到重視。美國加州便立法限制一般個人、商業或其他私部門僅得在爲了保護公共安全、個人財產或防止違法行爲時，合理使用生物辨識技術[169]。

4.3.1　金融機構之使用

根據美國聯邦交易委員會（Federal Trade Commission）統計，自 1998 年至 2003 年，約 2 千 7 百萬美國人曾經遭到身分盜用，消費者總計損失 5 兆美元，而商家以及金融機構則損失將近 48 兆美元[170]。而根據另一份於

169 McCormack, *supra* note 116, at 144.

170 Gwen “Wendy” Kennedy, *Thumbs up for Biometric Authentication!*, 8 COMP. L. REV. & TECH. J. 379, 380 (2004).

2003 年 1 月所做之調查顯示，在消費者對金融機構使用生物辨識技術之態度上，85%受訪者表示企業應該使用生物辨識技術確認以信用卡消費者，78%受訪者表示自動提款機應該加裝生物辨識技術。而在隱私權保障方面，90%受訪者表示如果企業蒐集、儲存客戶之生物辨識資訊，應該要揭露該訊息，85%的受訪者則希望有管道可以接近、更正他們的生物辨識資訊[171]。

美國之金融機構使用生物辨識技術可能帶來之隱私權隱憂在於，美國聯邦最高法院於 *United States v. Miller* 案[172]當中，確認個人對自己的銀行紀錄沒有正當的隱私期待，且美國之 GLB 法（Gramm-Leach-Bliley Act）允許銀行和其分支機構分享客戶資訊，因此，用戶之生物辨識資訊極可能因爲成爲銀行紀錄之一部分而失去隱私權期待，且蒐集客戶生物辨識資訊之金融機構更可能將該資訊與保險公司或其他分支機構分享[173]。

不過，由於生物辨識技術大多被金融機構採用爲用戶接近使用其帳戶時，確認身分之方式，而根據 GLB 法之規定，銀行不得與任何機構分享用戶接近使用帳戶之資訊[174]，因此，金融機構與其他機構分享用戶之生物辨識資訊的可能性並不高。而且，金融機構採用生物辨識作爲用戶接近使用帳戶之管制，亦可增加對用戶之保障。

我國於「金融控股公司法」中，雖規定金融控股公司及其子公司對於客戶個人資料、往來交易資料及其他相關資料，除其他法律或主管機關另有規定者外，應保守秘密，但對於金控公司與其子公司間的共同業務推廣、資訊交互運用等行爲，可於相關同業公會共同訂定自律規範，報經主管機關核定後實施[175]，其實質上已產生與美國 GLB 法類似的效果。近來關於金控法修正座談會中，主管機關亦表示考慮將放寬共同行銷之資訊共享行爲，如此

171 *Id.* at 399.
172 United States v. Miller, 425 U.S. 435 (1976).
173 Moo-Young, *supra* note 6, at 446.
174 Kennedy, *supra* note 170, at 398.
175 金融控股公司法第 42 條。

一來，則 GLB 法中關於銀行不得與任何機構分享用戶接近使用帳戶資訊之規定，於我國則有更重要之參考價值。

4.3.2 工作場合之使用

在工作場合使用生物辨識技術部分，加拿大之隱私委員會曾經針對私人企業員工之申訴做出裁決[176]，在該案件當中，員工申訴雇主強迫蒐集員工之聲音，以作爲聲紋辨識之用，而公司則表示由於該公司必須處理大量客戶資訊，爲了提供客戶資訊更高的保障，同時降低公司支出，因此採用聲紋辨識作爲管制員工接近、使用客戶資訊之方式。

在加拿大隱私委員會之調查下，認定由於該生物辨識系統確實可以增進公司的效率、節省費用、增加客戶資訊安全，且該系統僅可進行一對一比對，無法以一對多比對，並僅能用於客戶資訊之管制，無法對員工進行其他監督，因此在以該系統之實施所可獲得之利益與員工受損之隱私相權衡之下，認定該公司可以使用生物辨識技術，且不需要提供員工其他選擇。但是，隱私委員會同時強調，該公司對生物辨識技術之使用，不得用於其他不相關之目的，因此該公司之其他使用被隱私委員會認定爲不當之使用。

在我國，公司若於工作場合使用生物辨識技術作爲身分識別之用途，原則上只要能於事前告知，並使用於原先的特定目的範圍內，原則上即不違反個人資料保護法之精神[177]，但個人資料保護法修正草案中，對於蒐集個人資料時之告知事項有相關規定[178]，若草案通過後，則蒐集、利用生物辨識資訊之公司，自應遵守該等規定。

---

176 OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, PIPEDA CASE SUMMARY 281, http://privcom.gc.ca/cf-dc/2004/cf-dc_040903_e.asp (last visited on Sept. 8, 2005).

177 關於工作場合中雇主對員工之資訊監控行為與隱私權的關係，請參考王郁琦，「工作場合中電子郵件隱私權之研究」，資訊、電信與法律，頁 73-108（2004）。

178 相關規定請參考「個人資料保護法」修正草案第 8 條。

5. 結論與建議

隨著科技的進步，保有個人隱私似乎也變得越來越困難，但是，科技是否會對隱私造成侵害，端看人類如何使用與管制新科技的應用。如果政府能夠事先訂立完善的管制措施，詳細的評估各種應用可能帶來的隱憂，並建立良好的監督機制，那麼，生物辨識技術的應用，在促進國家安全的同時，並不必然會對隱私權帶來危害。

在美國 911 事件之後，各種恐怖攻擊事件時有所聞，世界各國紛紛開始努力朝向預防犯罪事件發生而努力，以避免任何可能造成重大傷亡的恐怖攻擊事件發生。但是在運用科技的同時，其實並不一定代表著隱私權保障必須有所讓步，以美國海關檢查爲例，運用透視機器檢查過往旅客，可以更精確的檢查出旅客是否攜帶了違禁物品，以及違禁物品藏於何處，但是同時也使得旅客的裸體爲海關人員所窺視，但是，只要以人體模型取代旅客的裸體形象，便可以在加強機場安全的同時，給予旅客應有的隱私[179]。

生物辨識的使用亦不例外，由於生物辨識技術用以確認個人身分之準確度遠勝過傳統之身分確認方式，因此，使用生物辨識技術作爲個人身分辨識方式以加強安全和保障，不僅可以幫助國家確定進出國界之旅客身分，同時對於各種重要場所之安全亦可增添幾分保障。但是，在廣泛使用生物辨識技術之前，應該先有完善的法律規範和評估，以確認生物辨識使用的同時，個人的隱私權亦受到應有之保障。日前我國司法院大法官針對戶籍法第 8 條建立全民指紋資料庫之規定所做之釋字第 603 號釋憲文當中便指出，由於政府蒐集、錄存人民指紋並建立資料庫之規定，缺乏法律明定其蒐集目的，並未明文禁止法定目的外之使用等，故而不符合憲法保障人民資訊隱私權之本旨[180]。但是該解釋並非排除日後政府機關使用生物辨識技術的可能性，只

---

179 Jeffrey Rosen, *The Naked Crowd: Balancing Privacy and Security in an Age of Terror*, 46 ARIZ. L. REV. 607, 608 (2004).

180 參見前揭註 167。

要符合該解釋所設定的條件，使用生物辨識技術仍不至於被認定爲侵害隱私權。

由於生物辨識資訊具有永久性和不可變更性，加以可預見未來生物辨識技術將會廣泛運用，一旦個人之生物辨識資訊外洩，所可能造成之損害難以預料，是故除了一般之個人資料保護外，應針對生物辨識資訊之特性，訂立明確的法律規範，並且應避免在明確的法律規範提供適當之隱私權保障前，貿然使用生物辨識技術或者蒐集個人之生物辨識資訊。而且，由於生物辨識資訊之特殊性與敏感性，對於生物辨識資訊更應加強保護，前加拿大隱私權委員會委員 George Radwanski 便曾提出一套類似美國法院所使用的嚴格檢查標準，用以作爲基本人權是否受到生物辨識技術使用之影響之判斷標準[181]。George Radwanski 認爲，法院應判斷其侵入性和所犯之罪是否成比例、對於阻止重罪發生是否具有實際效益、和防止重罪或恐怖攻擊之發生是否高度相關以及是否爲最小侵害手段。

綜合本文於前面章節之討論，生物辨識技術若使用於公共場合，則除非在使用生物辨識技術的過程中，以圖檔方式儲存可能會洩露個人敏感資訊之生物特徵，或者生物辨識技術辨識個人身分的同時，可能亦會揭露個人健康資訊，否則生物辨識技術使用於公共場合原則上可能並不會違反個人隱私權保障。再者，行政單位使用生物辨識技術於海關或邊界時，只要符合行政搜索之規範，爲了確保國家安全，原則上亦爲法律所允許之使用方式。至於執法單位使用生物辨識技術時，由於生物辨識技術目前已使用於一般日常生活當中，因此，一般人亦可輕易取得，若執法單位以一對一的方式比對生物特徵，對個人隱私亦無妨礙，但是，若是執法單位希望以資料庫比對個人身分，則資料庫當中僅能儲存執法單位欲發現之對象的生物辨識資訊，用以發現失蹤人口或通緝犯，如此對個人隱私侵害的疑慮較低。若執法單位以全民資料庫比對公共場合出入之個人的身分，則由於此舉將會揭露所有出入公共

181 Rosen, *supra* note 179, at 617.

場所之個人的身分，因此可能會對個人隱私造成侵害。

在私部門使用生物辨識技術部分，以金融單位爲例，銀行雖然應當保護客戶之個人資料，但是，由於相關法規可能會對於金融控股公司各子公司之間的資訊分享有所放寬，因此，若以個人生物特徵作爲接近使用帳戶之密碼，雖然可以提高帳戶之安全性，但是同時也可能導致個人生物辨識資訊在金融控股公司之子公司間成爲可分享之資訊。若生物辨識資訊使用於工作場所，則只要取得當事人之同意，原則上並不會被視爲對個人隱私權之侵害行爲。

本文認爲，在使用生物辨識技術之前，首先應該對生物辨識技術有正確的認知，瞭解生物辨識技術並非絕對正確無誤，同時，針對生物辨識技術之結果，應有完善的措施，進一步確認該辨識結果是否有誤，並提供受到辨識結果影響者應有之保障以及申訴之機會。另外，在使用生物辨識技術的同時，應明確告知使用者該生物辨識技術資訊之儲存方式、生物辨識資訊之管理和使用方式等訊息，並且應該給予當事人確認生物辨識資訊正確的管道。

在政府部門的使用上，應該盡可能禁止秘密的使用生物辨識技術，在當事人不知覺的情況下進行辨識或者蒐集其生物辨識資訊。若必須建立生物辨識資訊之資料庫，生物辨識資訊之儲存應與其他個人資訊分離，避免資料庫連結，同時應清楚說明該使用生物辨識技術之目的，禁止與該目的無關之使用與變更資料用途。對於執法單位之使用，應立有明確之規範，並透過法院監督確保執法單位之使用，並未對隱私權造成不當侵害。在私部門使用方面，應禁止以圖檔方式儲存當事人之生物辨識資訊以及建立大量生物辨識資訊資料庫之行爲，並建立妥善之監督機制，以防止用戶之生物辨識資訊外洩或遭到濫用。

隨著生物辨識技術之發展日趨成熟，以及世界各國對於身分認證準確之需求日增，可預見未來生物辨識技術之使用將不可避免地更爲廣泛與普遍，畢竟生物辨識技術之使用不僅可以減少各種身分盜用，亦可用於日常生活中，使得大眾之生活更爲便利與安全，在建構未來之無間隙社會（Ubiqui-

tous Network Society）的同時，生物辨識技術之使用亦爲不可或缺的一環，雖然我國目前生物辨識技術之使用尚未大爲普及，然亦不應輕忽建立生物辨識技術使用之隱私權保障規範的重要性，以避免未來各種生物辨識技術應用可能引發對個人隱私之衝擊。

參考文獻

中文書籍

王郁琦，《資訊、電信與法律》，元照出版，台北（2004）。

中文期刊

王郁琦，〈資訊時代隱私權基礎理論初探〉，《世新法學》，第 1 期，頁 283-305（2004）。

陳起行，〈資訊隱私權法理探討——以美國法爲中心〉，《政大法學評論》，第 64 期，頁 297-341（1990）。

劉靜怡，〈資訊隱私保護的國際化爭議——從個人資料保護體制的規範協調到國際貿易規範的適用〉，《月旦法學雜誌》，第 86 期，頁 195-205（2002）。

其他中文參考文獻

財團法人國家實驗研究院科技政策研究與資訊中心，〈市場報導：全球生物辨識系統市場〉，http://cdnet.stic.gov.tw/techroom/market/ee/ee001.htm（最後點閱時間：2005 年 9 月 8 日）。

黃雅詩，〈明年全面換身分證捺指紋〉，http://intermargins.net/Forum/2001%20July-Dec/privacy/nation/na04.htm（最後點閱時間：2006 年 9 月 9 日）。

英文期刊

Bennett, Kanya A., *Can Facial Recognition Technology Be Used to Fight the New War against Terrorism? Examining the Constitutionality of Facial Recognition Surveillance Systems*, 3 N.C. J.L. & TECH. 151 (2001).

Brogan, John J., *Facing the Music: The Dubious Constitutionality of Facial Recognition Technology*, 25 HASTINGS COMM. & ENT. L.J. 65 (2002).

Feldman, Robin, *Considerations on the Emerging Implementation of Biometric Technology*, 25 HASTINGS COMM. & ENT. L.J. 653 (2003).

Haas, Eric P., *Back to the Future? The Use of Biometrics, It's Impact on Airport Security, and How This Technology Should Be Governed*, 69 J. AIR L. & COM. 459 (2004).

Iraola, Roberto, *Light, Camera, Action!—Surveillance Cameras, Facial Recognition Systems and the Constitution*, 49 LOY. L. REV. 773 (2003).

Kennedy, Gwen "Wendy", *Thumbs up for Biometric Authentication!*, 8 COMP. L. REV. & TECH. J. 379 (2004).

McCormack, David, *Can Corporate America Secure Our Nation? An Analysis of the Identix Framework for the Regulation and Use of Facial Regulation Technology*, 9 B.U. J. SCI. & TECH. L. 128 (2003).

Moo-Young, Robyn, *"Eyeing" the Future: Surviving the Criticisms of Biometric Authentication*, 5 N.C. BANKING INST. 421 (2001).

Nguyen, Alexander T., *Here's Looking at You, Kid: Has Face-Recognition Technology Completely Outflanked the Fourth Amendment?* 7 VA. J.L. & TECH. 2 (2002).

Quarmby, Ben, *Biometrics: The Case for National DNA Identification Cards*, 2003 DUKE L. & TECH. REV. 2 (2003).

Rosen, Jeffrey, *The Naked Crowd: Balancing Privacy and Security in an Age of Terror*, 46 ARIZ. L. REV. 607 (2004).

Singleton, Solveig, *Privacy and Twenty-First Century Law Enforcement: Accountability for New Techniques*, 30 OHIO N.U. L. REV. 417, 435 (2004).

Star, Greg, *Airport Security Technology: Is the Use of Biometric Identification Technology Valid under the Fourth Amendment*, 20 TEMP. ENVTL. L. & TECH. J. 251 (2002).

Thornburg, Robert H., *Face Recognition Technology: The Potential Orwellian Implications and Constitutionality of Current Uses under the Fourth Amendment*, 20 J. MARSHALL J. COMPUTER & INFO. L. 321 (2002).

Thueson, Sean D., *Fourth Amendment Search—Fuzzy Shades of Gray: The New "Bright-Line" Rule in Determining When the Use of Technology Constitutes a Search*, 2 WYO. L. REV. 169 (2002).

其他英文參考文獻

Alden, Edward & Laitner, Sarah, *U.S. to Compromise on Biometric Passports*, http://www.msnbc.msn.com/id/8157125/&&CE=3032071 (last visited on Sept. 8, 2005).

Article 29 Data Protection Working Party (EU) Opinion No. 7/2004, the Inclusion of Biometric Elements in Residence Permits and Visas Taking Account of the Establishment of the

European Information System on Visas, http://www.statewatch.org/news/2004/sep/wp96.pdf (last visited on Sept. 8, 2005).

Article 29 Data Protection Working Party (EU), *Opinion on the 'Proposal for a Regulation of the European Parliament and of the Council Concerning the Visa Information System and the Exchange of Data between Member States on Short Stay-visas*, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp110_en.pdf (last visited on Sept. 8, 2005).

Article 29 Data Protection Working Party (EU), *Working Document on Biometrics*, http://www.statewatch.org/news/2004/feb/biometric-wp80_en.pdf (last visited Sept. 8, 2005).

Best, Jo, *Fingerprints, Iris Scans to Tighten U.K. Borders*, http://news.com.com/Fingerprints%2C+iris+scans+to+tighten+U.K.+borders/2100-1029_3-5566612.html (last visited on Sept. 8, 2005).

Best, Jo, *Supermarket*: *Let Your Fingers Do the Paying*, http://news.com.com/Supermarket+Let+your+fingers+do+the+paying/2100-1029_3-5559074.html (last visited on Sept. 8, 2005).

BOWMAN, ERIK, EVERYTHING YOU NEED TO KNOW ABOUT BIOMETRICS, http://www.ibia.org/EverythingAboutBiometrics.PDF (last visited on Sept. 8, 2005).

Clarke, Roger, *Biometrics and Privacy*, http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html (last visited on Sept. 8, 2005).

Clarke, Roger, *Biometrics' Inadequacies and Threats, and the Need for Regulation*, http://www.anu.edu.au/people/Roger.Clarke/DV/BiomThreats.html (last visited on Sept. 8, 2005).

CNET, IBM LAPTOP FEATURES FINGERPRINT SCANNER, http://news.com.com/IBM+laptop+features+fingerprint+scanner/2100-1044_3-5395368.html (last visited on Sept. 8, 2005).

DEPARTMENT OF COMMUNICATIONS, INFORMATION TECHNOLOGY AND THE ARTS, BIOMETRICS: AN AUSTRALIAN GOVERNMENT PERSPECTIVE, http://www.dcita.gov.au/_data/assets/pdf_file/23467/Biometrics_-_An_Australian_Government_perspective.pdf (last visited on Sept. 8, 2005).

ELECTRONIC FRONTIER FOUNDATION, BIOMETRICS WHO'S WATCHING YOU?, http://www.eff.org/Privacy/Surveillance/biometrics/ (last visited on Sept. 8, 2005).

ELECTRONIC PRIVACY INFORMATION CENTER, SPOTLIGHT ON SURVEILLANCE, http://www.epic.org/privacy/surveillance/spotlight/0805/ (last visited on Sept. 8, 2005).

E-mail from Hugh Clapin, Deputy Director, Policy, Office of the Federal Privacy 14. Commissioner, to John Carter, Sectional Committee Secretary, Joint Committee of Public Accounts & Audit, Framework for Assessing and Implementing New Law Enforcement and National Security Powers, http://www.aph.gov.au/house/committee/jpaa/aviation_security/submissions/sub64.pdf (last visited on Sept. 8, 2005).

Evers, *Biometrics Firms Seeks to Foil Fraudsters*, http://news.com.com/Biometrics+firm+seeks+to+foil+fraudsters/2100-7348_3-5905230.html (last visited on Jan. 8, 2006).

findBIOMETRICS.com, *About Fingerprint Scanning*, http://www.findbiometrics.com/Pages/fingerprint_articles/fingerprint_1.html (last visited on Sept. 8, 2005).

findBIOMETRICS.com, *Fingerprint Authentication—The Time Has Finally Arrived*, http://www.findbiometrics.com/Pages/fingerprint_articles/fingerprint_2.html (last visited on Sept. 8, 2005).

FINGERMAN, DAN, STATIC MEASUREMENTS AND MOVING TARGETS: PRIVACY, BIOMETRICS AND THE CONSUMER-BANK RELATIONSHIP, http://www.danfingerman.com/papers/Biometrics_ paper.pdf (last visited on Sept. 8, 2005).

GAO, CHALLENGES IN USING BIOMETRIC TECHNOLOGIES, http://www.gao.gov/new.items/d04785t.pdf (last visited on Sept. 8, 2005).

GAO, SOME PROGRESS MADE, BUT MANY CHALLENGES REMAIN ON U.S. VISITOR AND IMMIGRANT STATUS INDICATOR TECHNOLOGY PROGRAM, http://www.gao.gov/new.items/d05202.pdf (last visited on Sept. 8, 2005).

Gilbert, Alorie, *U.S. Moves Closer to E-passports*, http://news.com.com/U.S.+moves+closer+to+e-passports/2100-1012_3-5425314.html (last visited on Sept. 8, 2005).

Graziano, Claudia, *Learning to Live with Biometrics*, http://www.wired.com/news/privacy/0,1848,60342,00.html (last visited on Sept. 8, 2005).

Greene, Thomas C, *Face Recognition Fails in Boston Airport*, http://www.theregister.co.uk/2002/07/20/face_recognition_fails_in_boston/ (last visited Sept. 8, 2005).

Hlodan, Oksana, *For Sale: Iceland's Genetic History*, http://www.actionbioscience.org/genomic/hlodan.html (last visited on Sep. 9, 2006).

Ilett, Dan, *Fujitsu Sees Biometric Future in Palms*, http://news.com.com/Fujitsu+sees+biometric+future+in+palms/2100-7355_3-5611477.html (last visited on Sept. 8, 2005).

INFORMATION AND PRIVACY COMMISSIONER, THE USE OF BIOMETRIC FACE RECOGNITION TECHNOLOGY IN ONTARIO CASINOS, http://www.accessandprivacy.gov.on.ca/english/pir/

prov/pc010005.htm (last visited on Sept. 8, 2005).

INFORMATION AND PRIVACY COMMISSIONER, PRIVACY AND BIOMETRICS, http://www.ipc.on.ca/userfiles/page_attachments/pri-biom.pdf (last visited on Sept. 8, 2005).

INFORMATION COMMISSIONER'S OFFICE, THE IDENTITY CARDS BILL—THE INFORMATION COMMISSIONER'S CONCERNS, http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/id_cards_bill_-_ico_concerns_october_2005.pdf (last visited on Sept. 25, 2006).

INFORMATION COMMISSIONER'S OFFICE, THE IDENTITY CARDS BILL—THE INFORMATION COMMISSIONER'S PERSPECTIVE, http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/id_cards_bill_-_ico_perspective_dec_2004.pdf (last visited on Sept. 25, 2006).

INTERNATIONAL BIOMETRICS GROUP, FINGERPRINT GROWTH INHIBITORS, http://www.Biometricgroup.com/reports/public/reports/growth_inhibitors.html (last visited on Sept. 8, 2005).

INTERNATIONAL BIOMETRICS GROUP, HAND GEOMETRY: HOW IT WORKS, http://www.biometricgroup.com/reports/public/reports/hand-scan_tech.html (last visited on Sept. 8, 2005).

INTERNATIONAL BIOMETRICS GROUP, HAND GEOMETRY STRENGTHS AND WEAKNESSES, http://www.biometricgroup.com/reports/public/reports/hand-scan_strengths_weaknesses.html (last visited Sept. 8, 2005).

INTERNATIONAL BIOMETRICS GROUP, IRIS RECOGNITION ISSUES, http://www.biometricgroup.com/reports/public/reports/iris-scan_issues.html (last visited on Sept. 8, 2005).

INTERNATIONAL BIOMETRICS GROUP, OPTICAL – SILICON – ULTRASOUND, http://www.biometricgroup.com/reports/public/reports/finger-scan_optsilult.html (last visited on Sept. 8, 2005).

INTERNATIONAL BIOMETRICS GROUP, PRIMARY FACIAL RECOGNITION TECHNOLOGIES, http://www.biometricgroup.com/reports/public/reports/facial-scan_primary.html (last visited on Sept. 8, 2005).

INTERNATIONAL BIOMETRICS GROUP, SIGNATURE VERIFICATION: HOW IT WORKS, http://www.biometricgroup.com/reports/public/reports/signature-scan_tech.html (last visited on Sept. 8, 2005).

INTERNATIONAL BIOMETRICS GROUP, USER PERCEPTIONS, http://www.biometricgroup.com/reports/public/reports/facial-scan_perceptions.html (last visited on Sept. 8, 2005).

INTERNATIONAL BIOMETRICS GROUP, VOICE RECOGNITION: HOW IT WORKS, http://www.biometricgroup.com/reports/public/reports/voice-scan_tech.html (last visited on Sept. 8, 2005).

Kanellos, Michael, *E-passports to Put New Face on Old Documents*, http://news.com.com/E-passports+to+put+new+face+on+old+documents/2100-7337_3-5313650.html (last visited on Sept. 8, 2005).

Lemos, Robert, *Hand Scan Could Limit Kids' Net Access*, http://news.com.com/Hand+scan+could+limit+kids+Net+access/2100-1029_3-5571671.html (last visited on Sept. 8, 2005).

Lemos, Robert, *Researchers See Strides in Biometrics*, http://news.com.com/2100-1001-962734.html (last visited on Sept. 8, 2005).

McCullagh, Declan, *National ID Cards on the Way*, http://news.com.com/National+ID+cards+on+the+way/2100-1028_3-5573414.html (last visited on Sept. 8, 2005).

McCue, Andy, *Queen Gives Biometric ID Cards the Green Light*, http://news.com.com/Queen+gives+biometric+ID+cards+the+green+light/2100-7349_3-5464556.html?part=rss&tag=5464556&subj=news.7349.20 (last visited on Sept. 8, 2005).

NATIONAL INSTITUTION OF STANDARDS AND TECHNOLOGY, SUMMARY OF NIST STANDARDS FOR BIOMETRIC ACCURACY, TAMPER RESISTANCE, AND INTEROPERABILITY, http://www.itl.nist.gov/iad/894.03/NISTAPP_Nov02.pdf (last visited on Sept. 8, 2005).

OFFICE OF THE PRIVACY COMMISSIONER, GETTING ON IN THE ACT: THE REVIEW OF THE PRIVATE SECTOR PROVISIONS OF THE PRIVACY ACT 1988, http://www.privacy.gov.au/act/review/revreport.pdf (last visited on Sept. 8, 2005).

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, PIPEDA CASE SUMMARY, http://privcom.gc.ca/cf-dc/2004/cf-dc_040903_e.asp (last visited on Sept. 8, 2005).

ORIGIN, ATOS, UK PASSPORT SERVICE BIOMETRICS ENROLMENT TRIAL REPORT, http://www.passport.gov.uk/downloads/UKPSBiometrics_Enrolment_Trial_Report.pdf (last visited on Sept. 8, 2005).

OUT-LAW NEWS, BIOMETRICS INEVITABLE, BUT CHALLENGING, SAYS EU, http://www.out-law.com/page-5469 (last visited on Sept. 8, 2005).

Pasveer, Lars, *Europe Likely to Opt for Biometric Passports*, http://news.com.com/Europe+likely+to+opt+for+biometric+passports/2100-1012_3-5429679.html (last visited on Sept. 8, 2005).

PHILLIPS, P.J. ET AL., FRVT 2002: OVERVIEW AND SUMMARY, http://www.frvt.org/DLs/FRVT_2002_Overview_and_Summary.pdf (last visited on Sept. 8, 2005).

Ranger, Steve, *Tech Upgrade for Biometric Passports and ID Cards*, http://www.silicon.com/research/specialreports/idcards/0,3800010140,39150542,00.htm (last visited on Sept. 8, 2005).

Ranger, Steve, *U.K. E-passports Start Their Travels*, http://news.com.com/U.K.+e-passports+start+their+travels/2100-7348_3-6041491.html (last visited on July 8, 2006).

REID Journal, *Amex Opts for Biometric RFID Card*, http://www.rfidjournal.com/article/view/309/1/1/ (last visited on Sept. 8, 2005).

Reuters, *U.S. Pushes Back Europe's E-passport Deadline*, http://news.cnet.co.uk/gadgets/0,39029672,39190098,00.htm (last visited on Sept. 8, 2005).

Scheeres, Julia, *Smile, You're on Scan Camera*, http://www.wired.com/news/print/0,1294,42317,00.html (last visited on Sept. 8, 2005).

Sharma, Dinesh C., *Iris Scanning to Begin at German Airport*, http://news.com.com/Iris+scanning+to+begin+at+German+airport/2100-7348_3-5158973.html (last visited on Sept. 8, 2005).

Sharma, Dinesh C., *SanDisk Flashes Biometric Storage Gizmo*, http://news.com.com/SanDisk+flashes+biometric+storage+gizmo/2100-1041_3-5608589.html (last visited on Sept. 8, 2005).

Statewatch, *EU: The Collision of Chips*, http://database.statewatch.org/unprotected/article.asp?aid=26996 (last visited on July 9, 2006).

The National Business Review, *Face Scan Technology Fails at Border-Update*, http://www.nbr.co.nz/home/column_article.asp?id=5293&cid=3&cname=Technology (last visited on Feb. 7, 2005).

Tomko, George, *Biometrics as a Privacy-Enhancing Technology: Friend or Foe of Privacy*, http://www.dss.state.ct.us/digital/tomko.htm (last visited Sept. 8, 2005).

U.S. DEPARTMENT OF HOMELAND SECURITY, FACT SHEET: SECURE BORDERS AND OPEN DOORS IN THE INFORMATION AGE, http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0838.xml (last visited on July 9, 2006).

Working Document: EU-Passport Specification, http://www.statewatch.org/news/2005/mar/biometric-implement.pdf (last visited on Sept. 8, 2005).