目　次

表次

提要

壹、研究緣起

生物特徵，則是指任何可以用來辨識身分之用，並可被測量或使用的人類身體或生物特徵，包括臉貌、指紋、手掌紋、視網膜、聲音（語音）、體形等，因此，相應的生物特徵辨識技術，通常便有臉部識別、指紋識別、掌紋識別、虹膜識別、體形識別和簽字識別等。透過生物辨識技術的運用，可以作爲比對個人身分，進而得知個人出入的場所、活動的範圍等，這些活動原本均是涉及個人領域的活動，所以此等生物特徵辨識技術的運用，不免引發和個人資料保護及隱私權有關的爭辯。

這些對生物特徵辨識技術的應用現象，顯示科技的發展，已經激起政府使用生物特徵辨識技術的高度興趣。但是這種新技術的使用，難免對人民的隱私權產生另一波的衝擊。因此，各國莫不著手研擬保護個人資訊的新方式，有的國家選擇針對生物特徵辨識技術，另行訂立法律，有的國家則是在既有的個人資訊保護體制上，透過解釋的方式，因應新科技可能帶來的威脅。前者例如美國某些州的生物特徵法，後者最爲著名者則爲依據歐盟 1995 年「個人資料保護指令」（95/46/EC）第 29 條成立之「歐盟資料保護工作小組」於 2003 年 8 月 1 日公布了「生物辨識工作文件」，其中對於生物辨識特徵資料之應用所應注意的重點，也多所著墨。

反觀國內，對個人資訊普遍性的保護，來自電腦處理個人資料保護法的相關規定，但是，該法是制訂公布於 1995 年，當時生物特徵辨識技術尚未能普及應用，且該法對於個人資料的使用，無論是所謂公務機關或是非公務機關，規定都過於寬鬆，未能提供個人對其個人資

料充分的自主控制權。因此，在當前國家和許多私人企業正對方興未艾的生物特徵辨識技術投以關愛的眼神之際，我們有必要比較研究各國對生物特徵辨識技術帶來的衝擊，以及各國所採取的因應之道，除了分析台灣的法制現況之外，並應以考慮未來生物特徵辨識技術應用於我國可能產生的長遠影響，以及應有的政策方向，做爲討論重點。

我國先前曾換發身分證強制錄存指紋事件引起各界對於生物辨識議題的熱烈探討，並經司法院作成釋字第 603 號解釋，然而，即使如此，目前相關政府機關對於生物特徵辨識技術的採用企圖和作法，並未因爲釋字 603 號解釋的出現而減緩。

在我國政府積極採用生物特徵辨識技術之時，國際間各國政府也開始考慮生物特徵辨識技術的應用可能性。著名的事例包括美國在 911 事件後制定「2002 年美國強化邊境安全及簽證改革法」，要求目前不需簽證即可入境之國家，必須將該國國民護照改成含有生物辨識功能且機器可讀取的護照，否則將須申請簽證。國際民航組織（International Civil Aviation Organization，簡稱 ICAO）也在美國的壓力之下，研擬包含生物特徵資訊的新護照要求。另外，依據歐盟一九九五年「個人資料保護指令」（95/46/EC）第 29 條成立之「歐盟資料保護工作小組」，在二○○三年八月一日公布了「生物辨識工作文件」，該文件對於生物辨識特徵資料的應用所應注意的重點，也做了相當詳盡的分析和論述。同時，除了國境管理層面的運用之外，許多國家也計畫甚至已經將生物特徵辨識技術與傳統的辨識國民身分的方式結合，也就是將生物特徵資訊納入國民身分證明文件之中，將生物特徵資訊應用於國民身分的辨識。同時也有國家開始使用生物特徵辨識技術在社會福利的申請審核上，以增加社會福利分配的效率，避免申請者重複領取社會福利。由此可見，利用生物特徵進行身分辨識的技術和制度所引發的種種影響，已經是頗受國際社群重視而無從規避的議題。

國內晶片護照擬議的濫觴，和聯合國國際民航組織 ICAO 的倡議和要求具有密切的關係。該組織目前全體一百八十八個會員國，都已經同意在二○一○年四月一日起，全面使用機器可判讀護照（machine readable passport，簡稱 MRP），以因應全球化時代旅行通關所衍生的通關和身分驗證等需求。所謂晶片護照，顧名思義，便是在護照內加上電腦晶片，利用此一晶片記錄護照持照人的指紋、掌紋、臉部或眼球虹膜等個人特有的生物特徵經掃描後轉化與分析出來的數據資料。從過去數年來的發展來看，一般人普遍認爲這種生物特徵辨識系統是以每個人獨特的生物特徵來辨識身分，替代或僞造的難度都相當高，因此也就逐漸被應用在查緝非法移民、非法外籍勞工以及對抗恐怖組織犯罪等用途上。對於我國民航主管機關民航局和外交部而言，我國雖然不是聯合國國際民航組織的會員國，但是也決定基於和國際接軌的考量，配合國際民航組織規定發行晶片護照，並且針對現有的機場安檢和通關設備做必要的更新。至於晶片護照目前在各國實際運用方式，美國因爲反恐之故，和晶片護照的倡議關係緊密，固不待言，在亞太國家當中，馬來西亞、新加坡和香港等國均陸續進行晶片護照的推行工作當中，在歐洲國家方面，英國處在立法階段，德國和法國也各有進度。

在我國面臨此波運用生物特徵技術辨識身分的「國際潮流」的同時，對於各國的實務運作及相關爭論，進行研究與分析，以做爲我國未來研析生物特徵辨識技術運用可行性之參考，應具有其必要性。換言之，本計畫將以蒐集、分析和比較各國運用生物特徵辨識技術之制度與法規範，以及相關爭議問題之發展做爲主要目標，就我國生物特徵辨識身分之現況與問題分析、各國生物特徵技術運用之作法與規範及未來該技術應用於我國之政策建議等層面，進行研究，期能提出具體之政策建議。

貳、研究方法及過程

本研究採取文獻分析和他國經驗比較研究的方法進行。本計畫第一部分著重於文獻資料之蒐集及彙整，包括蒐集及彙整國際上和生物特徵辨識技術與制度有關之社會與管制變遷文獻，以及和生物特徵辨識技術與制度的政策及規範相關的學術論文、政府文件和實務見解。

第二部分著重在針對生物特徵辨識身分技術與制度所引發之規範與政策意涵分析研究，以及針對國際甚群針對此一議題所做的辯論和決策進行觀察，以瞭解全球化趨勢在生物特徵辨識科技與制度此一議題上所形成的共識和其實際限制所在。

第三部分著重於比較分析和政策建議的工作，本研究計畫在此一部分將研究國際社群發展趨勢所得，回饋於國內相關規範和政策的研究上，以期上述兩部分的研究，對於國內相關法制之建構有所啓發，進而尋找出對於現狀的改善之道。

參、重要發現和主要建議意見

一、生物特徵身分辨識科技發展趨勢潛藏的意義

生物特徵身分辨識技術，其精確度究竟有多高，安全性又是如何，同等科技水準的生物特徵身分辨識技術，在遇上不同的社會脈絡和不同的政府資訊安全防護文化時，究竟是否適合特定社會或政府立即採納，做爲身分辨識制度中所仰賴的主要工具，似乎應該是個可以受到質疑和討論的議題。

尤其，當絕大部分的民眾並不清楚政府即將全面核發晶片護照一事的詳細內容，對於何種技術將被運用於晶片護照內也所知不多的情況下，晶片護照內所使用的技術，例如 RFID 及生物特徵身分辨識技術，會使個人的資訊隱私權減損到何種程度，更是一個應該被公開討論、徹底辯論的議題。更重要的是，政府有義務使其公民充分知悉和

理解這樣一個有可能會影響其憲法所保障的公民自由權及內在自由的政府科技使用的發展趨勢。

二、生物特徵身分辨識科技運用於公部門所涉及的規範問題

台灣一般大眾和所有對科技不熟悉的社會大眾一樣，對於所謂的生物特徵身分辨識科技，多半處於並未深入瞭解的階段，遑論對於利用生物特徵辨識科技做爲工私部門的身分辨識機制此一重大公共政策，在正反資訊和意見都充分提供的前提下，在理解生物特徵身分辨識機制所涉及的各種風險的前提下，做過任何廣泛且深入的討論，形成政策層面的共識。同時，即使生物特徵身分辨識機制是所謂的「重要國際潮流」之一，是和國際民航組織要求進行「國際接軌」的重要手段之一，相關立法措施是否合憲且合宜，政府各部門在安全性保障和隱私保護等各方面的周邊制度，是否適時建立，而且運作良好，也都是必須細究到底的潛在爭議。這些潛在爭議，不應該僅僅止於針對移民相關法令和護照條例等相關規定進行形式上的增補修正，取得形式上的法律授權爲已足，而是應該正視立法蒐集人民生物特徵資訊此種作法的正當性，以及正視其所帶來的規範意涵。

以英國生物辨識議題爲例，雖然不乏立法授權蒐集人民生物特徵資訊甚且製成身分證件的相關討論，例如關於身分證法、移民及難民法，以及反恐怖主義法相關的刑事立法，然而，其間所涉及的根本辯論，卻始終才是最受矚目的焦點，形式的立法本身，卻不見得是最受關注的重點。

目前英國就生物辨識的相關討論，多集中於身分證法案部分所牽涉的生物特徵資訊取得問題。首先，侵害隱私權而取得生物資料需符合特定公共利益爲前提，但在身分證法案當中所提出的公共利益諸如防止犯罪、減少不法工作、身分欺詐等公共利益，皆未能被證實可經由身分證之實行而達成。其次，由於蒐集個人生物資料將有侵犯隱私權的問題，故其是否符合歐洲人權公約第八條的要求，在公共利益的

要求下以符合比例原則的權衡標準，非過度的干涉個人權利即爲重點。故在此諸如大型資料庫的設立、諸多資料的蒐集等是否違反比例原則，則爲考慮重點。另由於強制取得身分證將爲階段性的實施，則在此是否會違反歐洲人權公約第十四條禁止差別待遇的規定，亦有疑問。第三，就資料庫的管理部分，涉及資料保護的問題，從資料的取得、內容、管理等皆須小心討論實施，尤其在資料的揭露部分，對生物資料此種敏感資料的使用揭露規定，是否已臻完善，目前在現行英國身分證法當中將有許多機關可在模糊的定義下取得資料的情況下，恐尚有進步空間。最後，就生物特徵身分辨識技術而言，由於該技術尚在發展當中，其可能會造成的錯誤該如何解決，其技術該限制在怎樣的程度才不會過度蒐集資料而違反比例原則等，皆爲問題所在。以上英國經驗，或許不無目前準備以形式上的立法來處理規範層面問題的我國，值得借鏡之處。

再就亞洲地區的國家來說，亞洲地區雖然不乏已經開始實施生物特徵身分辨識制度和內建生物特徵身分辨識資訊的晶片護照者，但是，今年年初菲律賓 A PASIG City 地方法院的法院判決，卻命令該國外交部(DFA, the Department of Foreign Affairs) 暫緩該國晶片護照計畫之實施，此案對司法權介入國家採行生物特徵身分辨識制度的可能性，多少帶來某些啓示，其後續發展值得我們持續觀察。

此外，德國反國際恐怖主義法關於生物辨識特徵在身分制度的運用之規範目的乃以列舉的方式形成所謂的嚴格的目的拘束〈Zweckbindung〉。而這亦與我國釋字六〇三號解釋，大法官之解釋意旨不謀而合。在釋字六〇三號解釋認爲，資訊隱私權爲不可或缺之基本權，受憲法第二十二條之保障，雖然憲法對隱私權之保障並非絕對，惟當法律對隱私權作出干預與侵犯時，必須符合憲法第二十三條之比例原則。也就是符合目的合憲性、手段適當性、手段必要性以及狹義比例原則。而本號解釋，大法官認爲戶籍法關於按奈指紋，否不予核發身份證之規定，首先目的不明確，就算縱用以達到國民身分證之防僞、防止冒領、冒用、辨識路倒病人、迷途失智者、無名屍體等目的

而言，亦屬損益失衡、手段過當，不符比例原則之要求。因此宣告戶籍法第八條二、三項違憲。就以目的合憲性而言，由於指紋涉及個人之隱私權，爲人格發展不可或缺之基本權，且亦涉及到此項隱私的資料如何用、如何管理以及是否會外洩等問題。因此若僅單單以按捺指紋換發身份證可達到辨識、冒用、預防犯罪等目的上，則不符目的之合憲性。因此大法官在此採取最嚴格之審查，而這與德國反恐法關於生物特徵辨識特徵在身份制度的運用之規範目的以列舉的方式形成所謂的嚴格的目的拘束不謀而合，道理即在此。

而在應採取嚴格的目的拘束有共識後，若臺灣未來希望建立一套生物特徵之資料庫，或是爲了防止恐怖份子而採用電子護照時，首先在立法背景以致法律規範目的上，亦應如同德國反恐法之規範目的，採取最嚴格之目的拘束，亦如同美國三重審查之嚴格審查要求目的必須與公益有重大之關係，才能採取侵犯人民隱私權之方式，去建立一套生物資料庫或是利用生物特徵作爲能入出境之方式。再者，釋字六〇三號解釋亦提及個人資料的管理方式。因爲若有正當之目的，惟沒有一套管理方式，將會導致資料被濫用，此亦與人權之保障有所違背。而在德國有所謂之資訊監察官，除了避免生物特徵遭外洩外，亦爲個人之隱私權提供了一套保護方式。而臺灣未來應可參考德國之立法例，成立維護生物特徵之資訊監察官，以防止生物特徵之濫用。

三、生物特徵身分辨識科技運用涉及的風險爭議和社會辯論

生物辨識身分制度所引發的社會風險具有多樣化、難預測的特性，不能一味倒向唯科學化、實證主義的生產的邏輯。這套生產的邏輯是以線性因果的思維認爲生物辨識的科技系統爲可控制性(可確實保密、儲存)、可彌補性(爲了治安犧牲一點人權也是值得)、與可回復性(即使資料外洩名譽仍可回復)。然而，由於生物辨識系統涉及龐大的資訊儲存、辨識、利用、流通與管理，在任何一個環節皆有高度的不確定性，並且一旦外洩所引發的風險後果是目前難估計，因此，建

議需謹慎評估，並以其他方式來取代運用，並進行替代性的風險評估(alternative assessment)，而非僅以本生物辨識科技系統爲唯一的風險評估標的，以免產生政策上一去不返的滑坡效應，換言之，科學風險評估與政府與人民間的風險溝通，皆不可偏廢。

一般民眾對於風險之認知，容易受到資訊流通、媒體報導之影響，形成瀑布效應(cascade effect)，或是對大災難特別有恐懼感，或僅基於過去之經驗或情感式的影響，以及直覺式的損益分析，這種直覺式的損益分析，對於是否應該對某種風險加以管制，有時只看到利益面，而低估危險面，故在媒體造成的知溝(knowledge gap)差距下，公眾對於治安風險的未來性較清晰，反對於生物辨識技術的風險較爲模糊，因而在利益與風險分析上傾向於利益面考量，這同時意味著公眾並沒有充分、良好的告知或學習判斷，對於隱私權、資料外洩、科技風險仍處於有待自我啓蒙的社會階段中。

尤其，民眾的風險感知也跟科學技術官僚散佈的資料證據息息相關，因爲經由二手傳播之非經驗所形成的公眾風險意識，事實上也必須從科學風險評估或決策者傳遞的資料訊息引證。而我國的技術官僚，長期以來習慣由上往下、威權式的、線性因果的實證確定性來推動各種科學計畫，以簡單化約、工具性的現代化、單面利益論述建構生物辨識系統的好處，而這些端倪也反映在移民署通關辨識與外交部的晶片護照上。

其實現行爭議性科技所衝擊的領域已逾越了既有的社會、法律、倫理的界限，傳統自然科學風險評估方式雖能夠提供一定的解決功能，但對於爭議性科技所引起在不同社會領域的衝擊與不確定性並無法提供答案，而這個部分所要進行開放式的社會風險評估，關鍵正在於公眾對於爭議性科技風險的理解與認知。不同的風險感知和溝通可成爲強化分析階段的來源，但不是一次就讓政策決定，應要調停不同的感知進入單一政策中，以便處理安全和偶發事件。新科技總是改變社會環境，帶來和引進新風險，而一連串的研究建議以漸進的努力去

順應科技的利益與緩和科技帶來的缺點，安全管理者必須抓到科技、政策和行爲三位一體的概念。

就以晶片護照、生物辨識系統而言，我們看到，在不同場合中相關管制機構的官員一再追隨與強調主流科學的辨識率效果，以及多少國家已採用的趨勢，在此論點下，單一的科學評估就成爲決策的唯一檢證標準，並難以接受其它科學異議的聲音。換言之，在狹隘性之科學實證性的風險評估哲學下，技術官僚憑藉著獨大的專家政治立場，壟斷性地排除社會、倫理風險，而相對性的認定科學爲唯一評估與溝通的基礎。因此，風險溝通變成單面向的、教育的、扭正社會「情感的或不理性的感知」。

此外，若以高科技需要高思維相應之風險社會公民理性溝通、批判能力之觀點，來檢視台灣民眾對生物辨識技術、晶片護照反應，不得不指出我國全球在地化風險該加油的地方，包括主管官署的不負責任，置民眾於資訊無知的狀態；但相對的我國公民社會仍相當脆弱，對應於此種全球性的高科技風險社會並無法建立監督、溝通並理性批判政府的行動，而這也是台灣欲發展人文高科技島的一項重要警訊與隱憂，更是我們值得共同努力的地方。

各國經常以立法來延宕科技風險的可能性，但在美國的生物辨識技術發展霸權與競爭放任之下，所有的社會風險的門檻紛紛失守。外交部、移民署等晶片護照與生物辨識機器的購買，類此涉及人民重大權利、義務的事項，政府應慎思明辨、決策應保守而謹慎，實不宜在未經國會充分討論、生物辨識科技法源尚在未定之天、及有公民審議程序、聽證程序、公民諮詢與公民會議等公共討論，經過多次且多元廣泛的風險溝通後，達到社會共識時，就動輒撒下龐大資金，讓備受爭議的新制上路，這樣的決策未免過於草率，欠缺謀定而後動的智慧，萬一生物辨識技術有違憲的爭議，在立法程序無法過關，那麼購置的設備豈不是浪費公帑？故從本旨研究建議，不應該在反恐的大論述底

下，就冒然實施生物辨識技術、晶片護照等政策，否則將產生風險不可回復的後果。

其次，生物特徵身分辨識科技的應用和晶片護照的出現，無非是國家理性主導一切的近代社會的典型面貌。然而，思考這種監控社會統治體制下的 social sorting（社會性分類）將帶來何種風險，卻是值得目前積極考量採行這些措施做爲政府重大施政計畫的我國政府深入理解的。以英國爲例，到了二○一○年每位申請護照之英國國民皆會強制同時發放身分證件。但在政府不斷保證該計畫爲切合時代潮流且能提升公共安全的同時，諸多反對質疑意見仍然不斷，其對於隱私權及相關人權可能產生的侵害、可能發展爲監控國家的疑慮、甚至在技術上是否能真正實行、是否會造成花費龐大但效用不彰的情況等，皆造成英國社會，甚至政府官員、國會成員對於此項生物技術應用持保留態度，反對黨甚至明確表示一旦於下次大選勝利即會停止該身分證計畫的推行，目前英國這樣的道路是走向國家安全提升的康莊大道，或者走向監控社會隱私受限的警察國家，恐怕仍是未知之數。

再以反恐主導者美國爲例，在 911 恐怖攻擊事件後，爲了讓美國公民確信美國政府正盡力採取所有可能的方法，確保美國人民的安全，也爲了便利旅行及協助邊境執法人員判斷文件的有效性，美國政府要求所有與美國相互享有免簽證入境的國家（VWP countries），應該發展一套更安全的晶片護照系統，而負責核發美國護照的美國國務院，也基於互惠原則，發行晶片護照。美國的晶片護照除了涵蓋 1998 年版護照（Passport ’98）既有的資訊外，同時包含以數位相片方式展現的生物辨識碼（biometric identifier）。護照的封底還嵌入一個 RFID 晶片。值得我們思考的問題是：發行晶片護照的政策，到底隱含哪些我們應該正視的風險和社會辯論？當這些技術基於政府的要求而被用於一套全國性的身分辨識系統時，持有護照的一般公眾，其實根本失去了選擇他們想要持有何種護照的權利，他們變成只能選擇要或不要持新的晶片護照於美國以外的地域旅行。而晶片護照則很可能會成爲

追蹤公民穿越各國機場及跨越各國邊境的工具。這是一種喬治歐維爾式的憂慮：公民將會無時無刻地受到來自於國家的監視與追蹤。

雖然憲法所保障的隱私權、財產權和旅行權等並非絕對的權利，然而，晶片護照的發行及使用，所涉及根本的價值問題很可能在於：我們的社會把守法的公民都視爲潛在的恐怖份子，但卻未盡力地有效保護他們免於受到真正的威脅。同時，在適當安全防護措施尚未到位的情形下就發行晶片護照，很可能會對一般人科技警覺性不高的人，帶來一場科技上的災難。尤其，當護照上的資訊在每次被讀取時，都必須先下載到資料庫內，但政府卻無法保護外國政府資料庫內的我國公民的資訊時，也無從如歐盟的隱私權保護指令爲跨國的個人資料流動提供一套比較有效的管制架構時，持有晶片護照的人民，能夠受到何種程度的資訊隱私保障，其實是很值得懷疑的。

晶片護照的另一個主要弱點，不在於生物特徵身分辨識科技本身，而是在於可以接近使用晶片護照資訊的人。護照的核發審核者、邊境管制人員、執法單位及私人單位將會有管道接近這些個人資訊。相關的管制及防護措施應該要到位，才能確保護照的核發機關不致於在發照時就出錯，或是將護照發給潛在的恐怖份子，或是忽略了身分冒用者使用有效的文件來蒙混過關。此等弱點並不是新出現的，他們原本就存在，但若邊境管制人員及執法部門在決定一個人的真實身分時，過份仰賴科技，將無法篩選出真正的身分冒用者。相關的執法人員應該接受訓練，才能學會不要單純依靠電腦系統來決定文件的是否有效及進行身分辨識。護照的核發審核者在時間的壓力下，仍需要花更多的時間來挑出可能涉及身分僞造的因素，否則護照可能會錯誤地核發。如果要避免安全且有效的文件被發給恐怖份子，例如九一一事件中發給劫機者十九份美國簽證的問題，就必須要求相關執法者不全然仰賴科技來追求準確性，才能解決。

或許，究其實際，晶片護照從一開始就是一種無法避免人民

遭受未來的恐怖攻擊的脆弱文件。或許九一一事件爲世人帶來的震撼程度，促使各國政府迅速且不理性地採取各種極端的行動，晶片護照的推出，或許便是在這種歷史潮流下的產物。我們或許應該回到生物特徵身分辨識機制的根本面，思考一下晶片護照是不是根本便是一場巨大而無聲的滑坡效應的開端而已？不久的將來，各種政府是不是會把生物特徵身分辨識技術和 RFID 技術運用於駕照和國民身分證件上呢？在那一天來到之前，我們做過資訊充分而徹底的辯論了嗎？理解了生物特徵身分辨識技術及其相關配套技術的倫理、規範和社會意涵了嗎？

四、科技應用的風險評估

在我國廣泛運用生物特徵做爲身份辨識科技之前，應該落實相關科技的風險評估工作。確實的風險評估與溝通不僅只有科學面，還包含社會、法律、文化等面向，因此對於此種爭議性科技於其所產生不確定性的問題，除了要進行多元領域之自然科學風險評估與溝通之外，也應進行開放性、社會科學式的風險評估。這裏所主張開放性、社會科學式的風險評估，著眼於除了依據傳統自然科學式的風險評估之外，當代許多高度爭議的科技問題，必須增加自然科學領域之外的評估，也就是說，當爭議性的科學發展已經逾越了傳統的解決問題範疇、界限，科學的衝擊除了自身安全的不確定性外，往往也衝擊到了現行法律、倫理、社會的基礎，因此，風險評估的範疇與定義必須開放性的納入有關對這些社會領域的評估，來增進科學發展的正當性。

也就是在開放性風險評估典範下，對於科技爭議與不確定性部份的評估超越了單一領域自然科學式風險評估的限制，而在整體多元的評估過程中進行公共領域的學習、溝通與價值判斷，由社會公眾對科學爭議進行雙向式的理解與溝通判斷，在多元領域與價值的思考、批判下，逐步建構出社會對於不同高科技風險爭議的處理能耐，而發展出整體風險評估的治理策略。

關鍵詞：生物特徵、身分辨識、人權保障、科技風險評估、比較法與比較制度

運用生物特徵辨識身分制度之比較研究

XX

第一章　緒論

本章爲本研究之緒論，主要內容爲說明本研究計畫之研究緣起和研究背景、研究方法、章節安排、研究結論與預期效益等。

壹、研究緣起

所謂的安全生物辨識技術（technologies of biometrics），是指利用生物辨識特徵（biometric indicator）去辨識身分的技術，至於所謂的生物辨識特徵，則是指任何可以用來辨識身分之用，並可被測量或使用的人類身體或生物特徵，包括臉貌、指紋、手掌紋、視網膜、聲音（語音）、體形等，因此，相應的生物特徵辨識技術，通常便有臉部識別、指紋識別、掌紋識別、虹膜識別、體形識別和簽字識別等。透過生物辨識技術的運用，可以作爲比對個人身分，進而得知個人出入的場所、活動的範圍等，這些活動原本均是涉及個人領域的活動，所以此等生物特徵辨識技術的運用，不免引發和個人資料保護及隱私權有關的爭辯。

這些對生物特徵辨識技術的應用，顯示科技的發展，已經激起政府使用生物特徵辨識技術的高度興趣。但是這種新技術的使用，難免對人民的隱私權產生另一波的衝擊。因此，各國莫不著手研擬保護個人資訊的新方式，有的國家選擇針對生物特徵辨識技術，另行訂立法律，有的國家則是在既有的個人資訊保護體制上，透過解釋的方式，因應新科技可能帶來的威脅。前者例如美國某些州的生物特徵法，後者最爲著名者則爲依據歐盟 1995 年「個人資料保護指令」（95/46/EC）第 29 條成立之「歐盟資料保護工作小組」於 2003 年 8 月 1 日公布了「生物辨識工作文件」,其中對於生物辨識特徵資料之應用所應注意的

重點，也多所著墨。

反觀國內，對個人資訊普遍性的保護，來自電腦處理個人資料保護法的相關規定，但是，該法是制訂公布於 1995 年，當時生物特徵辨識技術尚未能普及應用，且該法對於個人資料的使用，無論是所謂公務機關或是非公務機關，規定都過於寬鬆，未能提供個人對其個人資料充分的自主控制權。因此，在當前國家和許多私人企業正對方興未艾的生物特徵辨識技術投以關愛的眼神之際，我們有必要比較研究各國對生物特徵辨識技術帶來的衝擊，以及各國所採取的因應之道，除了分析台灣的法制現況之外，並應以考慮未來生物特徵辨識技術應用於我國可能產生的長遠影響，以及應有的政策方向，做爲討論重點。

我國先前曾換發身分證強制錄存指紋事件引起各界對於生物辨識議題的熱烈探討，並經司法院作成釋字第 603 號解釋，然而，即使如此，根據媒體報導，外交部正積極著手研擬我國護照發展計畫草案，規劃推動我國護照以臉部影像和指紋等生物特徵做爲辨識特徵，此一草案同時亦將在護照條例修正草案的立法過程當中，處理法律授權的問題。[1]根據行政院送交立法院審議的護照條例修正草案，除了在修正條文第三條中明訂護照係中華民國國民在國外旅行所使用之國籍身分證明文件之外，並於修正條文第八條中，配合晶片護照的發展，增訂護照記載事項及得將其內容及持照人照片之影像，存入護照內植晶片之規定，並且刪除現行條文第十四條有關護照加簽及修正之規定，以避免未來護照晶片內儲存資料與記載事項不一致之情形發生。其次，同樣地，根據媒體報導，雖然相關立法授權狀態未明，移民署成立之後，亦決定未來無論是短期入境觀光，大陸配偶來臺長期居留，在入境通關之時，均須接受「按捺指紋、拍攝臉型、掃瞄虹膜」的三合一查驗身分政策。並且已經購置生物特徵辨識系統，將在相關授權法令

[1] 參見如：「電子護照 2010 年上路」，自由時報，94 年 7 月 13 日。

正式通過之後，分配在各個機場海關，做爲通關控制之用。[2]從我國現行法令內容來看，《兩岸人民關係條例》第十條之一規定「大陸地區人民申請進入臺灣地區團聚、居留或定居者，應接受面談、按捺。指紋並建檔管理之；未接受面談、按捺指紋者，不予許可其團聚、居留或定居之申請。其管理辦法，由主管機關定之」，此一規定可以說是在國境上蒐集生物特徵的主要依據，而這個規定，似乎也就成了我國目前蒐集生物特徵的濫觴，和上述媒體所報導之生物特徵蒐集規劃，似乎難脫關係。而針對上述媒體所報導的措施內容，相關部會雖然偶有駁斥之處，[3]強調其僅將採取「不具侵犯性」的「臉部特徵辨識」科技[4]，然而，從相關政府部會有限而零星的公開回應內容中，實在留下不少讓人頗難理解的問題。例如：如果是僅採取臉部特徵辨識的作法，移民署爲何決定購買昂貴的三合一生物特徵辨識系統？是否後續仍有進一步的措施，早在相關部會的醞釀之中？由於相關部會至今並未遵循「政府資訊公開法」的基本精神和相關要求，針對生物特徵相關措施徹底公開任何有效的資訊，所以，類似疑問不斷出現，恐非難以預見之事。而無論上述質疑的解答爲何，目前相關政府機關對於生物特徵辨識技術的採用企圖和作法，並未因爲釋字 603 號解釋的出現而減緩，則應該是無須爭執的事實。

在我國政府積極採用生物特徵辨識技術之時，在國際間各國政府也開始考慮生物特徵辨識技術的應用可能性。著名的事例包括美國在 911 事件後制定「2002 年美國強化邊境安全及簽證改革法」，要求目前不需簽證即可入境之國家，必須將該國國民護照改成含有生物辨識功能且機器可讀取的護照，否則將須申請簽證。國際民航組織

[2] 參見如：「晶片護照快易通?爭議多惹民怨」，中國時報，2007 年 1 月 15 日。

[3] 參見如：「機場生物辨識，七月啓用」，聯合報，96 年 4 月 19 日。移民署官員何榮村在接受媒體採訪時表示即便已購買三合一生物特徵查驗機器，現在及未來將不會採指紋及虹膜，僅取臉型。

[4] 但請參見本報告附錄四、附錄五、附錄七之內容，亦即由陸委會、外交部、內政部入出國及移民署所提出的意見。

（International Civil Aviation Organization，簡稱 ICAO）也在美國的壓力之下，研擬包含生物特徵資訊的新護照要求。另外，依據歐盟一九九五年「個人資料保護指令」（95/46/EC）第 29 條成立之「歐盟資料保護工作小組」，在二○○三年八月一日公布了「生物辨識工作文件」，該文件對於生物辨識特徵資料的應用所應注意的重點，也做了相當詳盡的分析和論述。同時，除了國境管理層面的運用之外，許多國家也計畫甚至已經將生物特徵辨識技術與傳統的辨識國民身分的方式結合，也就是將生物特徵資訊納入國民身分證明文件之中，將生物特徵資訊應用於國民身分的辨識。同時也有國家開始使用生物特徵辨識技術在社會福利的申請審核上，以增加社會福利分配的效率，避免申請者重複領取社會福利。由此可見，利用生物特徵進行身分辨識的技術和制度所引發的種種影響，已經是頗受國際社群重視而無從規避的議題。

國內晶片護照擬議的濫觴，和聯合國國際民航組織 ICAO 的倡議和要求具有密切的關係。該組織目前全體一百八十八個會員國，都已經同意在二○一○年四月一日起，全面使用機器可判讀護照（machine readable passport，簡稱 MRP），以因應全球化時代旅行通關所衍生的通關和身分驗證等需求。簡言之，根據 ICAO 的說法，各國同意配合採用 MRP 護照的結果，對於未來通關手續的簡化以及民航作業安全性的提升這些該組織所追求的全球化目標，具有相當。截至二○○六年的年初為止，已經有一百一十多個國家採用 MRP 護照，而且，其中有四十餘國，計畫二○○六年底之前，在護照上加裝電腦晶片，以便增加生物特徵辨識功能。至於在用途方面，未來 MRP 護照將會普遍使用於遍布於全世界的大使館、領事館、安全檢查、移民事務和海關檢查站等處，使得辦理旅行簽證和通關都因此變得更為便利。

對於我國民航主管機關民航局和外交部而言，我國雖然不是聯合國國際民航組織的會員國，但是也決定基於和國際接軌的考量，配合國際民航組織規定發行晶片護照，並且針對現有的機場安檢和通關設

備做必要的更新。

所謂晶片護照，顧名思義，便是在護照內加上電腦晶片，利用此一晶片記錄護照持照人的指紋、掌紋、臉部或眼球虹膜等個人特有的生物特徵經掃描後轉化與分析出來的數據資料。從過去數年來的發展來看，一般人普遍認爲這種生物特徵辨識系統是以每個人獨特的生物特徵來辨識身分，替代或僞造的難度都相當高，因此也就逐漸被應用在查緝非法移民、非法外籍勞工以及對抗恐怖組織犯罪等用途上。

至於晶片護照目前在各國實際運用方式，美國因爲反恐之故，和晶片護照的倡議關係緊密，固不待言，在亞太國家當中，馬來西亞、新加坡和香港等國均陸續進行晶片護照的推行工作當中，在歐洲國家方面，英國處在立法階段，德國和法國也各有進度。

詳言之，新加坡出入境通關管理局（The Immigration and Checkpoints Authority, ICA）在 2006 年 8 月 15 日推出新加坡生物特徵護照(BioPass)，因此可以讓新加坡繼續保有美國簽證豁免計劃（Visa Waiver Program, 簡稱 VWP）[5]的地位，亦即使新加坡生物特徵護照持有人繼續享有 90 日美國豁免簽證的權利。在香港方面，香港入出境事務處從 2007 年 2 月 5 日起，開使簽發生物特徵特區電子護照(HKSAR e-Passport)，該電子護照的封面設計與以往的香港護照相較之下，並無太多不同之處，但卻加入了電子晶片以及其他四十六種防僞功能，該護照內建非接觸式晶片，用以儲存了個人相片及資料。在法國方面，法國政府的計劃是從 2005 年起開始推動生物特徵護照計劃，護照內存有指紋以及臉部特徵資料，至於虹膜此一生物特徵，也規劃其日後也將成爲晶片護照所儲存的資料，從 2006 年起開始簽發此一新型晶片護

[5] 目前參與美國 VWP 計畫的國家總計有二十七個國家，這 27 個國家的國民可享有 90 日豁免簽證，條件是 2005 年 10 月 26 日之前這 27 國必需完成生物特徵護照的建置。這 27 國分別是，安道爾、冰島、挪威、澳洲、愛爾蘭、葡萄牙、西班牙、奧地利、義大利、新加坡、日本、比利時、婆羅乃、聖馬利諾、列支敦士登、斯洛文尼亞、丹麥、盧森堡、瑞典、芬蘭、摩納哥、法國、荷蘭、瑞士、德國、紐西蘭與英國。

照。在德國方面，德國政府的晶片護照計畫，主要是與 Royal Philips Electronics、Infineon Technologies AG 這兩家公司合作，於 2005 年 11 月起簽發此一新的生物特徵護照，德國的晶片護照內建儲存個人資訊及照片的晶片。

根據媒體報導，除了對本國人民簽發內建儲存個人資料晶片的晶片護照之外，因應外籍移住民和開放大陸觀光客的政策，移民署也準備以生物特徵做爲身分辨識的依據。換言之，雖然目前根據兩岸人民關係條例第十條之一的規定，僅限於大陸地區人民來台團聚、居留或定居者，應按捺指紋並建檔管理，然而，未來在大陸人士或其他外籍移住民入境時，極可能都必須現場按指紋、攝取臉部影像和掃瞄虹膜等，進行比對，若比對率過低，電腦系統將提醒移民官加強查驗證照和其他身分驗證的工作。[6]此種藉助生物特徵身分辨識系統所進行的入出境查驗程序，其目的不外乎提高查察利用改名和假冒身分方式從事偷渡、非法打工、逾期停留及其他不當或不法目的之行爲的效率。對照當今世界各國利用生物特徵技術辨識身分的發展情況，近年來固然出現生物特徵逐漸導入海關查驗或結合護照核發的流程中，但是，針對外國人或者移住民使用生物特徵辨識系統者，大部分與恐怖攻擊的後續效應脫離不了關係，美國及歐盟便可以說是最典型的實例。

在我國面臨此波運用生物特徵技術辨識身分的「國際潮流」的同時，對於各國的實務運作及相關爭論，進行研究與分析，以做爲我國未來研析生物特徵辨識技術運用可行性之參考，應具有其必要性。換言之，本計畫將以蒐集、分析和比較各國運用生物特徵辨識技術之制度與法規範，以及相關爭議問題之發展做爲主要目標，就我國生物特徵辨識身分之現況與問題分析、各國生物特徵技術運用之作法與規範及未來該技術應用於我國之政策建議等層面，進行研究，期能提出具體之政策建議。

---

[6] 同前註二。

綜合以上所述可知，本研究計畫的研究主題，偏重於是運用生物特徵辨識身分制度的比較研究。本研究希望可以比較各國運用生物特徵辨識身分的制度，檢討在何種特定目的下，國家或私人機構得以蒐集個人的生物特徵資訊、蒐集的範圍爲何，以及這些生物特徵資訊的保存、使用與揭露等，這些與個人資訊保護相關的制度設計。透過這些比較分析，可以進一步了解目前各國應用生物特徵資訊的方式和用以保護個人資訊的法制，這些分析，將有助於我國擬訂將來應用生物特徵辨識技術的政策方向。

本研究預期的目標，首先除了要檢視分析目前關於生物特徵辨識制度的國際發展趨勢之外，也希望檢討我國運用生物特徵辨識身分之現況，包括警察職權行使法、移民相關法規、和 2005 年 9 月 1 日開始施行的大陸地區人民按捺指紋等規定，同時，針對其他現存的指紋資料庫，以及依據去氧核醣核酸採樣條例所建置的 DNA 資料庫等，也將在適當的行文脈絡下加以分析。希望透過對這些現存制度的分析，了解我國現行法制和實務運作所涉及的個人生物特徵資訊保護。

接著，本研究希望比較各國運用生物特徵辨識身分的作法與規範，包括各國使用生物特徵辨識技術的緣起，相關的法規範，以及運用此等技術與制度的成本分析，以便收「他山之石，可以攻錯」的效果。換言之，本計畫認爲其他國家目前所累積起來的經驗，或許可以對我國將來的政策決定有所啓發，同時，在瞭解他國生物特徵辨識技術的實施經驗之後，也可以儘量避免決策於未然可能產生的風險。

最後，本研究計畫希望可以提出生物辨識技術未來應用於我國的政策建議。在檢討我國應用生物辨識技術的現況和比較外國的應用經驗之後，本研究希望可以提出一系列具體且具有可行性的政策建議，作爲將來政府使用生物辨識技術的參考。

貳、相關研究檢討

如前所述，許多政府對於生物特徵辨識技術抱持著濃厚的興趣，我國亦無例外。而國內除了已經建立犯罪嫌疑人指紋資料庫、役男指紋資料庫之外，也有部分犯罪嫌疑人和加害人的 DNA 資料庫。在大法官宣告戶籍法強制全民按捺指紋的規定違憲之後，政府卻在同年開始實施臺灣地區與大陸地區人民關係條例第十條之一的規定，要求申請來台團聚、居留或定居的大陸人民必須接受指紋的錄存，並且通過大陸地區人民按捺指紋及建檔管理辦法，處理這些大陸地區人民的指紋資料。此外，法務部建議大陸觀光客來台也要按捺指紋。可見雖然釋字 603 號解釋使得政府蒐集全民指紋的計畫暫時受挫，但是政府對於生物特徵辨識技術的運用前景依然看好。

國內對於生物特徵辨識身分相關的研究，除了王郁琦在交通大學出版的全國科技法律研討會有發表過「生物辨識技術對隱私權的影響」一文之外[7]，大多數的研究都是與釋字 603 號解釋相關。例如該號解釋作成前四位鑑定人黃昭元、李建良[8]、顏厥安[9]和徐正戎[10]四位教授的鑑定意見書，以及其他與戶籍法相關的文章，包括詹鎮榮教授的「請領國民身分證，先捺指紋」[11]；李仁淼教授的「再論強制按捺指紋之合憲性」[12]；范姜真媺教授的「按捺指紋與合憲性審查標準－以日本判例、學說爲主」。[13]至於討論強制按捺指紋議題的學位論文，則有熊德

[7] 王郁琦，生物辨識技術對隱私權的影響，收於劉尚志主編，全國科技法律研討會論文集 2005 年，國立交通大學出版，頁 287-317。

[8] 李建良，「戶籍法第八條捺指紋規定」釋憲案鑑定意見書，臺灣本土法學雜誌 73 期，2005 年 8 月，頁 38-56。

[9] 顏厥安，戶籍法八條與全民指紋建檔合憲性問題之鑑定意見，臺灣本土法學雜誌 79 期，2006 年 2 月，頁 145-177。

[10] 徐正戎，「戶籍法第八條捺指紋規定」釋憲案鑑定意見書，臺灣本土法學雜誌 75 期，2005 年 10 月，頁 57-81。

[11] 詹鎮榮，請領國民身分證，先捺指紋，月旦法學教室，2005 年 7 月，頁 8-9。

[12] 李仁淼，再論強制按捺指紋之合憲性，月旦法學教室，2005 年 8 月，頁 8-9。

[13] 范姜真媺，按捺指紋與合憲性審查標準－以日本判例、學說爲主，律師雜誌，

仁的論文，題爲「論全民指紋制度之合憲性問題」，此爲中央警察大學法律學研究所之碩士論文。[14]在大法官解釋作成之後，也有李震山教授和李惠宗教授分別在期刊雜誌發表評論文章。李震山教授分析強制按捺指紋涉及的憲法基本權利類型，他認爲強制按捺指紋涉及的權利範圍有小到大分別爲資訊自決權、隱私權、一般人格權最後則是由人性尊嚴作爲最上位的補充概念。戶籍法的規定，他認爲應該以資訊自決權作爲討論的基調。此外李震山教授的這篇文章也提及資訊權的建構，資訊權的內涵包括積極向國家請求資訊的知的權利，以及要求國家保障個人的資訊隱私權或資訊自決權。[15]

李惠宗教授的「領取國民身分證按捺指紋違憲性之探討—從法學方法論評大法官釋字第六○三號解釋」一文，則是從法學方法論評析聲請案是否應該受理、探討人性尊嚴在違憲審查規範上扮演的功能、國民身分證與指紋之間不當連結的問題、國民身分證的性質與其在社會生活中所能扮演的功能、法律保留原則與法律明確性原則在本案中的應用以及大法官審理該案件的程序，包括要求相關機關盡舉證責任、不處理相關機關否認的立法目的等，對大法官作出解釋的方法和適用的憲法原則做出分析檢討。16顏厥安教授和李建良教授，也都分別公開發表了針對戶籍法第八條所引發的指紋釋憲案而寫作的鑑定意見書。

此外，林燦都與傅美惠教授也在釋字 603 號解釋公佈之後，發表「按捺指紋措施之合憲性問題探討」這篇文章除了介紹美國日本的相關制度之外，作者解析強制按捺指紋與人民資訊自決權的關係，並且

2005 年 8 月，頁 54-71。

[14] 熊德仁，論全民指紋制度之合憲性問題，中央警察大學法律學研究所 91 學年度碩士論文。

[15] 李震山，來者猶可追，正視個人資料保護問題－司法院大法官釋字第六○三號解釋評析，臺灣本土法學雜誌 76 期，2005 年 11 月，頁 222-234。

[16] 李惠宗，領取國民身份證按捺指紋違憲性之探討－從法學方法論評大法官釋字第六○三號解釋，月旦法學雜誌 126 期，2005 年 11 月，頁 172-186。

討論按捺指紋的合憲性問題。[17]

至於生物辨識技術國外的相關研究，除了上述「歐盟資料保護工作小組」於 2003 年 8 月 1 日公布的「生物辨識工作文件」之外，國際民航組織也在 2004 年公布關於在機器可以辨讀的護照中使用生物特徵資訊的報告。歐盟資料保護工作小組的文件主要是描述生物特徵辨識技術，以及分析個人生物特徵資訊如何適用歐盟的個人資料保護指令。該份文件認爲大部分的生物特徵資訊屬於個人資訊，因此對於這些個人資訊的處理，必須遵守歐盟個人資料保護指令的規定。尤其是必須考量生物特徵資訊可以在資訊主體不知情的情形下被蒐集，和生物特徵資訊與個人的緊密連結特性。國際民航組織的報告則著重在於比較各個生物特徵資訊的相容性，以衡量適合用於旅行證件的生物特徵資訊。

當然，在這些國際組織的研究之外，許多國家也對生物特徵辨識技術的應用問題展開詳盡的研究。舉例而言，澳洲的聯邦隱私委員在 2002 年發表一份報告，分析檢討生物特徵辨識技術的使用。加拿大安大略省的隱私委員也在 1999 年發表關於隱私權和生物特徵的文件。這份文件分析生物特徵辨識技術對隱私權可能產生的威脅，並且對於多倫多市計畫在社會福利事項上使用生物特徵辨識技術提出一些具體建議。

再者，英國倫敦政經學院在 2005 年的 6 月以英國的身分證法爲對象，作出一份鉅細靡遺的報告。其中有一部份檢討英國的身分證法對於生物特徵資訊的相關規定，和比較世界各國辨識身分的制度。美國聯邦政府的審計總署（General Accounting Office），在 2002 年之際也針對生物特徵辨識技術在國境管理上的使用，提出一份技術評估，該份報告衡量各種將生物特徵使用於邊境管制的模型，並進行成本效益

[17] 林燦都、傅美惠，按捺指紋措施之合憲性問題探討，法令月刊 56 卷 10 期，頁 12-32。

的分析。

整體而言，以上所述之國內研究，多半是僅僅鎖定特定類型的生物特徵辨識技術和相關法律爭議做爲討論分析的重點，至於各國的制度發展、相關研究分析、乃至於因而引發的社會辯論，國內尚無有系統的研究出現，這也是本研究計畫要進一步著力之處。

參、我國目前研議中的生物特徵身分辨識制度可能引發的爭議

平心而論，臉部辨識並不是太新的技術，而臉部辨識技術的缺陷也不斷被提出來討論，所以，移民署準備設置的臉部辨識系統，是不是有效的身分辨識方式，或許是應該深入討論的重點之一。電腦辨識以 3D 技術爲臉部測點，雖然一般認爲誤差率低，但是，此種技術還是會受到環境、裝扮與長相改變等因素影響，則也是不爭的事實。因此，用臉部辨識技術來處理護照真僞查驗的問題，其實可靠性不高，護照防僞如何設計，以及如何確定護照持有人和護照上的個人資料具有同一性，而不是將照片或臉部辨識技術這種應屬護照查驗中的輔助項目當做重點，或許才是癥結所在。同樣地，臉部辨識技術之外的其他生物特徵身分辨識技術，其精確度究竟有多高，安全性又是如何，究竟是否適合做爲身分辨識制度中所仰賴的主要工具，似乎也不盡然是不應該受到質疑的對象。

其次，台灣一般大眾和所有對科技不熟悉的社會大眾一樣，對於所謂的生物特徵身分辨識科技，多半處於並未深入瞭解的階段，遑論對於利用生物特徵辨識科技做爲工私部門的身分辨識機制此一重大公共政策，在正反資訊和意見都充分提供的前提下，在理解生物特徵身分辨識機制所涉及的各種風險的前提下，做過任何廣泛且深入的討論，形成政策層面的共識。同時，即使生物特徵身分辨識機制是所謂

的「重要國際潮流」之一，是和國際民航組織要求進行「國際接軌」的重要手段之一，相關立法措施是否合憲且合宜，政府各部門在安全性保障和隱私保護等各方面的周邊制度，是否適時建立，而且運作良好，也都是必須一一細究的潛在爭議。

舉例來說，美國政府於 2005 年 12 月 30 開始核發晶片護照（先針對外交人員和某些政府官員發放的護照）之後，民權團體（如 ACLU）消費者團體以及一些公眾意見，均提出不相信晶片護照如美國政府所宣稱般地安全的看法，換言之，關於晶片護照所涉及的隱私權保障和安全性的爭議，逐漸成爲爭執焦點。這些異議的聲音一一羅列使用晶片護照的負面影響，其中包括質疑晶片護照安全措施不足，將會使儲存在微晶片中的個人資料受到他人瀏覽或複製，而如果這樣的情況發生，將使恐怖份子和犯罪集團能夠順利地發動攻擊，犯罪集團能製作複製的護照等。另外，當反對者也認爲：由於包含透過 RFID 進行遠距離讀取的功能，當晶片護照成爲全球性的身分文件時，也可能發展成爲追蹤個人行蹤的工具。同時，隱私權團體也擔心晶片護照的使用，會引發骨牌效應（domino effect），尤其當晶片護照包含了許多個人的生物特徵資料，如果沒有適當的安全防護措施，政府將有可能追蹤個人行蹤。有鑑於美國運用晶片護照至今，引發不少社會爭議，社會大眾對於晶片護照也逐漸發展出負面的印象，因此，我國在擬議採行晶片護照的同時，如何處理晶片護照所使用的生物特徵身分辨識技術和 RFID 科技對於社會整體和晶片護照持照人帶來的不安，很可能將是另一個嚴峻的挑戰。

肆、研究方法

本研究擬採取文獻分析和他國經驗比較研究的方法進行。分析各國和國際組織關於生物特徵辨識法制的相關文獻，以及比較他國使用

生物特徵辨識技術的經驗，希望得以藉由他國的研究和實踐，對於生物特徵辨識相關的問題有更深入的理解，爲將來的政府政策擬定提供參考。

本計畫第一部分將著重於文獻資料之蒐集及彙整，包括蒐集及彙整國際上和生物特徵辨識技術與制度有關之社會與管制變遷文獻，以及和生物特徵辨識技術與制度的政策及規範相關的學術論文、政府文件和實務見解。

第二部分將著重在針對生物特徵辨識身分技術與制度所引發之規範與政策意涵分析研究，以及針對國際甚群針對此一議題所做的辯論和決策進行觀察，以瞭解全球化趨勢在生物特徵辨識科技與制度此一議題上所形成的共識和其實際限制所在。

第三部分將著重於比較分析和政策建議的工作，本研究計畫在此一部分將研究國際社群發展趨勢所得，回饋於國內相關規範和政策的研究上，以期上述兩部分的研究，對於國內相關法制之建構有所啓發，進而尋找出對於現狀的改善之道。

伍、章節安排

基於以上研究方法，本研究之初步章節安排如下：

第一章　緒論

第二章　生物特徵辨識身分制度的發展與現狀

第三章　從美國制度談起：恐怖主義陰影和美國法的國際擴散

第四章　英國制度沿革與實踐現狀

第五章　德國制度沿革與實踐現狀

第六章　歐洲之制度沿革與實踐現狀

第七章　日本制度沿革與實踐現狀

第八章　生物特徵辨識身分制度所引發的社會風險及其辯論

第九章　結論與建議：生物特徵辨識技術未來應用於我國之規範與政策建議

陸、研究結論與預期效益

本研究透過對各國制度發展現狀的比較、對我國個人資訊保護法制面對生物特徵辨識身分技術的規定現況予以檢討，以便瞭解目前生物特徵辨識技術應用可能產生的問題。同時，本研究計畫進一步藉由比較政策和比較法制的觀察研究，分析外國法制對於生物特徵辨識技術的相關規範和學術研究，爲我國利用生物特徵技術辨識身分之相關決策可能產生的問題，尋求衡平而完善的解決之道。此外，本研究計畫也藉由對他國實踐現狀的觀察，分析生物特徵辨識技術和制度的運用在成本效益以及技術應用上可能產生的複雜問題，以及其因應的方式。這些研究發現，應有助於政府擬定與生物特徵辨識技術運用相關的政策。

第二章 生物特徵辨識身分制度的發展與現狀

壹、身分辨識政策的意義

在現代社會中，「辨識」（identification）幾乎可以被比喻成空氣，是我們生活中不可或缺的一部份。我們通常可以分辨空氣品質的好壞，當我們的感官無法分辨時，我們會利用科學的方法，去研究這種空氣是否對人的健康產生威脅。然而，通常我們對待「辨識」的態度，都是出諸直覺式的反應，例如在美國常聽到的口號「向國民身分證說不！」便是最好的實例。

然而，不可否認的是：隨著資訊時代的到來，舊有的辨識政策正受到考驗。過去幾十年，通訊技術的進步以及大型機構的產生，所代表的正是各種不同機構和組織基於各種不同的新目的，辨識他人身分的努力。這些機構和組織使用新的、不同的方式辨識他人，也使這些辨識過程產生新的、不同的影響。再者，隨著數位溝通科技、電腦和資料儲存科技的進步，更多與人有關的資訊，便更容易被取得，也有更多人、機構和組織可以有效利用這些資訊。

然而，這些因爲科技進展而來的新挑戰，卻未真正改變舊有的辨識政策。因此，要理解目前的生物特徵辨識科技，到底對人類生活帶來怎樣的影響，我們應該有必要重新檢視傳統的身分辨識政策。

「辨識」是一種重要的經濟生活和社會生活的黏著劑，它存在於所有人際關係的開端，也存在於所有人際關係的延續發展過程。通常，「身分辨識」總是與某種型式的紀錄連結在一起，而所

有的紀錄系統，都會形成某種類型的監視系統，這些監視可能是好的，也有可能具有負面影響。監視使得企業可以提供消費者以較低的消費得到較好的服務，但是也使得企業可以利用垃圾郵件騷擾消費者。因此，我們首先必須瞭解的是，對於辨識最主要的需求，乃是監視，辨識構成監視系統的前端工作，或者可以說是構成監視系統的基礎。[18]

然而，與辨識相對的「匿名」，無論是在文化傳統或法律制度中，卻經常被認定爲具有一定的價值。當匿名是預設的規則時，個人將得以創設自己的人際關係，並且隨心所欲地經營私人生活，同時，匿名也可以保障某些對社會長遠發展而言有價值的行爲，例如自由的言論、不同的意見甚至不服從等。[19]

整體而言，「身分證明文件」往往是辨識過程的焦點，也是辨識政策爭議的中心點。身分證明文件是一種溝通工具，它可以提供某些個人資訊給進行身分辨識者（verifier），使得出示身分證明文件的任何個人，在第一次出現時，就被當作已知者（known）看待。

隨著科技的進步，新的辨識科技可以擴張監視系統的使用範圍，並且讓個人檔案的建立，無論在數量或容易程度方面，都隨之增高。辨識科技和監視系統的使用，在很多方面固然對我們是有利的，但這些使用也會對社會帶來相當程度的威脅。在晚近歷史上，不乏威權統治政府使用身分辨識系統執行恐怖監控計畫的經驗，納粹統治便是最典型的實例。事實上，統一化的身分辨識系統所產生的成本，不只是極權統治的受害者需要承受的成本和

---

[18] *See* JIM HARPER, IDENTITY CRISIS: HOW IDENTIFICATION IS OVERUSED AND MISUNDERSTOOD 1-7 (Cato Institute, 2005).

[19] *See generally* NANCY CHANG, SILENCING POLITICAL DISSENT: HOW POST-SEPTEMBER 11 ANTI-TERRORISM MEASURES THREATEN OUR CIVIL LIBERTIES (NEW YORK: SEVEN STORIES PRESS, 2002).

後果，即使是和平穩定的國家（如同今日的美國），其人民一樣必須承擔類似的成本和後果。在辨識科技高度發達的今天，此一現實或許更值得重視。[20]

同時值得一提的是：多元化的辨識系統，比較容易防止身分詐欺的情形發生，也因而能夠賦予個人更多的自主權和更高的自由度。究諸實際，要提出一個完整的身分辨識政策，並非易事，因此，我們或許同時應該考慮的是：我們所追求的政策，無論是企業或政府，到底是頻繁地使用身分辨識系統，還是應該減少身分辨識系統的使用？因爲，身分辨識可能無法產生如我們所預期的效益，但是卻會逐年增加成本，而這些成本不見得是在我們預料之中的成本。所以，當我們不需進行身分辨識即可授權（authorization）時，應該偏好使用這種降低身分辨識需求的模式。再者，除了多元化的身分辨識系統之外，多人競爭的身分辨識產業，也比政府獨占、統一化的身分辨識系統更好，更能保護人民的自主性和自由度。

貳、理解身分辨識的發展：生物特徵辨識科技現狀鳥瞰

一、瞭解身分辨識

身分辨識深植於我們日常生活中，我們鮮少仔細思考辨識的過程爲何，但身分辨識卻是社會經濟生活中相當重要的一部份。試想一個沒有辨識的世界，你將無法辨識他人的身分，他人也無法辨認你，如此一來：任何有系統的生產都可能隨之瓦解。就身

[20] *See, e.g.,* Peter Galison & Martha Minow, *Our Privacy, Ourselves in the Age of Technological Intrusions, in* HUMAN RIGHTS IN THE "WAR ON TERROR" (Richard Ashby Wilson, ed., Cambridge University Press, 2005).

分辨識而言，有以下幾個重要基本概念，值得先予以說明：

（一）辨識符碼（identifier）

辨識符碼是建構起整個身分辨識的基礎，也就是區別某特定個人和其他人的一些事實。辨識符碼是一些用來將人群分類的事實。雖然，目前有很多種類的辨識符碼，辨識符碼通常被歸類爲三種，個人本身的某類資訊（something you are）、個人知道的資訊（something you know）和個人擁有的資訊（something you have），但還包括另外一種類型的辨識符碼，可以與上述三種加以區別，也就是個人被指定的資訊（something you are assigned）。不同的辨識符碼具有不同的品質，有一些辨識符碼是固定不變的，或至少它們有可能固定不變，例如指紋或母親未婚時的姓氏。有些辨識符碼是暫時的，只存在短暫的時間。有些辨識符碼是因人而異的（DNA），有些則是相當普遍，很多人都擁有相同的辨識符碼，例如棕色的頭髮。這些辨識符碼的品質，包括是否固定不變、因人而異和永久存在，都會幫助我們決定，哪些辨識符碼適合用於身分辨識。[21]

（二）辨識（Identification）和確認（Authentication）

身分辨識是指進行辨識者（verifier）將個人的辨識符碼，與辨識者之前蒐集的其他辨識符碼加以比對的過程。辨識者可以因此取得被比對者的資訊和其他資料。在傳統社會中，身分辨識在人際關係中是自動發生的現象，但是，隨著大型且複雜的機構和組織出現，身分辨識也隨之遭到挑戰。大型的機構和組織無法再像過去的地方組織一樣，透過感官方式去辨識個人的身分。同樣地，遠距通訊，特別是網路的產生，也改變人們辨識他人身分的方式。例如：我們無法在網路的互動中，看到對方，但僞造的身

[21] HARPER, *supra* note 1, at 15-17, 23-26.

分，卻往往是犯罪的重要的工具。因此，線上交易的重要步驟之一，就是確認身分。例如，透過使用者名稱和密碼的方式，確認使用者的身分。然而，此處值得注意的是：身分辨識雖然意味著接近完全正確的辨識過程，但確認卻允許比對可能出現錯誤的風險。在面對面的情境下，絕對的身分辨識是很容易、簡單的，但是在遠距或是與機構的互動中，辨識是不方便且成本昂貴的。當機構選擇辨識符碼時，它們是減少確認錯誤的風險，但是並非達到完全的辨識。

（三）授權（Authorization）

授權是指當某人決定一個交易行爲或互動是否繼續的過程。許多人或許會假設自動櫃員機使用的是身分辨識，但是，事實上，大部分的自動櫃員機（使用卡片和密碼）實際上是進行非身分辨識的授權行爲，因爲：任何擁有提款卡和知道密碼的人，都可以提款，無論他們的身分爲何。

當然，有時候身分辨識的確是決定是否授權的重要因素。換言之，身分辨識常在決定授權與否的過程中，被當做一個工具使用，但是授權卻可以在沒有身分辨識的情形下進行。

一般而言，身分辨識系統通常會在其他的辨識系統上進行：某個人被一個機構或其他個人辨識其身分之後，這個辨識會被另外的機構或他人所接受，此一過程相當自然，而且是必要的，但是，這種過程卻越來越被用於身分的冒用。簡言之，一個冒用身分者可以藉由一個身分辨識證件，取得其他的身分辨識文件，再透過這些具有公信力的身分辨識證件，進行詐騙行爲，例如開立銀行帳戶。

（四）多種要素的辨識（Multifactor Identification）

爲了降低身分辨識錯誤的風險，使用不同種類的辨識符碼，

便是多種要素的辨識。換言之，多種要素的身分辨識，可以降低錯誤和誤認的風險。

（五）身分辨識證件（Identification Cards）

身分辨識證件是最複雜的辨識工具，他們屬於「個人擁有的資訊」此一類型的辨識符碼，但是身分辨識證件卻也含有持證件者的資訊（個人所屬的資訊）或密碼（個人知道的資訊），也就是說，身分辨識證件是屬於一種多種要素的辨識工具。

當身分辨識證件有效使用時，所提供的是即時且單一步驟的身分辨識功能。同時，身分辨識證件也可以被當作溝通的工具，它將個人的資訊，透過有公信力的第三方，予以傳遞出去。這個溝通的鎖鍊，可以分爲三個步驟，從資訊的主體到核發證件者、從核發證件者到辨識者，再由辨識者進行確認。也就是首先由資訊的主體將其自身的資訊提供給核發證件者，核發證件者透過證件的發給，將資訊傳達給辨識者，最後則由辨識者確認證件上的資訊是否符合證件持有人的資訊。這個鎖鍊的每一個部分都有其弱點，第一個步驟，資訊主體可能提供錯誤的資訊；在第二個步驟，身分辨識證件可能被僞造或變造；第三個步驟辨識者可能沒有仔細比對證件的資訊和持證件者的資訊。

二、傳統身分辨識符碼的類型及其意涵

如前所述，透過某人所知道的資訊辨識其身分，是根深蒂固於人際關係和人與人的互動當中。每一個人或多或少都會觀察他人是否言行一致。人們在溝通的過程中，很少試圖欺騙他人，而通常我們也會使用知識很快且微妙的確認他人所聲稱的身分。我們都預期擁有某種身分或地位的人會知道某些事，例如他們的家庭史、特殊的技巧等。而且由於假設大部分的人都是誠實的，也很少人會有辦法假裝他擁有某種知識，因此，在大多數的情形下，

個人知道的資訊（something you know）可以確認個人宣稱的身分。身分辨識符碼類型，大致上可以區分成以下類型[22]：

（一）母親未婚的姓氏

在美國社會中，幾乎每一個與金融機構或理財人員通過電話的人，都曾經爲了確認身分，而被要求過提供母親未婚的姓氏。然而，因爲普遍使用的結果，以母親未婚姓氏做爲辨識符碼的品質，卻正在下降當中，其原因在於：將母親未婚姓氏做爲銀行的辨識符碼的事實，已經眾所周知，而此類資訊又不是很難取得。

因此，比較具有警覺性的機構或組織，漸漸將其所使用的辨識符碼朝多元化的方向發展，使用例如父親的中間名等資訊作爲辨識符碼。擁有大量個人資訊的機構或組織，也可以利用其他個人資訊作爲辨識符碼，例如詢問某些個人很容易回答的問題（例如你上次購物買的物品爲何），以確認個人的身分。

雖然這種「個人知道的資訊」辨識符碼，常被用於與大型機構或組織的交易當中，但是，這種辨識符碼的使用，最早並非源自這類的交易。這種以知識爲基礎的辨識符碼，使得身分辨識機制比姓名的使用更往前進一步。當然，這種辨識符碼需要仰賴日漸精緻的語言系統，而且可以適用於較大範圍的交易和商業活動。這種「個人知道的資訊」辨識符碼所具有的效用，與其他辨識符碼不同，在某種意義下，這種辨識符碼是相當好用的，因爲其很難爲他人得知，可以是隨機的。但是他們也會因爲使用者貪圖方便的心態，而破壞其辨識的功能。

（二）密碼

和母親未婚的姓氏一般，密碼也是「個人知道的資訊」的辨

---

[22] *See generally* HARPER, *supra* note 1, at 35-45.

識符碼之一。密碼可以改進其他辨識符碼的缺點，但是也有自己的缺點。其他的「個人知道的資訊」辨識符碼的缺點，例如母親未婚的姓氏的缺點，主要是無法改變，以及容易爲他人得知。而密碼則只是由一連串的數字和符號所組成的，可以改變，同時也難以猜測。

然而，密碼也有缺點，許多人爲了避免需要記憶太多密碼，可能會在不同的系統中使用相同的密碼，也可能在犯罪者可能找得到的地方寫下密碼。因此正確地規劃密碼系統的使用，亦即應該設計一個很難使外人使用但是便利使用者的密碼系統，便成了關鍵所在。[23]

（三）加密技術

加密技術是使用數學公式，將可閱讀的內容轉變成一種無法瞭解的形式。傳統的加密技術，兩個人擁有相同的解密鑰匙，可以將訊息加密和解密，以互傳訊息。

公共鎖鑰加密（public key cryptography）則是一種較新且更複雜的加密。在這種加密中，一個人擁有一個私人鎖鑰和公共鎖鑰。他會保持私人鎖鑰的秘密，而讓公眾知道公共鎖鑰。一個經過私人鎖鑰加密的訊息，只能經過公共鎖鑰解開。同樣地，將過公共鎖鑰加密的訊息，只能透過私人鎖鑰解開。

既然個人的私人鎖鑰是秘密的，收到經過私人鎖鑰加密訊息的人，既然可以透過相應的公共鎖鑰解密，就可以確定該訊息是由該個人所發送的。這種一對一的鎖鑰，是由數位認證機構核發的，此一公共鎖鑰的設置，可以使網路使用者確定他們交易對象的身分是經過認證的。所有可以透過該個人公共鎖鑰解密的訊息，都可以確定是由該個人所發送的。這種鎖鑰就是一個辨識符

[23] *See* BRUCE SCHNEIDER, APPLIED CRYPTOGRAPHY 4-5 (1996).

碼，他們可以確定訊息作者的身分。[24]

（四）個人所有的事物

「個人所擁有的事物」是第四種辨識個人的辨識符碼，亦即透過比對個人所擁有的事物，確認個人的身分。與其他辨識符碼相同的是，這種辨識符碼有時是用作辨識是否得到授權，而非辨識身分。例如 UPS 的制服，就是被用來辨識是否得到 UPS 公司的授權，而非辨識個人的身分。[25]目前最常用來做爲辨識符碼的是證件，例如駕照或其他政府或私人核發的證件。

三、理解生物特徵辨識科技

「生物特徵辨識」此一概念的出現，並不是晚近之事，舉例來說，在父母和子女的關係中，很重要的一環便是他們都很會辨識對方。當母親和小孩互相凝視對方、觸碰對方的手和臉、觀察對方的舉動、聽對方的聲音時，他們會直覺地記錄他們的觀察，之後並會利用這些觀察所得，辨識對方。

雖然，科學研究結果可能尚未顯示大腦如何精確地進行這種身分辨識過程，但是我們或許不難想像一個人的心智如何組織這些身分辨識資訊：我們觀察、獲得的關於個人的資訊都是個人的特徵，某些特徵是因人而異的。例如人的臉，因人而異的特徵包括各個感官的位置、眼睛的顏色、嘴的形狀和嘴唇等。而且，更重要的是，絕大部分的人，都是辨識這些特徵的能手。

（一）　生物特徵辨識符碼的本質[26]

有一些因人而異的特徵，可以被用做某種索引，也就是我們

---

[24] *See* HARPER, *supra* note 1, at 42-45.

[25] *See generally* HARPER, *supra* note 1, at 47-53.

[26] *See generally* HARPER, *supra* note 1, at 159-62.

會有意識地用來形容他人的某些資訊，例如髮色、眼睛顏色、身高、體重、膚色等。當我們再次的看到這些人，我們的感官和大腦立即觀察他們的特徵，並與我們之前觀察的特徵連結。這些被用作索引的特徵，就是辨識符碼。當然臉部和身體的特徵只是許多辨識符碼當中的一部份，有許多不同的辨識符碼，使用不同的辨識方式。

當我們看到一個朋友從街上走來，我們會注意並且將此人身上的物理特徵，與之前我們蒐集的辨識符碼資訊比對。這個過程就是生物特徵的辨識，biometrics 這個自是由兩個希臘字組成的：bio（生命）和 metron（尺寸或程度）。生物特徵辨識身分只是對於生命體（或過去的生命體）的度量，以辨識生命體的身分。生物特徵辨識身分被廣泛的說成是一種新興的高科技產物，但是生物特徵辨識身分早在史前就已經開始被人類社會所使用。所謂的新興領域，只是在生物特徵辨識身分的過程中，加入電腦和設備的使用而已。

（二）生物特徵辨識身分機制的特色

生物特徵辨識身分的方式，有兩個主要的類型：物理的類型和行爲的類型。物理類型的生物特徵辨識身分機制，是度量人身體上的各種獨特的特徵，例如髮色、眼睛顏色，以及許多隨著科技進展會成爲辨識符碼的虹膜和視網膜等。

另外一個種類，亦即行爲類型的生物特徵則是度量個人的獨特行爲，這些很爲他人很難模仿。包括聲線和步伐，這種行爲特徵的分析，較難完全藉由機器進行分析，但是分析的技術卻也正在進步當中。常見的行爲特徵，就是個人的簽名。

大部分的生物特徵辨識身分符碼，是由我們的基因所影響的，然而這並不會使生物特徵永久固定不變或較容易測量。染髮、隱形眼鏡、手術、受傷、化妝等都會改變這些辨識符碼。雖然 DNA

現在被當作非常可靠的辨識符碼，但是將來基因科技的發展，卻有可能會改變一個人的 DNA。

許多生物特徵辨識方法是以非基因的生物特徵或是混和的（基因的和非基因的）辨識符碼，做爲基礎。這種辨識符碼反應基因和生活經驗在人體上的永久遺留，包括體重、刺青、牙齒記錄、照片、出生記錄等。

無論是早期的使用化學物質的照片或是現在的數位照片，都紀錄我們的臉部特徵和生活，這些臉部特徵是我們習於辨識的。這些辨識符碼會隨著生命的經過而累積甚或改變，一個人年輕和年老的照片是不同的，因此，生物特徵辨識身分符碼的品質是很重要的。

參、生物特徵辨識身分相關制度的發展

一、匿名性的重要性

所謂的匿名，就是人民不表示其身分的行爲。匿名的權利，就是所謂不被強制辨識的權利。然而，除了涉及憲法權利的情況之下，我們是否保障不被強制辨識的權利？隨著個人所得稅的課徵、福利國家的興起、以及政府權力的擴張，我們主張不被強制辨識的權利，似乎越來越沒有可能性。即使是在刑事法領域，長久以來受到捍衛的「緘默權」也處於節節退敗的狀態。[27]在晚近的 Hiibel v. Sixth District Court of Nevada[28]此一判決中，美國聯邦最高法院認爲在警方有一點懷疑，某人可能涉及犯罪時，該某人在警察的盤查時，必須表明身分。法院認爲透過身分的辨識，警

[27] *See generally* HARPER, *supra* note 1, at 103-110.
[28] 124 S. Ct. 2451(2004).

察可以知道該人是否涉及其他犯罪、其心理狀態如何，可以幫助警察辦案。但是警察爲了辨識該人的身分，必然將調查的重點從當前的犯罪，轉移到調查該嫌疑人的身分之上。這種焦點的轉移，使得警察可以透過懷疑任何人的狀態，便取得調查任何人身分的權利。

究諸實際，除了在法律領域之外，人們也透過匿名的方式，避免自己的行爲受到他人的影響。例如，在公司裡，告密者透過匿名得以揭露許多不當的行爲，同時免於失去工作。而網路上的討論區，也透過匿名使得人們得以討論性等敏感的話題，而不必向其熟識的人交代他們的心態。所謂的匿名是給予人們選擇何時揭露其身分的權利，而人們自願性的揭露其身分的情形，通常會對其個人和社會都是有利的。匿名可以給予個人對抗強大社會壓力和國家專制權力的權利。

二、身分辨識制度的運作及其風險

（一）駕照做爲身分辨識證件[29]

在現代社會中，我們常常在各種場合裡被要求出示證件，例如銀行開戶、進入某棟大樓等各種情形，皆屬之。然而，要求出示身分辨識證件和移動能力是一起隨著歷史而發展的。

汽車發明之後，由於法院認爲汽車本身是一種危險的機器，因此透過一系列的判決，使得操作這種危險機械成爲國家賦予人民的特權，而非人民的權利。這也使得國家可以規制駕駛汽車者。這種看法在過去是合理，但是隨著汽車成爲許多人的交通工具後，對汽車的限制將成爲對人們移動權利的限制，而美國法院則是透過認定汽車使用相關規定和駕照要求是合乎正當法律程序的

[29] *See generally* HARPER, *supra* note 1, at 114-116.

方式，來迴避這個問題。

早期在駕駛汽車仍是特權之時，國家已經要求駕駛者必須有駕照。歐洲最早有這種規定，隨後美國也繼受這種規定。我們很容易假定，駕照的規定是爲了安全的考量，但是，歷史證據顯示這是很複雜因素。早期的駕駛者大都很有錢，或是將汽車用於商業，因此國家透過駕照可以增加稅收。

以 American Association of Motor Vehicle Administrators（AAMVA)爲例，AAMVA 除了致力於加強對駕駛的控制外，也積極推動全國性身分辨識證件（簡稱 ID）的核發此一工作。而在全國性身分辨識證件出現之前，駕照便是其中最重要的身分辨識證件之一。我們將 ID 持有者，稱爲 ID 主體。進行辨識者，稱爲辨識者。核發 ID 者，稱爲 ID 核發者。在沒有身分辨識證件的情形下，機構和個人交易，必須在第一次接觸時，蒐集個人辨識符碼，以便在之後的交易中辨識個人。但是身分辨識證件可以使機構在第一次與人接觸時，透過身分辨識證件，立刻辨識個人的身分。ID 核發者可能透過身分辨識證件辨識個人，當然其他非 ID 核發者也可以透過身分辨識證件辨識他人身分。駕照就是最好的例子。交通部門透過駕照，辨識人民，但是，在實際運作狀況下，也有其他政府或私人也使用駕照作爲辨識的工具。

透過身分辨識證件，辨識者可以瞭解 ID 主體的身分，這個辨識的過程是透過 ID 核發者在身分辨識證件上所登載的資訊來進行的。不過，值得注意的是，整個身分辨識的過程都可能潛藏風險，而問題的根源，則是在於統一的身分辨識系統，會成爲受攻擊的目標，而某一身分辨識證件扮演越多角色，便越會成爲受攻擊的目標。

（二）駕照做爲身分辨識證件的風險[30]

近年來，美國許多州都陸續發現在 Department of Motor Vehicles（簡稱 DMV)工作的員工，有私自販賣駕照的情事。其實，除了員工的貪腐問題之外，DMV 在核發駕照時，也可能基於冒用的身分而受到錯誤的引導，核發駕照。在 2005 年的 Real ID Act 通過之前，各州要求申請駕照的身分文件不一，一般都是要求要有兩項身分證件，以證明該申請者的姓名、住所、年齡等。但是州允許申請者使用的身分辨識證件種類十分繁多，因此當申請者使用罕見但又受到允許的證件申請時，DMV 部門的員工很容易無法判斷真僞而受到欺騙。根據從 2002 年 7 月到 2003 年 5 月，the General Accounting Office(簡稱 GAO)進行一項調查，派遣員工持假造的證件到各個州去申請駕照，結果發現 DMV 的員工很少可以分辨出申請者證件的真假。

其次，美國社會安全部門在線上有一個辨別社會安全碼的系統，用來避免冒用社會安全碼的情形。但是 GAO 發現這個系統本身具有設計和管理的瑕疵，這個發現導致州減少使用該系統。GAO 上述調查也利用過世者的姓名、社會安全碼和其他資訊申請並取得駕照。當然政府可以透過改善計畫，加強申請駕照時的證件查驗工作，但是當冒用身分者可以冒用身分取得真正的社會安全碼時，使用社會安全碼而進行的身分辨識，便無法控制品質。

當社會安全碼這種辨識符碼基於冒用的身分而發出時，DMV 的員工將無法分辨社會安全碼的真假，因爲此時社會安全碼確實是真的。GAO 上述調查曾經利用兩個捏造的身分去申請社會安全碼，而取得兩個社會安全碼。透過這些基於僞造資訊而發出真正的辨識符碼，冒用者將可以取得其他州核發的身分辨識證件。多

[30] *See generally* HARPER, *supra* note 1, at 121-26.

年來，因爲喝酒的年齡限制，也使得許多年輕人去僞造駕照。或許駕照的核發程序可以符合政府管制駕駛行爲的目的，但是越來越多的行政或私人目的，加諸駕照之上，事實上，駕照或許根本缺乏這些目的所要求的身分辨識功能，但卻使駕照成爲對冒用身分者極具吸引力的對象。

由政府所核發的身分辨識證件和私人核發的證件相較之下，很大的不同之處在於：當政府核發證件的程序出問題、或受到冒用時，政府會傾向花更多的錢、雇用更多的人去解決這個問題。當然 DMV 的員工不會希望核發駕照的程序有問題，但是他們也沒有動機去改善這個程序，因爲一旦程序出問題，他們不需要負責，反而可以得到更多的經費和設備。至於私人機構或組織，當其所設計的身分辨識系統出問題，將會影響公司的利益，同時也會威脅員工的工作前景。

以信用卡詐欺爲例，信用卡詐欺行爲已經威脅到私人機構核發者的利益，因此他們會積極採取措施預防，結果詐欺的情形的確隨之減少。私人核發的證件與政府核發者最大不同在於，政府核發的證件，在核發過程中大多仰賴 ID 主體提供的資訊，而私人核發的證件，核發過程不但仰賴 ID 主體提供的資訊，同時也仰賴 ID 核發者自己蒐集和從第三者處購得的資訊。例如公司在發給一個員工證件前，除了該員工提供的履歷表資訊之外，還有其他雇主在面試過程以及將來的雇用過程中取得的資訊。同樣的在信用卡的核發過程中，除了申請者提供的資訊之外，發卡銀行也會透過將來寄發信用卡、開卡的程序來確認證件核發過程的正確性。

一般的信用卡詐欺與冒用身分辨識證件兩者的不同之處，在於信用卡詐欺通常會發生在辨識者沒有仔細辨認信用卡與持卡人的身分之上，而非發生於一開始的核卡過程。同時，冒用者的動機也不同，信用卡冒用可以獲得巨大的商業利潤，但是冒用駕照

可能只是青少年爲了飲酒而爲而已，因此執法單位不會爲了這種飲酒的衝動，花費大量的資源追查這類駕照僞造行爲。

（三）身分辨識證件僞造風險及其防僞措施

2005 年內華達州曾經發生有歹徒在半夜闖進 DMV 部門，偷走電腦和一些空白的駕照的事件。這使得歹徒得以使用這些空白駕照，僞造駕照，賺取龐大的利潤。證件核發者爲了確保證件的安全，通常會採用很多技巧。傳統的證件是用紙製造的，現在的證件大多中間爲合成的印刷，前後層還有多層的碳酸脂。特別是在證件內層，印刷技術和其他的技巧，都是用來使得僞造或變造證件變得更爲困難。

透過特殊的墨水、印刷技巧，證件核發者希望確保證件不會被僞造或變造。爲了避免發生像之前的 DMV 部門失竊事件，證件核發者將證件編號，並加強儲存地的警備。雖然這些措施大多可以使得僞造、變造證件變得更困難，但是這無法使僞造或變造成爲不可能。所有可以用於確保證件真實性的技術，犯罪集團都有可能取得，透過黑市或是貪腐的員工，犯罪集團可以取得一般人無法合法取得技術或材料。簡言之，如何確保身分辨識證件的真實，一直是證件核發者和犯罪集團的武器競賽。

這場競賽也關係到辨識者是否能分辨證件的真僞。經過一定訓練的個人，應該具有分辨證件的真僞，但是隨著科技的進展，這場武器競賽的戰場將延伸到電腦和加密技術的領域。越來越多的證件內含晶片，因此電腦被用來辨識證件的真僞。

有兩件事會決定這些防僞措施的功效：僞造證件的成本、僞造者的動機。以鈔票的防僞爲例，從 1996 年開始，美國財政部就開始爲鈔票添加防僞措施，但是直到 2003 年新的 1 元鈔票仍未有新增的防僞措施。這並不是因爲官僚體系的效率太差，而是 1 元美鈔僞造的利潤遠低於 20 元或 100 元美鈔。身分辨識證件也是如

此，如果一個身分辨識證件扮演多種功能，他受到僞造的可能性就大增。

政府永遠必須發行高面額的鈔票，但是政府是否有必要核發具有高價值的身分辨識證件？如果一個證件可以取得個人甚至是許多人的財產，一定有人會前仆後繼的僞造該證件。但是如果沒有一個證件或系統可以取得個人某部分的財產，僞造該證件的動力就會隨之減少。證件安全性的戰爭是一個具有吸引力但是不必要的戰爭。他可以透過核發多個證件和多種的身分辨識避免這個戰爭。最後值得一提的是，上述內華達州失竊的證件並沒有流出市面，警察在一個工地找到所有失竊的空白證件和電腦。

信用卡的使用與身分辨識證件的使用有很大程度是相同的，發卡者透過核對持卡人的資訊，核發信用卡，而特約商店則是透過信用卡，確保購物的金額可以被支付。當 First Hawaiian Bank 開始核發印有相片的信用卡時，的確減少信用卡詐欺的情形發生。因爲當時銀行要求持卡人必須親自到銀行照相。但是當持卡人可以郵寄相片時，相片本身產生的辨識作用與持卡人交給銀行的其他資料一樣，不再具有特別的辨識能力。而將照片放置在信用卡上的發卡銀行，必須冒著盜用信用卡者將自己的相片寄至發卡銀行，而發卡銀行誤將之放置於卡片上的風險。

身分辨識過程的另外一個風險就是，辨識者必需要仔細地辨識證件上的辨識符碼與持卡人的辨識符碼是否一致。就如同特約商店會比對信用卡持卡人的簽名和卡片背面上的簽名是否一致，其他身分辨識證件的辨識者也必須辨識持證件者的辨識符碼與證件上的辨識符碼是否一致。

然而，辨識者的這種辨識能力是有限的。一個主要的原因是因爲辨識者缺乏注意。在海關或酒吧門口，這些辨識者在不同的光線下，全天候進行辨識工作，他們當然可以犯錯。再者，不同

種族的人辨識其他族群的人的能力，本就較差。出於禮貌或是害怕尷尬，辨識者在發覺照片和人不相似時，可能因爲害怕被指稱種族歧視，而不願意指出照片與真人的差異。有時，處於社會經濟階層底層的警衛，可能害怕仔細辨識上層的長官。試想：一個公司的警衛，應該不敢將公司的 CEO 攔阻的門口，而其目的只是爲了再三的辨識其身分。此外，有時辨識的過程是有時間壓力的，例如海關在辨識出境旅客時，可能因爲隊伍太長，而感受到壓力，勉強讓有疑問的人也通過詢問。

以上種種都顯示出辨識者辨識證件持有人的身分時，可能出現的問題。因此，開始有機構使用電腦從事辨識者的工作，藉著比對證件上的生物特徵和持證件者的生物特徵，取代人爲的辨識。讓機器取代人爲的辨識最大的問題在於，機器缺乏判斷能力。人們可以藉由感覺此人是否誠實（雖然會出錯），而進行辨識。但是機器卻是使用同樣的標準對待每一個人。

肆、結語：利用個人生物特徵所涉及的規範議題

如上所述，身分辨識總是隱含冒用偽造等風險，所以勢必需要討論規範問題，而普遍被認為具有個人獨特性的生物特徵身分辨識，一旦遭到冒用或偽造，其所引發的災難，想必更為嚴重，因此，利用個人生物特徵辨識身分，應該討論要同時面對哪些規範層面的問題，應是不可迴避的任務。

一、生物特徵辨識身分證據的可接受度

在美國法院用來判斷證據是否可以被接受的兩個標準爲「一般接受度」（general acceptance）和「科學有效度」（scientific

validity)。事實上，不同的法院會採用不同的標準。第一個標準，「一般接受度」是來自 Frye v. United States，[31]哥倫比亞特區的上訴法院維持原判的一個判決，該判決拒絕接受基於測量心臟的收縮壓，以偵測某人是否測謊的技術所爲的專家證詞，該技術在當時是相當新的技術。判決認爲，法院會接受的專家證詞，必須來自廣爲大眾接受的科學原則或發現，這個原則的建立，已經成爲這個原則所適用的領域普遍接受的事實，過去許多年來，Frye 標準已經變成法院是否接受科學證據的主要判斷指標。法院判斷某項科學證據是否具有一般接受，通嘗試透過專家證詞和現存的文獻、或是該科學方法是否曾用於非司法的用途，以及考慮其他適用該方法的案子。

第二個標準，「科學有效度」是來自 Daubert v. Merrell Dow Pharmaceuticals 這個判決。[32]這是一個關於治療暈眩藥物的所導致的兒童天生缺陷的案子。在本案中，聯邦最高法院駁回下級審法院的判決，下級審法院基於一般接受的標準，拒絕毒物流行病學的證據。法院認爲 Frye 標準的一般接受很難達到，因此不應適用於聯邦證據規則，並且認爲可以接受的證據應該構成「科學知識」(scientific knowledge)，且受到一定的有效性的支持。這個標準應該考量下列因素：該項理論或技術是否或可否在一定的控制項下被測試、這項理論是否受到同儕評核(peer review)和公布、是否有已知的潛在錯誤率；簡言之，也就是該項理論是否受到一般的接受。

適用這些標準於從頭髮上取得的腺粒體 DNA 證據，我們發現即使是相較之下很少或不具有代表性的樣本，都已經被法院接受。在一個腺粒體 DNA 比對符合的情形，一般接受的命題是，

---

[31] 293 F. 1013 (D.C. Cir. 1923).
[32] 509 U.S. 579 (1993).

此 DNA 幾乎總是從母系遺傳，且通常不會隨時間而改變。

至於被用於臉部辨識的電腦運算技術（algorithms），這一種相對而言新的生物特徵辨識身分技術，是否會被法院接受的問題，首先我們必須知道，這個運算技術是否受到充分的測試，並且結果已經被公布，或者是屬於私有的技術，而未受到公布；是否有足夠的文獻支持這種方法的有效性；是否已經建立錯誤可能率；比對的結果如何被呈現（是一種二元的方式，或是對於兩個樣本來自同一人的可能性大小），最後是否一般而言，大家接受這種運算技術可以進行正確的辨識。

就指紋的辨識而言，法院在 Frye 標準下通常會接受指紋辨識證據，然而指紋分析家對指紋的分析、比較、評估和辨識，最近在 Daubert 標準下也受到了挑戰。有人認爲使用專家分析在某些方面缺乏科學嚴謹度，例如在建立已知的錯誤率方面，以及建立控制標準方面。因此這項辨識技術一直受到挑戰。

律師通常會引用一些生物特徵辨識方法的資訊，希望阻止生物特徵辨識身分資訊在法庭上被使用，如果這些資料被使用，律師也會試圖找到可以影響生物特徵辨識身分方法正確性和有效性的因素。通常，基於 Daubert 標準所提出的抗辯，是律師最後的選擇，但是這個抗辯在指紋資料構成本案重要證據的情況下時，往往非常重要。

二、從社會安全碼經驗學到的教訓

由於美國社會安全碼廣泛使用產生的身分竊盜問題，所以，是否應該訂定法律，以避免使用於身分辨識的生物特徵，產生與社會安全碼類似的問題，也就成了備受討論的建議。這個建議與近年來國會提案的禁止販賣和展示社會安全碼的法案一樣，主要的目的在於減少大家接觸高品質的生物特徵圖片（例如虹膜、指紋等）。這樣的立法，將舉證證明爲何可以販賣和展示生物特徵的

負擔，移轉給進行該項行爲者。但是此一建議也討論是否排除相片這項生物特徵，因爲相片通常並非秘密，且通常不會被使用於保安措施上。同時，這個建議也討論是否應排除用於治療和研究的 DNA。此外，加密是否爲傳輸和儲存生物特徵資訊的最佳方式，也是重點之一。其他相關的問題，還包括如何區分應該受到保護的生物特徵、以及這些生物特徵應該如何定義。

三、生物特徵科技引發的法律與社會意涵

雖然實定法並沒有直接與生物特徵科技相關的完整立法，但是從憲法對搜索、扣押相關規範的判決先例、資訊隱私權領域的判決、以及針對親密關係所做成的判決等等，對於我們理解發展生物特徵科技政策所涉及的法律和社會意涵，都有所幫助。此外，我們也應該考量規範層面對於隱私的期待爲何，這種隱私期待也應該是我們決定生物特徵科技使用界限的重要考量因素。

雖然，資訊隱私權的學說在憲法層次上不見得已經出現完整的發展，但是憲法卻的確已經提供了指導原則，幫助我們思考在使用生物特徵以增進安全或便利時，如何和個人隱私權利的保護取得平衡的問題。以美國爲例，Whalen v. Roe 這個判決，在我們考量儲存和分享生物特徵資訊以及保護隱私的必要性時，應該提供我們某些原則。同時，一些關於涉及個人重要事項決定權的判決，也指出一些蒐集生物特徵資訊隱含的問題。在 Planned Parenthood Federation of America v. Ashcroft 此一判決中，法院面對的是決定隱私權是否足以阻止司法部蒐集關於每一個診所實施墮胎數目的資訊此一問題。法院認爲隱私權的確會構成政府資訊蒐集的限制，因此法院禁止政府蒐集這一類的統計資訊，因爲這會影響在這些診所治療的個人的重要事項決定權。這個判決所彰顯的原則，或許可以告訴我們利用生物特徵取得個人重要事項決定資訊的界線何在。

四、生物特徵晶片護照所引發的規範意涵

如前所述，對於關切政府採用晶片護照所帶來的個人隱私侵犯和社會影響的團體而言，在針對晶片護照上內建生物特徵身分辨識機制和追蹤功能所引發的種種安全性保障和隱私保護尚未被當做一個重大的公共政策來辯論，政府部門和民間部門對於晶片護照所引發的隱私權保護議題未做徹底研究、也未特別針對生物特徵晶片護照建立明確的特別法制規範之前，堅持採行生物特徵晶片護照制度，時機未免嫌過早。甚至，生物特徵晶片護照最主要的特色，便是政府在此一護照制度下所掌握的龐大個人生物特徵資料庫，必須配合幾乎滴水不漏的資訊安全防護措施，才能畢竟資訊隱私保護和國家安全維護之全功，這樣的資訊安全防護措施，固然需要搭配相當嚴格的程序規定和法律規範，以發揮應有的功能，但即使如此，仍然難保哪一天政府的資訊安全防護措施，不會遭到侵犯或破壞，屆時無論個人隱私權或者國家安全，均將受到頗大的破壞和挑戰。同時，因爲政府資訊安全防護遭到侵犯或破壞而引發的風險，應該有怎樣的程序保障和實質規範，做爲處理依據，方足以妥善處理，也是一個無從迴避的規範議題。

第三章　從美國制度談起：恐怖主義陰影和美國法的國際擴散

壹、美國身分辨識政策的新發展：以 Real ID Act 為主軸

Real ID Act 此一立法，是美國身分辨識政策晚近最重要的發展。Real ID Act 這個法律，表面上是針對防止恐怖份子進入美國而制訂的，就連其審議過程，也是依附在給予美軍在伊拉克和阿富汗戰役上更多經費的法案之後。[33]但是，事實上，這個立法是爲了防止非法移民入境而訂定的，因此該立法訂定了許多方法，以補救州核發身分辨識證件的既有缺點。

究諸實際，自從 1986 年開始，每國會已經設法要透過立法解決非法移民的問題。例如 Immigration Reform and Control Act 要求雇主在雇用新進員工時，必須蒐集其身分證件和確認其是合法居留，否則將課以罰金或自由刑。[34]透過私部門，也就是雇主，解決非法移民的問題之所以成效不彰，主要原因是有太多隨手可得的假證件，而雇主也沒有太大的動力去維護該法的確實執行。同時，對於雇主而言，出賣這些願意辛勤工作的員工，也是與他們自己的利益相違背的。

相對地，Real ID Act 則是要求州所核發的身分證件必須具有某些形式，不符合要求的身分證件，將不能用於進入聯邦機構、核電廠、登機以及其他國土安全部指定的用途。本報告在第二章

---

[33] *See generally* JIM HARPER, IDENTITY CRISIS: HOW IDENTIFICATION IS OVERUSED AND MISUNDERSTOOD 145-46 (Cato Institute, 2005).

[34] *Id.*

中所敘述的政府核發證件時的身分辨識過程，亦即 ID 主體提供資料給 ID 核發者，ID 核發者製造身分證件，最後辨識者比對身分證件和持證件者的識別符碼。以上每個步驟都有其弱點，隨著政府核發證件所發揮的功能越多，這些弱點也就越會受到攻擊。因此，Real ID Act 針對每一個弱點，試圖予以改善，但是這樣的要求，對於一個國家身分辨識系統到底帶來怎樣的影響，或許還有待評估。

首先，在第一個步驟，也就是 ID 主體提供資訊的步驟，Real ID Act 要求要蒐集四個種類的資訊：

- 一份有照片的證件。如果該證件有個人的全名和出生日，沒有照片的話，也可以例外接受。
- 個人出生日的文件。
- 個人社會安全碼號碼的證明，或如果個人未能擁有社會安全碼，其證明的文件。
- 顯示個人姓名和主要住所地址的文件。

Real ID Act 也要求個人必須提供其合法居留的證件。同時要求 DMV 部門必須將所有申請的文件數位化，將申請文件的紙本保存 7 年，電子檔保存 10 年。DMA 不能再接受其他的外國文件，除了護照之外，每一個申請者必須強制照相。該立法也要求 DMV 向這些文件核發機關確認這些申請者提供的文件的真實性、完整性和有效性。要求各州設立課程，教導 DMV 的員工分辨文件的真僞。[35]

如同私部門在證件核發過程後會透過其他管道確認個人的身分一樣，Real ID Act 也規定在核發證件後，州應該定期使用

[35] *Id.* at 146-50.

Systematic Alien Verification for Entitlements System，這個系統可以確認在美國境內外國人的狀況。同時也要求州必須向社會安全部門確認社會安全碼。也就是要求州利用其他政府蒐集的資訊，確認申請者的身分。但是 Real ID Act 並沒有要求政府必須向其他私部門確認申請者的身分。向其他私人確認他人身分是私部門常用的手段，但是，對政府而言，卻是有爭議的作法。

CAPPSII（全名爲 Computer Assisted Passenger Prescreening）是國土安全部運輸安全局在 2000 年中期用來確保飛航安全的計畫。這個計畫的內容一直在改變當中，但是其中一度美國政府會用航空公司的旅客名單和私人的紀錄比對，以確定旅客的身分。政府對於沒有嫌疑的人進行背景調查，有許多不同種類的方式，例如政府可以透過私部門爲了市場或行銷的目的而蒐集的資訊來進行調查。另外一種方式，則是政府自己蒐集更多的資訊，例如 Real ID Act 要求州政府必須確認申請者提供的資料，以及保存這些資料，同時也要求州政府必須將資料交給全國駕駛者資料庫。這種蒐集和保存資訊的作法，所顯示的是美國的身分辨識政策走向，出現了一個相當明確的趨勢：透過一個高品質的生物特徵，例如將 DNA 加入辨識的文件中，國家將可掌握所有的美國人，並且在有必要核發身分證件時，核發這些證件，而不需要靠 ID 的主體提供這些資訊。如果這種單一、國家核發的身分證件的政策不改變的話，未來勢必會產生一個老大哥的資料庫，而這正是許多美國人所抗拒的未來。

在證件的安全性方面，Real ID Act 要求證件必須使用一定的安全標準，以避免受到僞造和破壞。在證件製造的場所必須有一定的安全防護，對於證件的材料的紙張也必須有一定的安全保護。其中一種防護的方向就是使用加密。例如在證件上加入晶片，而晶片是經過加密的。如果晶片是透過公共鎖鑰加密，辨識者使用核發者的公共鎖鑰，將可以將晶片上的資料解密，並且確保這些資料是由證件核發者所加入的。也可以使用其他的儲存資料的

型態，例如晶片上可以含有一組密碼或其他的識別符，這些也是被加密的。辨識者操作的辨識器可以透過密碼向中央資料庫要求資訊，確保卡片上的資料不是經過僞造的。然而這些技術的運用，將會使整個辨識過程對於一般美國人而言，更加的不透明。辨識過程將不再是爲了他們而進行辨識的工作，而是將成爲將他們當做辨識的客體，而進行辨識工作。[36]

在此一身分辨識的最後一個步驟中，Real ID Act 要求建立一個機器可讀取的辨識系統。指紋、虹膜、手部辨識和其他機器可讀取的生物特徵，在今天的美國邊境上，已經是對外國人廣泛使用的身分辨識機制，透過這些生物特徵，可以更加確認儲存於證件上的生物資訊，與證件持有人爲同一人。也就是我們可以將個人的生物資訊儲存於晶片中，並附於身分證件上。進行辨識時，就是辨別證件上所儲存的生物資訊與持證件者的生物資訊是否符合。機器不會累，也不會受到壓力或感到難堪，機器通常也不會有人工辨識的種種弱點，所以利用機器辨識可以提高準確度和辨識的速度。當然這種辨識的方式可以有很多種，身分證件上的晶片可以只是一組經過加密的密碼，辨識者透過密碼存取中央資料庫的生物特徵。也可以根本不需要身分證件，將晶片放置於鑰匙圈、手錶或是人身體上。

既然個人可以透過生物特徵而被他人辨識出來，那麼根本就不需要身分證件了。透過人身上的指紋與資料庫的指紋，即可比對出該人的身分。究諸實際，現在也的確已經有相當高品質的電腦辨識系統，根本不需要任何實體的證件，就可以進行身分辨識。我們可以將所有的辨識資訊都存在同一個資料庫中，所以個人生命中發生過的重要事件，以及個人的法律地位，都可以包含在內，

[36] *Id.* at 150-51.

而這些資訊都與個人的生物特徵連結。這樣的資料庫可以用於追蹤恐怖份子，瞭解恐怖份子的行蹤，證明恐怖份子與他人的聯繫。當然，也可以用於一般性的執法工作。

但是當這個資料庫儲存的資訊越多，就會有越多的人想要破壞或入侵該資料庫。同時，這任何加強資料庫防護的措施，可能都忽略了一點，也就是這個身分辨識系統最後仍然必須仰賴人力操作，只要是有人操作的地方，就會有貪腐存在。換言之，這個立法改革還是忽略了當國家使用單一的身分辨識系統時，將會有更大的動機誘使他人去破壞和入侵該系統，而這種強化過的辨識系統，則是會損害大多數誠實的人的方便性，因爲，這些誠實的人必須忍受的，是對他們自由的侵害，以及個人自主權空間的縮小。從這個角度來看，此一身分辨識系統到底是爲誰帶來了方便，又爲誰帶來的風險，似乎便是一個頗值得深入思考的議題了。

貳、生物特徵身分辨識的陷阱

一、使用生物特徵辨識身分的趨勢

雖然生物特徵辨識的可靠性較高，幾乎已經是共識，但是，未來有可能出現生物特徵僞造的情況，例如透過人造的 DNA 和指紋，個人可以使用這些僞造的識別符碼，則更是早已有人預測的景象。究其實際，有兩個因素使現代的生物特徵辨識更加獨特：第一個因素是其使用標準化的測量方式，DNA 的檢測是使用科學的過程，他人用同樣的過程將可以得到相同的結果，這可以降低人爲的錯誤，指紋的辨識也是如此。目前大家對於指紋和 DNA 的辨識過程，大致上說來是充滿信心的，雖然我們對於其他生物特徵的功能，未必這麼有信心，但是隨著科技的進步，很可能有一天其他生物特徵也會得到青睞。

第二個因素可能是更重要的因素，也就是現代的生物特徵是

機器可以辨識和記錄的對象。機器記錄的生物特徵，和其他與生物特徵連結的個人資訊，可以輕易地被複製、廣泛地與他人分享、與其他資訊連結、以及可以保留很久的時間而不會變質。這就是現代辨識系統對於我們在傳統上所享有的隱私權帶來的威脅。以往我們透過記錄存取的不易而保有的隱私，都將因此消失。這種生物特徵資訊具有高度正確性，而且是有用的個人資訊。任何機構都可以蒐集其他個人資訊，並與個人生物特徵連結，使生物特徵成爲一種索引資訊。

現代機構蒐集資訊和儲存資訊的能力，會隨著科技的進展而進步。這將改變我們與機構之間的關係，其中身分識別技術的改變，更將會對我們產生很大的影響。人與人之間事實上的距離，正在改變中，雖然這個改變是相當輕微的，但是這個改變方向將會造成莫大的影響。這種事實上的距離往往可以確保即使是非隱私的個人資訊，也不會成爲眾所周知。我們選擇吃的東西、去的地方、見面的人，這些事情都是某種事實上隱匿的狀態下，所做的決定。然而，機器辨識系統和其他個人資訊的蒐集結果，將會改變這個狀況。

當然，很多人會在某種情境下選擇被辨識，例如消費者希望收到某些爲其量身打造的購物促銷計畫，這是個人理性的選擇。然而，也有很多人想要更多的隱私，在購物時保持匿名，但是卻很少有市場去肯認這種偏好，也沒有實際的市場調查，瞭解消費者這部分的偏好。在一個同質性的市場中，消費者很難得到任何保護隱私的選擇。即使可以找到例外的例子，例如某些汽車保險業者，允許被保險人選擇是否在其車子上加裝記錄器，這個記錄器可以記錄車主的使用行爲，作爲保費打折的計算基礎。不願意安裝的車主，將無法取得折扣。在在多數的情形下，想要更多隱私和匿名的消費者並無法形成一個市場區塊，而使市場願意提供這類消費者其他選擇。如果有足夠的消費者願意花費成本，維護

自己的隱私，企業將會發展出不需要識別的交易型態，此時授權將是關鍵。許多的交易只需要確保買受人願意付錢即可，此時根本不需要辨識身分，只需要一定的授權，即可進行這類的交易。

在上述情況下，最重要的是，必須把選擇權留給個人。如果我們的政策是每一次與企業或政府接觸都必須先經過身分辨識的話，我們將沒有辦法選擇匿名。因此爲了保留選擇權，我們應該認爲預設的狀態是匿名的，如果個人願意揭露其身分，便可揭露。只有在非常重要的情形下，才應該以受到辨識爲預設的狀態。相對地，統一的身分辨識系統，則將會使得個人的隱匿性消失，因爲統一的識別系統，例如社會安全碼，將會將個人的所有資訊連結在一起，尤其隨著科技的進步，機器可以大量的蒐集個人資訊的情形之下，更是如此。此時唯一的選擇便是我們可以選擇使用不同種類的識別符碼，使得不同的識別系統間資料無法互相流通，這樣就比較可以保護我們行動的隱匿性。

二、國家使用生物特徵辨識系統的歷史經驗

從歷史上來看，使用生物特徵辨識系統的歷史，並非短淺。例如：在南非，立法者便曾經通過 the Asiatic Law Amendment Act，要求印度人在一定期間內必須完成註冊和按捺指紋，同時印度人也必須隨時隨地攜帶身分證件，警察可以隨時進入他們的家中，檢查他們的許可證。隨著一連串的抗議，甘地的組織和政府達成妥協。在 1914 年時，甘地離開南非，但幾十年後，南非開始實行惡名昭彰的種族隔離政策，要求所有黑人必須隨時攜帶身分證件。事實上，南非只是使用註冊和識別的方法控制人口的許多政府之一。[37]

---

[37] *See generally Calvin Kytle, Gandhi's Story in South Africa, in* NATIONAL IDENTIFICATION SYSTEMS: ESSAYS IN OPPOSITION 255-63 (Carl Watner ed., 2004).

在俄國 1920 年末期和 1930 年，強制的集體化管制，使得許多人被迫遷徙。因爲在那段期間許多人遷移到都市，影響原先的配給制度，所以政府開始發給城市居民證件，規定有證件者才可以繼續居住，其他沒有蓋章證件的人就會被驅離。許多人因爲違反這個法律，被送至西伯利亞的勞動營。[38]

另外一個出於良善目的的註冊系統，則是荷蘭。在二次大戰前，在大多數歐洲，都市傳統上會記錄人民的出生、死亡和遷移。這些記錄方便荷蘭政府分配權利、義務和福利，人民也習慣性的遵守。然而當德國佔領荷蘭時，這些記錄被納粹用來拘捕和驅離居民。因爲荷蘭之前的紀錄，使得居民覺得抗拒納粹的登記和身分證件是沒有用的，因爲政府早就掌握這些資訊。隨後，政府要求居民必須攜帶身分證件，這個身分證件含有許多詳細的居民資訊，並且有防僞措施。之後，納粹更在猶太人的證件上附加註記。[39]

身分識別和壓迫之間的關連性，雖然有時候可能被太過於誇大了，但是我們實在不可能忽略其中的關連性。或許有人會認爲這類種族屠殺的事不會發生在今日，然而，在 1994 年盧安達的種族屠殺事件中，身分證件上的註記 Tutsi 便扮演相當重要的角色。有人會認爲這種事不會發生在美國這樣的國家，的確，美國一直是一個有自由傳統的法治國家，但是從歷史經驗來看，美國曾加犯過一些錯誤。從立國到內戰，美國的歷史其十是個充滿了人類奴隸的歷史。在二次大戰期間，美國政府利用人口調查局的資訊，

---

[38] *See generally Nicholas Werth, The Russian Card: The Propiska, in* NATIONAL IDENTIFICATION SYSTEMS: ESSAYS IN OPPOSITION 116-19 (Carl Watner ed., 2004).

[39] *See generally Bob Moore,Population Registers in the Netherlands During World War II, in* NATIONAL IDENTIFICATION SYSTEMS: ESSAYS IN OPPOSITION 120-24 (Carl Watner ed., 2004).

監禁在美的日本人。在 1970 年早期，美國尼克森總統想要透過政府機關影響選舉結果；1975 年有個調查則是發現 CIA 和 FBI 爲了打擊反對政府的團體，進行許多違法行爲。換言之，每個世代都不免會產生對法治的威脅，即使是一個自由傳統深厚的國家，也難有例外。

參、恐怖主義下的生物特徵辨識系統

一、身分辨識的需求和嚴格程度提高

在 911 事件發生之後，美國政府大肆擴張行政權，這些擴權行爲當然比不上納粹時期和蘇聯政府的行爲，這些作爲是否能夠有效抑止恐怖主義，仍可留待歷史公斷。但是，這至少提醒了我們，每個世代都不免會產生對法治的威脅，即使是一個自由傳統深厚的國家，也難有例外。

政府對於身分辨識系統的濫用，可能對人民的生活產生很大的影響。駕照作爲一種政府核發的身分證件，個人必須透過這個證件獲取生活必須的物資、服務等。但是許多州都規定許多違規行爲的處罰，就是吊扣駕照。甚至這些違規行爲與駕駛無關。任何一個仰賴政府核發身分證件以取得物品、服務和基礎設施的社會，政府將擁有權力透過取消這些證件，使人民無法獲得這些物資。這種剝奪身分證件做爲懲罰的政府行爲，應該經過仔細的衡量。隨著科技的進展，識別系統將會使用網路和資料庫，而不是傳統的證件。人們將會難以辨識是何人或哪一個機關，做出令其無法使用該識別身分的決定。

有論者認爲美國是一個保護人民自由的國家，一個全國性的身分辨識系統不會產生這些問題。Amitai Etzioni 在 The Limits of Privacy 一書中指出，身分證件在歐洲已經有長久的歷史，我們沒有原因認爲在美國使用這種身分證件將會損害個人的隱私和自

主。[40]的確，身分辨識系統本身並非是暴政的催化劑，但是其卻是政府掌控人民的重要工具之一。

我們爲了防範火災，會採取許多安全措施，包括保險絲、警報器、滅火器、安全門，還會建置消防隊、消防栓。但是荷蘭的身分辨識系統並沒有建立類似的安全措施，所以當荷蘭落入納粹德國的控制之後，這個系統就被德國所利用。很奇怪的是，社會可以花費這麼多心力，保護人們的安全和財產。卻不花費任何成本去保護人民的自由，而失去自由也會導致失去財產和生命。

美國在 911 事件發生之後，乘客逐漸瞭解到：以往配合劫機者的態度是錯誤的，配合劫機者只會使飛機成爲一個極具殺傷力的武器，不但無法保存自己的生命，反而會對其他地面上的人造成極大的傷亡。但是基於以往的風險分析，對於 911 事件最主要的反應就是不但加強機場的安檢，也對人們進入大樓、住宿飯店、停車等其他日常生活，加強他們的身分辨識。只有透過辨識恐怖份子和罪犯的身分，才可以對其實施制裁，並且破壞他們的犯罪計畫。而 911 的元兇通過機場安檢的畫面不斷在電視上播放，更加強人們認爲犯罪者得以進入機場是讓整個攻擊事件可以發生的原因。因此，在任何場所加強進出者的身分辨識是必要的。

究諸實際，截至目前爲止少有研究可以支撐上述的分析，更沒有研究顯示這種看法是符合成本效益的，或者是符合美國憲法價值的。匹茲堡大學教授 Emeritus Joseph Eaton 在其 1980 年代中期所著的 Card-Carrying Americans 一書中，主張建立一個全國性的身分辨識系統，可以加強對非法移民的控制，和減少私領域的身分冒用，降低逃犯潛逃的能力，甚至找到遺棄小孩的父母。同時，這個系統也會使恐怖份子很難冒用他人身分。[41]但是，作者

[40] *See generally* AMITAI ETZIONI, THE LIMITS OF PRIVACY 103-37 (1999).

[41] *See generally* JOSEPH W. EATON, CARD-CARRYING AMERICANS: PRIVACY, SECURITY,

在這本書中並未提出一個可以適用於真實世界的具體計畫，他沒有提到政府的辨識身分的檢查點的設置等問題和政府監控等可以使全國身分辨識系統有效運用的問題。

至於知名的社會學家 Amitai Etzioni，晚近也在 The Limits of Privacy 一書中討論許多當代的隱私議題。Etzioni 和 Eaton 一樣，列舉許多缺乏全國辨識身分系統可能產生的問題，例如冒用身分、逃漏稅、遺棄小孩等等。但是他只處理詐欺、貪腐和僞造身分的辨識系統的問題，而不處理爲了健全全國身分辨識系統而必須設置許多的檢查點和國家必須進行的監視問題。同樣地，保守主義者 David Frum 和 Richard Perle 贊同 Etzioni 的看法，強調公共利益，他們在 An End to Evil: How to Win the War on Terrorism 一書中，針對外國恐怖主義的問題提出看法。他們認爲許多恐怖份子都是非法居留的，因此全國性的身分辨識系統可以將這些恐怖份子驅逐出境。[42]另外，Progressive Policy Institute 是一個附屬於 Democratic Leadership Council 非營利性智庫。它發表許多支持全國性身分辨識系統的文章，這些文章一樣對於在全國性身分辨識系統中控制冒用身分、貪腐和僞造證件的困難性一事，絕口不提。他們省略了這個系統運作所需的檢查點和國家監視問題，更不提對自由和民權的影響。[43]

或許，人們在進出一些敏感的地區時，應該被識別身分，例如登機、進出火車站、購物中心等。拒絕出示身分辨識證件有時候的確太過於個人主義，尤其是當整個國家正處和恐怖主義的對抗當中時，更是如此。

然而，有些人也認爲事實並非如此，政府在檢查點要求人民識別身分只不過是一個以安全作爲主題的儀式，唯有停止這種儀

AND THE NATIONAL ID CARD DEBATE (1986).

[42] DAVID FRUM & RICHARD PERLE, AN END TO EVIL: HOW TO WIN THE WAR ON TERRORISM (2003).

[43] *See, e.g.,* Shane Ham, *Winning with Technology*, BLUEPRINT MAGAZINE, Jan. 2002.

式，我們才可以找到真正確保安全的方法。雖然廣泛的身分辨識可以使得人們守法，但是卻無法影響恐怖份子。這種身分辨識政策，只有在恐怖份子的身分是已知的情形下，才能發揮作用。亦即這種對於識別的要求和廣泛的監視，並無法透露恐怖份子的計畫。雖然安全和反恐是採取身分辨識政策的主要理由，但是大部分的辨識都是不需要也無助於目的達成的。一般性的檢查旅客只會造成守法旅客的不便，對於安全的目的沒有太大助益。

單純地辨識個人的身分，並無法得知該人是否會從事何種犯罪行爲。單純地辨識身分，無法確保這個人會是誠實、循規蹈矩的。911 的恐怖份子事實上並未掩蓋他們的身分，他們用旅遊簽證進入美國，使用本名開設銀行帳戶。恐怖組織固然會使用僞造或變造的證件，特別是護照，做爲國際往來的文件，但是僞造的身分辨識，卻根本不是 911 事件恐怖份子計畫的一部份。[44]

有一些恐怖份子的攻擊，會使用匿名做爲他們的行爲模式。但是造成最大傷害的恐怖份子，往往不在乎被識別身分。現在在中東最盛行的恐怖份子攻擊，「自殺炸彈客」，就具有這種特質。換言之，匿名並不是恐怖攻擊活動的重點，因此，剝奪一般人民匿名的權利，並不會減少恐怖攻擊。

二、911 事件之後的身分辨識政策發展

在 911 事件發生後，加強身分辨識系統這項政策，是美國政府大力推動的政策。在 911 事件發生沒多久，國會就通過 the Aviation and Transportation Security Act，建立運輸安全局以取代長久以來由航空公司和承包商管理的機場。國會設立的 the

[44] *See generally* THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES (THE 9/11 COMMISSION REPORT) (2004).

National Commission of Terrorist Attacks upon the United States，則是在 2004 年發表一份報告，指出爲了防範恐怖攻擊，應該標準化全國駕照的核發和識別功能。這份報告影響了 the Real ID Act 的制訂。

事實上，加強和集中式的身分辨識系統，並不見得是對抗恐怖攻擊的好方法，例如英國的 Privacy International 組織，在 2004 年發表的報告指出全國性的身分辨識系統與恐怖攻擊間沒有什麼關係。[45]然而，由於一般人認爲識別可以增進人民負責和守法的直覺，所以其仍然影響人們處理恐怖攻擊的方式。

使用飛機做爲一種攻擊的武器，是前所未見的，當然也出乎大加的風險評估之外。聯邦飛航委員會的一般政策，要求乘客配合劫機者的要求。將飛機作爲攻擊的武器，所會造成的傷害，比單純地將飛機在空中炸毀來得大得多。而政府根本未對於這種攻擊行爲擬定預防的方式。這也是恐怖份子會成功攻擊的重要原因。

降低風險的辦法包括加強駕駛艙門的鎖、登機前新的檢查程序、以及加強乘客和空服員對抗威脅的能力，這些方法都可以降低風險。甚至是加強維護空服員心理狀態的穩定，確保他們與恐怖份子的距離，都可以進一步減少風險。一個好的風險控制方法會將焦點放在危險和風險本身上，而不需要留意何人會引起這些危險，而且這些降低危險的方法，往往是在任何犯罪者被辨識身分之前，即已降低風險。

加強駕駛艙門的鎖，是使任何人都無法輕易進出駕駛艙的方法；加強空服員和乘客對抗威脅的能力，根本就不論這些威脅者是誰。這些方法可以有效降低風險，而根本不需辨識個人的身分。

在犯罪者的身分是已知的情形下，身分辨識系統是很有用的

---

[45] Privacy International, Mistaken Identity: Exploring the Relationship between National Identity Cards and the Prevention of Terrorism (2004).

對抗犯罪的工具。然而對抗恐怖攻擊，往往不是對付已知的恐怖份子，而是必須在攻擊前瞭解何人是恐怖份子，以及他們的計畫爲何。只要我們知道恐怖份子的行動和身分，可以很容易的找到他們的行蹤。因爲現代的科技，有很多追蹤人的方式，這些方式包括信用卡的使用記錄、網路使用記錄等。

根據美國政府 2003 年 9 月發佈的 Homeland Security Presidential Directive 6，設立了 the Terrorist Screening Center，並且賦予這個中心檢測恐怖份子的任務。這個中心保有一個恐怖份子的資料庫，這個資料庫主要由很多恐怖份子名單組成，資料的來源包括 the National Counterterrorism Center 和 FBI。這個資料庫所包含的個人，是已知或有可能被懷疑與恐怖行動有關，或幫助恐怖攻擊之人。

美國政府沒有辦法在外國追訴恐怖份子，而且外國人在美國也無法享有和一般美國人一樣多的基本權利，所以在邊境透過名單比對的方式，阻止有嫌疑者入境是可以接受的行爲。但是若是在國內使用這種名單檢測國人，這種作法會與美國禁止政府對無犯罪嫌疑者搜索的傳統相左。

不過，在邊境過濾篩選恐怖份子的方法，其成效是有疑義的。這種名單可以篩選出恐怖份子，必須是恐怖份子自願使用他們受到懷疑的身分出現，並接受檢查。此外，恐怖組織也可以透過政府查驗身分的行爲，瞭解哪些成員是受到政府懷疑的，進而由那些未受懷疑者進行恐怖攻擊。在 911 事件中，他們選擇那些從未與恐怖行動有關者進行攻擊。因爲恐怖攻擊所需的人很少，這種透過名單想要找出恐怖份子進而阻止恐怖行動的策略，對恐怖組織而言功效有限。因此在機場廣泛的辨識個人身分，並比對名單的行爲，或許只不過是爲了使旅客對航空安全更有信心而已。

但是，這種使大眾產生一種安全假象的方式，除了將美國民

眾當成小孩一般安撫之外，事實上可能隱含一個危機：會使得美國民眾在發現真相後，對政府失去信心。透過廣泛的身分辨識機制，希望建立的安全假象，一旦最後被民眾發現其根本無用，民眾會對政府失去信心。

另外一種支持使用身分辨識以對抗恐怖主義的論點，認爲身分辨識使得政府得以監視人民的行動，而在恐怖活動籌畫之時，及早發現該行動，予以阻止。在 2002 年初，美國國防部的 Information Awareness Office of the Defense Advanced Research Projects Agency 開始一個 Total Information Awareness program，這個計畫大量蒐集關於每個美國人的各種資訊，並分析個人爲犯罪行爲的可能性。這個計畫以侵害隱私爲由，遭到強烈的反對，美國國會也在 2003 年終止對這個計畫的補助。但是類似的計畫卻正在籌畫和進行中。這類的計畫認爲，藉由資料庫和運算技術，我們可以在眾多的資料中，得出個人爲犯罪行爲的可能性高低，藉此找出恐怖份子。

這種資料分析在某些情形下是具有一定效用的。例如行銷者透過分析消費族群的行爲，可以有效地銷售其商品。但是分析一個族群的消費習慣，與分析個人的行爲不同。因爲消費者的行爲有一定的模式可循，同時可以分析的樣本總是非常多。相反地，恐怖攻擊活動爲了出人意料，往往都沒有一定的模式，再加上恐怖攻擊發生的頻率不多，可供分析的樣本也較爲缺乏。既然恐怖活動缺乏一定的行爲模式，想要透過資料分析找出恐怖份子的努力，也只是徒勞無功的嘗試。行銷者基於錯誤的資料分析所爲的行銷行爲，可能的後果只是浪費一些成本，將郵件寄給沒興趣者而已，但是若用這種資料分析的方式尋找恐怖份子，不但錯誤率會使得國家花費大量的成本，同時也會影響一般人所享有的自由權利。

另外一個支持廣泛身分辨識的理由，就是這種身分辨識和監

視，將有助於犯罪鑑識。但是將身分辨識用於犯罪鑑識，身分辨識不會是一種預防犯罪的方式，而是在犯罪行爲發生後，找尋犯罪者的方式。然而，以往所使用的在犯罪行爲發生後，用來找尋犯罪者的方法，並沒有任何缺點。例如：在 911 事件發生後幾天，恐怖份子的身分，便已經是眾所周知的事情。因爲恐怖份子爲了表示他們的不滿，往往會在行動中表明他們的身分，以吸引大眾的注意力。當然有些情形是恐怖份子的行動，因爲某種錯誤原因，而無法表示行爲者的身分，此時監視攝影器或許可以幫助我們追查他們的身分。但是在社會建立廣泛的監視系統，只爲了在恐怖份子失誤時，可以辨識他們的身分，顯然太過浪費。

在 911 事件後，美國政府積極尋找對抗恐怖份子的方法。擴大身分辨識系統就是這種政策之一。這種擴大身分辨識的政策，不但花費更多的成本，也犧牲了個人的隱私。當我們被要求表示身分時，我們應該先瞭解，到底是誰在詢問我們的身分。之後我們必須考量被辨識可以換取的利益爲何，最後我們決定是否被他人辨識。當然我們必須準備好拒絕被辨識，這種拒絕有時可能會使交易的對象必須考慮是否與我們進行交易。如果個人同意被辨識，我們必須考慮想要與他人建立多深的關係，藉此決定透露多少識別符碼。雖然拒絕被辨識，可能會對個人的生活帶來許多不方便，但是爲了更自由的生活，必須有足夠多的人拒絕隨時被辨識，這才能使政府和其他機構開始改變他們的身分識別政策。

肆、恐怖主義預防與生物特徵身分辨識系統的結合：代結語

生物特徵身分辨識科技目前的發展高峰，可以說是多半藉助於高度的恐怖主義預防心態和作法，而晶片護照結合生物特徵身

分辨識科技，則是當代預防恐怖主義的代表作。自 2006 年年初起，美國、澳洲、紐西蘭以及新加坡等國政府在舊金山國際機場、樟宜機場和雪梨機場等地，開始進行一項電子護照的實地試驗計畫。這個計畫是屬於美國國土安全部（Department of Homeland Security，簡稱 DHS）所屬之 US-VISIT (United States Visitor and Immigrant Status Indicator Technology) 的一環，參與這項實地試驗計畫者，包括美國持有電子護照的外交部門人員、新加坡航空人員、以及澳洲及紐西蘭持有試驗性電子護照的官員及一般人民在內。這種電子護照內配置存有個人資料和生物特徵資料的晶片，根據這些資料提供入出境美國時必要的身分認證檢驗工作。

究其實際，這種電子晶片護照是由美國國土安全部針對打擊僞造、盜取個人資料、恐怖主義之 US-VISIT 計畫下之簽證豁免計畫（Visa Waiver Program，簡稱 VWP）所提出之重要措施之一。目前共有二十七個國家參與 VWP。參與這項計畫的國家，其人民可於 90 日內，以免簽證的非移民身分進入美國，從其設計理念來看，可以很清楚地推知：這項計畫的進行，有賴各國政府共同採行晶片護照系統，做爲通關控管的機制。因此，這項計畫可以達成的附帶目的之一，也在於促成各國政府發展符合國際民航組織（ICAO）制訂的規範所要求的電子護照標準。過去幾年來，ICAO 發布了各項標準，其中包 ICAO 9303 標準在內，這項標準以「機器可判讀旅行文件」（Machine Readable Travel Documents (MRTDs) 應該具備的標準爲主要內容，亦即 ICAO 規定用於 MRTDs 的非接觸式 IC 晶片，必須符合 ISO/IEC 14443 當中所訂定的 Identification cards、contactless integrated circuit(s) cards 和 proximity cards 等標準。同時，ICAO 的標準也要求使用公共金鑰系統架構(Public Key Infrastructure，簡稱 PKI)，以電子簽章方式防止資料遭到竄改。

這項計畫其實是先前 2005 年 6 月在洛杉磯國際機場和雪梨機場所進行的晶片護照計畫的後續延伸計畫，兩者的目的，其實不

外乎藉此發展出完善的晶片護照運作系統。根據 DHS 在 2006 年年初所做的統計，已經有超過 4 千 6 百萬人次的觀光客，透過 US-VISIT 計畫進入美國，在此同時，透過該系統的生物特徵身分辨識技術，也攔截近千位個罪犯或者非法移民者。

如前所述，美國的民權組織和、隱私保護團體甚至消費者保護團體，對於晶片護照的採行抱持頗爲保留的態度，其中美國民權聯盟(The American Civil Liberties Union，簡稱 ACLU)公開發表聲明反對，針對國務院就晶片護照計畫所提出的行政規則 70 Fed. Reg. 8305-8309, "Electronic Passports," RIN 1400-A893 予以批評，認爲這種晶片護照不但侵害人民的個人隱私，不僅無助於而且反而會使人民陷於恐怖份子與罪犯的威脅之下，但在此同時，卻只能提供低度的安全維護而已。其中頗值得注目的是，ACLU 建議捨棄非接觸式晶片，採用接觸式晶片(contact chip)，也就是改採必須透過與讀卡機接觸而讀取資料的晶片，才能有效保障護照持有者的隱私。

換言之，目前美國的晶片護照，是規劃使用 RFID 科技。RFID 是一種廣泛運用於快速收費票口以及大樓入出管制等用途的無接觸式感應晶片，其具有遠距讀取資料的功能，同時也附有追蹤功能。由於晶片護照的法律基礎即 2002 年制訂通過的邊境安全加強法(The Enhanced Border Security Act of 2002)，要求護照提供可供機器辨識的生物特徵資料，但是並未強制規定要使用 RFID 做爲其技術基礎，所以，ACLU 乃建議以接觸式晶片做爲技術基礎，既符合 2002 邊境安全加強法中的規定，而且又比較能保障護照持有者的資訊隱私。

換言之，RFID 的主要技術目的，便是能夠提供遠距離資料讀取，即使主張使用 RFID 者認爲這些資料不可能遭到解碼，但是，只要有 RFID 機器者，便可以很容易地擷取到晶片護照內所儲存

的資料，無論這些資料是否有受到密碼保護，均無不同。根據國際民航組織 ICAO 在 Use of Contactless Integrated Circuits In Machine Readable Travel Documents 這份書面報告中所提出的意見：資訊安全的考量，絕對是採行晶片護照時最重要的管制面向考量之一，而 RFID 的訊號在超過一公尺以外的距離，仍然可以接收得到，這個事實是不容忽視的事實。至於美國國務院準備採用的 RFID 技術系統，其可接收範圍則是達到三十公尺，而非如其所宣稱的只有四英吋的訊號距離。在這種情況下，持有此種晶片護照者反而很容易便成爲恐怖份子或者外國政府鎖定的鏢靶目標。再者，由於此種晶片護照內含極有價值的資訊如個人出生年月日等，一旦取得此類資訊，就可供追蹤取得個人出生證明。

同時，國務院主張晶片護照中將安裝防盜裝置，故而安全無虞。不過，無論是相關領域的學者專家或相關倡議團體，都認爲目前仍無法確定這種防盜拷裝置的可靠性如何，因而抱持反對貿然採用晶片護照的立場。甚至，ACLU 也針對這一議題，發表了一份討論 RFID 潛在危險的白皮書（全文可參見 www.aclu.org/passports），主張在 RFID 技術的安全性被充分證明不具疑慮之前，不可貿然採行這種晶片護照。

除了資料直接外洩危險以外，RFID 技術在資料傳輸到讀取機的同時，還有可能被第三者側錄擷取的危險。美國國務院針對此一一律，提出辯護，認爲要在機場或海關裡拿出機器盜錄資料極容易被發現，所以現實上不可能有這種危險。相對地，ACLU 則以三點理由反駁，第一、隨科技發展，盜錄機器製作日益精良，可預見其體積越小而功能越強。第二、國務院忽略了邊境控管可能發生的盜錄行動。根據 ICAO 科技諮詢小組在 Biometric Deployment of Machine Readable Travel Documents 此一報告中指出：這類晶片護照內所含的身分資料，可做爲其他識別用途使用，例如銀行開戶證明或是用以預定旅館房間，而當這些護照作一般商業用途使用時，就很容易發生不管是直接盜取或測錄晶片資料

的危險。第三、國務院認爲沒有授權解碼鑰匙的讀取機器將很難進行資料測錄，但是，事實上，授權解碼機制，只是幫助資料讀取者將加密的資料還原成可讀的原始資訊，但仍無法防止資料外洩，不論資料是否加密，都不會有太大的不同。

最後，除了本身具有資訊隱私外洩的危險之外，ACLU 認爲 RFID 技術本身還隱含許多安全缺失。首先是晶片失效的風險，根據 ICAO 指出，目前 RFID 晶片只有 2-3 年壽命，美國政府目前也正在實驗如何讓晶片延長壽命到 5-10 年。換句話說，任何有意破壞者，也可以直接癱瘓晶片功能以破壞晶片護照所建構的安全網絡。其次，晶片護照運作不穩定的結果，將增加旅客以及政府部門在各相關方面所支出的成本。同時，資料複製的問題也是受關切的重點之一，因爲晶片護照上儲存了所有的護照持有者資料，包括持有者相片，所以也非常容易僞造護照。再就成本考量來說，根據 ACLU 在 2003 年的一項報告指出，晶片護照的製作成本將爲每本 6-10 美元，高於現行使用護照的每本 2.4 元，而在目前晶片護照耐用性尚待突破的情況下，可以想見成本將高於此。簡言之，ACLU 認爲：內建生物特徵身分辨識功能的晶片護照，只能提供相當有限的國家安全維護功能以及經濟效益，以此與維護個人隱私以及護照系統維護成本作比較，目前不應該是使用該種晶片護照的好時機。

以上這些辯論，都不是在生物特徵身分辨識科技掛帥和對抗恐怖主義的迷思下，便不具有重要性的辯論。相對地，或許是我國在積極進行結合生物特徵身分辨識系統和晶片護照系統的建置工作時，更應該積極去理解和釐清的爭議。

第四章　英國制度沿革與實踐現狀

壹、相關法案

一、Identity Cards Act 2006

二、Immigration, Asylum and Nationality Act 2006

三、Immigration And Asylum Act　1999

四、Anti-terrorism, Crime and Security Act 2001

貳、法案沿革與政府政策

一、Identity Cards Act 2006

在 1939 到 1952 年間，英國基於全國註冊法（National Registration Act 1939），存有身分證的制度，以維護國家安全及戰時物資配置。但在 1951 年全國註冊法取消之後，該身分證的制度隨即廢除，往後數年間雖有類似法案的提出，但皆未果[46]。

這次身分證政策的想法，是在二○○二年二月由內務部大臣 Rt Hon David Blunkett 所提出。隨即內政部在二○○二年七月至二○○三年一月之間進行對權利卡及身分濫用的討論，並於同年十一月發表相關報告。在此同時，內政部亦提出了建立國家身分證強制取得基礎的計畫─「身分證：下一步驟」（Identity Cards: the next steps）。五個月之後，政府即就該計畫爲基礎提出身分證草案，並

[46] See Sixth Report：Identity Card Technologies: Scientific Advice, Risk and Evidence

積極予以推行。但該草案在下議院進行至二讀階段時，由於國會因大選而解散，故法案亦告失敗。新的草案在二○○五年五月提出，其內容與前一版法案非常相似，並最終在二○○六年三月得到了皇室的御准[47]。

表 4.1：法案沿革大事紀

2002. 6	內政部開始對權利卡及身分詐欺部分的研商
2003. 1	內政部完成商議
2003. 11	政府回應內政部商議報告，發表身分證：下一步驟（Identity Cards: Next Steps）
2004. 4	政府發表身分證相關草案並開始關於草案的研討
2004. 7	下議院內務部針對身分證提出報告（Fourth Report of Session 2003-04, HC 130）
2004 .10	政府對內務部報告做出回應
2005. 11	第一版草案的提交與一讀
2005. 4	由於國會解散，身分法草案失敗
2005. 5	提交新版身分證草案
2006. 3	身分證草案獲得皇家御准

[47] See IDENTITY CARDS ACT 2006, EXPLANATORY NOTES

2006. 4	建立身分證與護照系統（Identity and Passport Service ）

能夠證明本身的身分在現今生活而言乃爲一項基本的需求。在每次旅遊、銀行開戶、申請社會福利、甚至加入圖書館時，都會需要確定該人身分。而目前的身分證明系統，乃藉由其他文件，諸如駕照等來確定其身分。但這樣的制度將使不同的機構使用不同的證件來確定個人身分，而多項證件亦容易被僞造或改變來取得假身分，罪犯也會偷得該類證件使用之。而這樣的情況將使恐怖主義份子可經由多重身分來隱藏其犯罪活動，而護照等證件有可能被發放予錯誤之人，公共服務亦有受到濫用可能。是故英國需要一個健全且安全的方式來確定個人所宣稱的身分乃爲真實。

而近期的科技發展，尤其是生物辨識技術，已使得一項更有效且安全的身分計畫乃爲可能。生物資料在世界各國已開始被使用於護照以及邊界移民控管等，諸如美國、歐盟、國際航空組織等。故英政府必須回應這些改變，引入生物辨識技術來加強邊界安全、護照正確性等。故已有生物護照之發放措施。而這意味著百分之八十擁有護照之英國國民將會註冊其生物資料，未來只要藉由本法，取得百分之二十之國民生物資料，即可對英國社會及國民在身分辨識方面皆取得更高的利益。

二、Immigration, Asylum and Nationality Act 2006

此法案乃於二○○五年六月二十二日提交於下議院，並於七月五日進入二讀階段。在二○○五年十月十八至二十七日間經由下議院常務會員會詳細審查，並改進修正之。於十一月十六日進行三

讀通過，並於十二月間提交上議院[48]，該法並於二○○六年三月三十日得到皇家御准。

本法根據兩項政府發表之提案而成，一爲控制邊界（Controlling our borders），此乃於 2005 年內政部就難民及移民所作出的五年計畫；一爲在安全英國中的自信社會（Confident Communities in a Secure Britain），其於 2004 年發表，乃爲內政部 2004 年至 2008 年間的政策計畫。

政府承諾將快速的落實其對難民及移民的五年政策，當中關鍵的條款必須經由立法賦予基本基礎始可落實，而該立法亦令部分政策能獲得更廣泛的實踐。其亦包括一些條款，能令政策的執行更加容易，且該系統亦更透明化[49]。

三、Immigration And Asylum Act　1999

政府在一九九八年七月二十七日所發表的白皮書,「迅速且安全－關於移民與難民的當代方式」（*Faster And Firmer - A Modern Approach To Immigration And Asylum*）乃爲一九九九年移民與難民法的立法基礎。該白皮書之立意乃在於使移民與難民系統現代化且整體化。本法的整體目標乃在於發展更彈性且流暢的移民控管制度，好提供英國公民以及有資格進入或居留於英國之人更高品質的服務，同時也對沒有此等權利之人進行更好的控管。

四、Anti-terrorism, Crime and Security Act 2001

本法目的乃在是在提供政府面臨 911 事件發生之後對恐怖主義的新興局面，希望在各領域能皆有足夠的權力來對付英國可能面臨的威脅而生之立法基礎。相關手段措施包括：切斷恐怖份子

[48] See http://www.ind.homeoffice.gov.uk/lawandpolicy/legislation/

[49] See IMMIGRATION, ASYLUM AND NATIONALITY ACT 2006, EXPLANATORY NOTES

資金來源、確保政府部門機關能收集並交流對抗恐怖威脅所需的資料、增進相關移民程序效率、加強可能會作爲恐怖份子目標或工具的危險物品安全管理、擴展警力至相關程度、確定英國可達成歐洲在警方及司法合作和反貪腐的義務、使英國反恐怖的權力合乎現代要求。

參、法案內容

一、Identity Cards Act 2006

（一）設立目的

本法設立之目的，在第一條第二、三項中規定，乃爲提供個人就驗明正身之要求，一項方便證明自己身分的方式；並在公共利益要求辨認個人身分時，提供可靠安全的方式爲之，故有身分證之設立。此處的公共利益，包括預防或偵查犯罪、確保國家安全、落實移民控管、維護公共服務條款的有效性以及核實對於非法工作或雇用的禁止。

（二）生物特徵的取得

1.　管理人

國務卿（Secretary of State）依照第一條第一項的規定，乃有建立註冊中心(the National Identity Register).並落實計劃之責。

2.　生物特徵取得對象

第二條規定，原則上有權爲註冊登記之人，乃爲十六歲以上並屬於英國國民之人以及經由國務大臣以規章規定的居住於英國之人，而目前規章訂定包含在英居住三個月以上之人。同條第四項規定，在與該法案目的一致情況，可能例外的容許未提出申請

或不符申請資格之人資訊之登記。例如在申請難民庇護未通過之人，該個人資訊的儲存，可能在將來可用來比對避免其以不同身分再次提出難民申請。

3. 資料範圍

第三條第一項規定，該資料只能在與註冊目的一致時，登記並保存於註冊中心。第五條第六項則規定，除非與第一條第三項所規定的目的一致，否則不得要求個人提供資訊，若超出該規定範圍，則需有新的立法基礎始可。

第一條五至八項，進一步釋明什麼樣的資訊可能會被登記註冊，包括了個人姓名、出生日期、出生地、國籍、性別、移居狀況、地址、個人外部特徵。而在第六項中因配合 1998 年的個人資料保護法，就敏感性資料，例如種族、種源、政治意見、性生活、前科等資訊乃不得記載登記。

在該法附錄的列表一，規定將會被記錄於註冊中心的資訊，包括－

(1) 個人資訊：姓名、出生日期、出生地、性別、地址。

(2) 辨識資訊：照片、簽名、指紋、其他生物特徵。

(3) 居住狀況：國籍、留置許可、該留置許可的期限與條件。

(4) 個人編號：例如註冊中心所核發的編號、其他機關核發編號、相關證件有效期間。

(5) 記錄歷史：先前記載的資訊、改變的情況等。

(6) 註冊及身分證歷史：申請日期、資料改變、確認情況、其他身分證已發放的情形、依照第十一條所爲的通知與證件交還。

(7) 批准資訊：申請註冊、修改、確認時所提供的資料，其

他關於確認申請資訊正確性之資料、確認是否已註冊過之紀錄、修改的通知等。

(8)　安全資訊：個人身分號碼、密碼、對於確認修改人身分所提出的問題及答案。

(9)　提供資訊紀錄：如何及何時提供個人或團體相關資訊的紀錄。

4.　資料取得方式

此法經由身分證或其他指定證件如護照的發放，取得該人生物資訊。相關條文規定如下。

第五條規定，身分證的申請可經由選定證件的申請一併爲之或者單獨爲之。

在第四條規定國務卿可經由上下議院的肯定決議，定出有關被選定證件之規則，並依照第五條第二項的規定，就該選定證件的申請，必然包括對於身分證的申請。但依照第六條第七項的規定，在二○一○年一月一日前的護照申請，乃爲例外。

第六條第七項亦規定，除非申請是在二○一○年一月一日前提出，否則就選定證件的申請（例如護照申請）必需同時包含對身分證的申請。第八項指出，身分證的申請應該依法定的方式，向國務卿或者選定證件方發放機關提出。

至於法案第七條則規定了身分證的強制發放，在該條第二項中規定，個人所持身分證即將過期失效，或者未持有身分證者，必須在法定的時間內申請之。而第三、四項中規定，爲了令國務卿得以確認其所提供的個人資料是否正確，其將有權利要求個人在同意或未同意的時間及地點中出席，收集並登記該人照片與生物特徵，及其他與本法目的一致的規定資訊。違反本條規定者，將被處以一千元英鎊以下的罰款。

（三）資料管理

1. 更正與取消

第十條第一項，要求身分證持有人，在其規定的範圍之內，對其個人資訊有所更動或本身已知的錯誤必須在法定期間內通知註冊中心，諸如住址或姓名的更改等。此將有助於維持註冊中心資訊的正確性。同條第二項則要求當事人通知變更或更新資訊時，必須提供進一步的資訊以確保其爲真實，諸如再一次的照相、取得生物特徵或提供其他必須資訊等。違反該條的規定將會被處以一千元英鎊以下的罰款。

第十一條第一、二項則規定，當持卡人發現身分證被偷、遺失、遭竄改、毀損的情形時，必須通知註冊中心或其他法定人員，並在身分證基於錯誤資訊而發放、或者如同上述發生遺失、竄改、毀損等情形時，該身分證則將被取消。

2. 資料的流通

第九條則規定，註冊單位以及發放選定證件部門，可基於確定其將要註冊或已註冊的資訊是否正確之目的，交換其所儲存之資訊。在此只限於此種應用此可得分享所持資訊，不能因爲更廣泛或與確認目的不相干的理由而從事交流。

第十二條則規定，國務卿可在當事人同意的情況下，提供他人註冊中心的相關資料。但其所提供的資料乃是受有限制的，該條第三項即列出即使獲得當事人同意，仍然不得提供之資料包括，指紋或其他生物特徵資訊、密碼、安全號碼等。而隨著各種不同的情況需求，其所限制的範圍亦會改變，例如就變性人方面，其可能就會有不同的限制需要。而該項資料提供，亦不得違反相

關法令，例如 1998 年的個人資料保護法等。

第十七條第一項規定，只要在本條授權範圍之內，在不違背第二十一條使用未經他人資訊之原則的情況下，皆可提供個人資訊。第二項即規定就國安及情報機關，在符合該機關目的的情形之下，將可提供相關個人資訊。第、三、四項則規定，就警察首長、稅務管理局等單位，爲偵查犯罪、保護國家安定等目的，得提供除了審核資訊(audit log information)以外的個人資訊。

第十八條第二項規定，基於 2001 年反恐法的規定，其將可提供相關資料予國安或情報單位等，第四項則規定，在偵查或預防重大犯罪時，可提供個人的審核資料(audit log information)，在這裡由於審核資料所需的門檻較一般個人資料來的高，故其所規定的乃是重大犯罪的情形。其他如改正不正確或不完全的資料或藉由其他條文的規定，亦有可能提供個人資料。

第二十一條規定，在沒有經當事人同意提供資訊時，依照前述規定提供附表一的相片、簽名、指紋或其他生物資訊時，其必需遵守下列原則。首先，在第一項指出，在要求資訊機關本身有其它方式獲取該項資料時，其不可要求註冊中心提供之。例如，若警政機關要求註冊中心提供指紋，則其應先就本身資料庫進行搜尋而未果後始可爲之。註冊中心亦可增加其對該機關的要求、或令其列明可得請求資訊的職位等級。

第三十四條規定容許基於確認發放或撤回護照時之資訊是否正確，而爲之資訊分享。第一、二項規定個人乃具有義務，在申請護照或做出撤銷護照決定時，提供國務大臣相關資料，以確認其正確性。而這樣的要求，在國務大臣命令的目的範圍內，亦可能向各大臣。政府部門、北愛機關、威爾斯議會等其他機構提出。個人該提供資料之義務，將可能經由民事法庭程序強制之。而對政府部門的要求，則將依一般公法救濟程序，例如司法審查等方

式處理之。

（四）監督機關

第二十四條規定，應設立國家身分計劃委員（National Identity Scheme Commissioner），監督身分證計畫及註冊中心就身分證的應用及對登記資訊的提供。就其第一項的規定而言，國務卿乃負責建立該委員會。同條第三項的規定闡明，該委員會不但要審理相關異議，亦應就資料處理的保密性及公正性，審理註冊中心之應用情況。第五項及第七項則指明了應由國務卿負責提供委員會執行其功能所需的相關資訊與人員配置。而該委員會依第八項的規定，乃爲 2000 年資訊自由法之目的而設的公共機構。而依第二十五條，國家身分計劃委員會應於各計畫年度結束之時，向國務卿提出報告，而國務卿亦應將該報告提交議會。

（五）身分證的使用

身分證法案第六條第一二項中指出，身分證乃是一存有與註冊中心相同之個人登記資料，令該卡可用來確認註冊中心資訊，例如身分證號碼等。

同條三款則指出，身分證只能以加密的方式記載規定的資訊，並有法定的有效期限。第六條第六項則指出，身分證的發放只在個人提出申請，且登記或已登記該個人資訊時始可爲之。而關於身分證內記載的資訊內容、資訊的形式、與該法目的相同而可被記載的資訊之相關規定，皆須由國務卿擬定後，經過上下議院的肯定決議始可成立。

第十三條規定公共服務系統，在其需要確定該人身分以減少公共服務濫用時，可依照第一項的規定，要求當事人出示身分證，或者註冊證明以比對個人身分。且有選擇性的，在其未攜帶證件時，可以提供生物資料與註冊中心比對的方式證明自己身分。但

同條第二項亦規定，關於法定補助之領取或其他免費服務使用的部份，在身分證強制登記實行之前，不能強行要求其出示身分證件或者提供生物資訊比對身分。而第三項則特別強調，不可因該條之規定而強制個人應攜帶身分證，亦不可以其他的理由，強制其隨身攜帶或出示身分證件。

第三十五條就現行護照會被要求出示的情形，做出一連串的修法，令將來身分證就護照具有同樣的效力。例如其在 1989 年足球觀眾法部分，修改原本應出示護照部分，令身分證亦有同樣的旅行證件效力。同樣的修法在 2001 年刑事司法與警察法當中，就煙毒犯離開監獄之後的監控，亦令身分證件得以適用。這一連串的修法，擴展了未來身分證件得以使用的範圍。

（六）相關罰則

第二十五條、二十七條、二十八條、二十九條則分別對持有僞造身分證件、不法揭露登記資訊、提供錯誤資訊、竄改登記資料等行爲列入刑法規範。第三十一條至第三十四條，則就民事罰則部份進行規定，其包含民事處罰的施加情況、處罰對象、對處罰的異議及上訴等。在第三十一條就民事罰則的目的，闡明並非爲了懲罰或增加歲收，而是要確保法案當中的條文能被落實，因此當該未遵行法律或遲延遵行之行爲乃有合理的理由時，該處罰通常會被撤銷。而如何執行該罰則、處罰金額與處罰的時機，則待國務大臣進一步對此制訂執行條例。

二、 Immigration, Asylum and Nationality Act 2006 & Immigration And Asylum Act 1999

1.生物特徵之取得

關於生物特徵取得部份，可分兩部分論述，首先就二○○六年

移居、難民與國籍法當中，其第二十七條第五項，規定爲查明護照或相關證件的真實性，實行該項查核之人可請求被檢查之人提供外部特徵資料，諸如指紋、虹膜、或其他眼睛部位特徵等。

其次在一九九九年的移民及難民法（Immigration and Asylum Act 1999）第一四一條以下就指紋的取得進行規範。

第一四一條規定可由有權之人，包括警官、出入境官員、監獄長官等人對本條適用之人在相關時間內取其指紋。該條第七項並進一步對可採取指紋之人做詳細的規定，包括有－

I. 在抵達英國國境時，由於其無法提出有效的附照片護照，或其他能證明其身分、國籍、公民的證件，而由出入境官員要求爲指紋的取得之人；

II. 被拒絕進入英國國境，但例外的依照 1971 年法案表二段二的規定暫時留置者，若移民官員合理的懷疑其違反該暫時留置許可所要求的住居或向警方報告之條件時，可取其指紋；

III. 移民官員對非法進入、滯留、破壞暫時留制規定、詐欺取得留置許可和其家人已發出遷移命令者，或是國務大臣對非法進入者，或是對將被驅逐者皆可採取其指紋；

IV. 任何依據一九七一年表二段十七而被逮捕之人：

V. 任何請求政治避難者；

VI. 任何受上述人員撫養者，在此包括在英無居留權的配偶以及十八歲以下孩童。

而該指紋取得方式則於同法第一四二條規定，該指紋之取得可由相關授權單位提出書面通知，令該人於發出通知七日後，前往指定地點提供指紋。若該通知無法取得其指紋，則警察機關得在無逮捕令的情況下予以逮捕，並移往取得指紋之處所強制取得

該指紋。

在此部份二○○六年的移民、難民與國籍法分別在第二十八、二十九條的規定，修改１９９９年的移居與難民法，將取得指紋的對象，從原本範圍爲逮補之人擴展爲逮捕以及扣留之人皆可適用。並將原本１９９９年的移民及難民法中，第一四一條的規定略加修改。一九九九年的法案本規定可取得難民或受其撫養家屬的指紋，但該取得必須先以書面通知，指紋之取得至少在通知七天後始可爲之。本法第二十九條則將書面通知後爲指紋取得間隔縮短爲一至三天，在通知後一到三天，其即可要求難民資格申請人或撫養家屬在特定的時間前往特定地點提供指紋。

2.生物特徵之管理

一九九九年移民及難民法中第一四三條規定了指紋必須在一定期間內被銷毀，該特定期間將由國務大臣擬訂規則，在規則不備的情況下，則最多在十年內即須銷毀指紋。而在第二至八項，規定在下列的情形中，指紋必須盡速銷毀：

I. 當事人證明爲英國國民或在英國具有居留權時

II. 當難民確定取得永久進入或居留於英國的許可

III. 在其未有違背短暫拘留條件的情況下，暫時居留者已離開英國時

IV. 第七項 c 款因指令而可採取指紋者，在指令失去效力時

V. 因有驅逐命令而被採取指紋者，當驅逐命令廢除時

VI. 當受逮捕之人被釋放時

VII. 當前述之人資料被銷毀時，撫養家屬之資料亦須立即銷毀

但此部分規定，在二○○一年的反恐怖、犯罪與安全法（Anti-terrorism, Crime and Security Act 2001）當中，進行了修

改，在其第三十六條提到，就前述三至八項的立即銷毀規定就此失效，已經取得或將來取得的資料，都可依原本第一項的規定，保存十年之久。

三、 Anti-terrorism, Crime and Security Act 2001

1.生物特徵的取得

I. 指紋

一九八四年的警察與刑事證據法（Police and Criminal Evidence Act 1984）經過二○○一年的刑事司法與警察法的修改（Criminal Justice and Police Act 2001），已賦予司法警察對於定罪、起訴、警告或其他有合理理由認爲其涉入犯罪之人，在未經其同意的情況下採取其指紋。該指紋的取得，是用來在法院或警局就保釋與否的問題，對其身分產生爭議時爲確認或反駁。也就是說指紋是來確定其是否涉入犯罪，而且指紋的取得亦僅能在相當層級的警官監督之下完成。其不能只是爲了確認其身分而採取指紋，例如目前法律基礎不得對拒絕證明自己身分之人或者對其表示身分有所疑義之人，採取指紋來確定其身分。

在此情況之下，在本法第九十條第二項，即提供了對於被逮捕之人，爲確定或驗證其身分而採取指紋的法律基礎。但同項二款亦規定，除非當事人拒絕表明其身分，或者有理由的懷疑其並非該宣稱之人,否則亦不得直接僅爲了確定個人身分而採取指紋。

在 2000 年的恐怖主義法（Terrorism Act）附表八規定可對依該法羈押之人經警察督察長以上層級之授權，採取指紋以確定其是否從事該法犯罪，或者教唆、幫助或煽動犯罪。

本法第八十九條則對該附表八的規定，增加兩種得採取指紋的情形，首先是在該人拒絕表明其身分或在警察合理懷疑其提供假身分時，警方可在認爲指紋將能辨識該人身分的情況下，由警

察監督長以上的警官授權採取其指紋；其二是在確認該人並非特定人士的情況，例如在警方懷疑嫌犯所聲明之身分並非自身，而是兄弟或朋友時。

II.　相片

在一九八四年的警察與刑事證據法（Police and Criminal Evidence Act 1984）規定中，不具有對疑犯攝錄照片的法律基礎。警察機關僅能對其已定罪、起訴之人照相，亦即其必須確定涉入該犯罪，並存有該犯罪的辨識證據時始可爲之。故當某些人在立刻被逮捕的情況下，想要馬上拍照確定是誰被逮捕，又是在何時何地被逮捕的情況，則無法律可適用。

而本法第九十二條則規定警方，在必要的情形之下，得進行拍照，並可要求其脫下面具或去掉油漆等，以確定辨識其身分。

2. 生物特徵之管理

依照二○○○年恐怖法附表八第十一條的規定，在爲指紋之採取之前，必須告知該指紋採取之目的，以及採取指紋之處所等。在強制採取指紋的部份，亦應告訴其授權採取情形、依據理由、所涉犯罪等。

該指紋依照二○○一年刑事司法與警察第八十二條的規定，爲辨認身分所採取的指紋，無論當事人後來被証明有罪或無罪，皆可保存，但其使用之目的必須與預防或調查、偵查犯罪、進行起訴等目的相關。

至於在本法第九十二條第四項規定所攝照片將在預防或調查、偵查犯罪、進行起訴等目的之下使用或揭露予相關人士，故該照片將可繼續被保存，但僅可就相關目的使用之。

表 4.2：法規重點整理表

	本國人相關法案內容	外國人相關法案內容
資料取得對象	原則上爲十六歲以上並屬於英國國民之人以及合法居住於英國三個月以上之人。	1.需查明護照或相關證件的真實性之被檢查人(Immigration,Asylum and Nationality Act 2006) 2. I. 在抵達英國國境時，由於其無法提出有效的附照片護照，或其他能證明其身分、國籍、公民的證件，而由出入境官員要求爲指紋的取得之人； II. 被拒絕進入英國國境，但例外的依照 1971 年法案表二段二的規定暫時留置者，若移民官員合理的懷疑其違反該暫時留置許可所要求的住居或向警方報告之條件時，可取

	本國人相關法案內容	外國人相關法案內容
		其指紋； III. 移民官員對非法進入、滯留、破壞暫時留制規定、詐欺取得留置許可和其家人已發出遷移命令者，或是國務大臣對非法進入者，或是對將被驅逐者皆可採取其指紋； IV. 任何依據一九七一年表二段十七而被逮捕之人： V. 任何請求政治避難者； VI. 任何受上述人員撫養者，在此包括在英無居留權的配偶以及十八歲以下孩童。（Immigration and Asylum Act 1999） 3.

	本國人相關法案內容	外國人相關法案內容
資料內容	(1) 個人資訊：姓名、出生日期、出生地、性別、地址。 (2) 辨識資訊：照片、簽名、指紋、其他生物特徵。 (3) 居住狀況：國籍、留置許可、該留置許可的期限與條件。 (4) 個人編號：例如註冊中心所核發的編號、其他機關核發編號、相關證件有效期間。 (5) 記錄歷史：先前記載的資訊、改變的情況等。 (6) 註冊及身分證歷史：申請日期、資料改變、確認情況、其他身分證已發放的情形、依照第十一條所爲的通知與證件交還。	1.外部特徵資料，諸如指紋、虹膜、或其他眼睛部位特徵(Immigration,Asyluma nd Nationality Act 2006) 2.指紋（Immigration and Asylum Act 1999）

	本國人相關法案內容	外國人相關法案內容
	(7) 批准資訊：申請註冊、修改、確認時所提供的資料，其他關於確認申請資訊正確性之資料、確認是否已註冊過之紀錄、修改的通知等。 (8) 安全資訊：個人身分號碼、密碼、對於確認修改人身分所提出的問題及答案。 (9) 提供資訊紀錄：如何及何時提供個人或團體相關資訊的紀錄。	
資料管理	身分證持有人，在其規定的範圍之內，對其個人資訊有所更動或本身已知的錯誤必須在法定期間內通知註冊中心，並須提供進一步的資訊以確保其	指紋必須在一定期間內被銷毀，該特定期間將由國務大臣擬訂規則，在規則不備的情況下，則最多在十年內即須銷毀指紋。（Immigration and Asylum

	本國人相關法案內容	外國人相關法案內容
	爲真實。 持卡人發現身分證被偷、遺失、遭竄改、毀損的情形時，必須通知註冊中心或其他法定人員，且該身分證則將被取消。	Act 1999）
資料流通	註冊單位以及發放選定證件部門，可基於確定其將要註冊或已註冊的資訊是否正確之目的，交換其所儲存之資訊。國務卿可在當事人同意的情況下，提供他人註冊中心的相關資料。	
資料監督	設立國家身分計劃委員（National Identity Scheme Commissioner），監督身分證計畫及註冊中心就身分證的應用及對登記資訊的提供。	

從上述的比較可約略看出，經由身分證法案的立法，爲求立

法周延，顯得針對英國國民的規定反較非英國人而言更爲繁複且嚴苛。英國國民由於採用身分證的緣故，經由生物資料的收集、資料庫的建立等，多了許多個人隱私權或相關人權受到侵害的機會。但這樣的情況，隨著二○○七年一月二十五日邊境草案(Borders bill)[50]的提出，未來在英國居住的外籍人士，亦須強制申請含有生物辨識資料的身分證件，並可能在二○○八年率先由在英居住的外籍人士開始強制發放身分證件，於此草案通過之後，在英外籍人士除了面臨予英國國民同樣的隱私權、資料保護等議題之外，則尚可能有新的問題產生。[51]

肆、相關爭議討論

生物辨識技術，概括來看，似乎可被描繪成詹姆斯龐德的一項科技裝備，光滑、性感、且能夠吸引金錢投資。利用個人身上獨一無二的特徵－指紋、眼睛、DNA 等來作確認的技術，是一熱門的選擇，甚至被視爲在身分確認上即將到來的一大進步。然而，其同時有著疑問存在，花費的價值、資訊的可互通性、資料保護、隱私權、私人權利等議題，甚至在現實技術上的疑議皆引人深思。但生物辨識技術於英國的應用部分，目前則以其如火如荼進行中的身分證法案最受矚目，故分就下列幾點對生物辨識技術應用的相關討論予以介紹。

---

[50] http://www.publications.parliament.uk/pa/pabills/200607/uk_borders.htm

[51] 請參見本文肆、三、(二)、3.經由強制發放取得資料之討論。

一、 身分證法立法目的之疑議

反恐戰爭的白熱化，使得身分證法案的腳步加快，然而，不但在內閣當中對此議題有某些人士採取保守的意見，從網站上的民意調查來看，針對該議題所發表的電子郵件當中，即有 97%是反對該計畫的。律師會在 2003 年 3 月邀集各界人士針對該計畫進行討論。

大部分律師認爲，要求每個人就其身分證件註冊，呈現出在個人及國家平衡關係當中的轉移，除非有清楚迫切的社會需求以及補償的利益，否則這樣的變動當然是不受歡迎的。政府應證明從身分證計畫當中所獲得的利益，足以使其對個人自由的侵犯正當化。

由於身分證計劃無可避免的將經由個人資訊的取得，而產生隱私權侵害的風險，故就歐洲人權公約第八條的要求來看，除非首先該系統有可能達成其所指稱的公共利益，否則身分證根本不需要存在，該立法亦不符合第八條的要求。人權聯合委員會同樣也發現在草案的討論以及之前的諮詢報告當中，都曾經對建立全國註冊中心以及身分證制度實際上是否真能就其宣稱的目標產生作用提出質疑。而即使這些目標真符合第八條第二項所規定的範圍之內，委員會亦注意到全國註冊中心及身分證制度與這些目標的關連性及有效性將會與其是否符合第八條規定有極大的關係。而在收集、持有、揭露個人資料的情形，其對個人的隱私權必須是在其需要下最小程度的爲之，其將無其他更不侵犯人權的方式

來達到其目的。[52]

但就英國內政部所作出的研究而言，其並無法證明身分證計畫與其所指稱的目的有任何重要或確實的關聯。內政部認爲身分證計畫將能減少身分詐欺的依據，亦僅是一份十年前的內閣研究計畫。而在近年來其他獨立組織的研究調查則顯示，就恐怖犯罪、詐欺、移民控管等方面，就有身分證制度與無身分證制度的國家相互比較研究，其所得到的結論皆與政府的立論相反。是故，就大部分的研究所得而言，即使政府所宣稱的目的符合第八條隱私權干預的要求，但在身分證的實行根本無法達到其立法目的的情形下亦顯得毫無用處。甚至就算其確實在防止非法移民及就業的方面有所助益，其所產生的影響亦小到不符比例原則。[53]

對此基本上法界對於身分證打擊不法的實效性同樣採取存疑的態度。在沒有社會號碼的情形之下雇用不法員工的老闆，在將來仍然會雇用沒有身分證的員工。而犯罪偵防的問題通常亦不在辨識個人的身分，而是在如何去確定何者觸犯該罪。且即使是在身分證法及資料保護施行良好的西班牙，其恐怖行動仍舊猖獗。

身分證法案也許真能從其所宣稱可得的利益而正當化，但雖然我們被告知該計畫將可對抗恐怖犯罪、身分詐欺、非法移民、降低犯罪...，身分證法案幾乎成了現行社會的萬能藥，但事實上當中沒有一個立論可以在仔細的審核後成立。政府似乎也知道身分證計畫無法對恐怖犯罪有重大的影響，就像是現在他們以恐怖

[52] Joint Committee On Human Rights, Session 2004-05 Fifth Report, 26 January 2005.
[53] David Redmond, Licence to live?, New Law Journal, 24 June 2005.

份子通常會僞造相關證件爲由來延長羈押時間的立法，沒理由恐怖份子不能僞造身分證，除非該身分證真的是不可能被僞造的，否則基本上是毫無用處。而就打擊犯罪而言，極少數的犯罪是因身分認定問題而無法偵破，事實上，偵查的困難多是因爲證據因素，若是要打擊犯罪，有許多更好的方法來花費這龐大的預算。而詐欺犯罪更是只有百分之五是關於身分的問題，更別說該身分詐欺多是遠距進行，身分證件的使用根本派不上用場。

這裡有兩個根本的問題，首先，是否其他具有身分証制度的國家就不會有英國現在所面臨解決的問題；其次，與其將龐大的預算花費在強制身分證計畫中，以該預算來加強警政系統是否會是更好的抉擇。[54]

法界同樣關心隱私權及資料保護的問題。高度個人的資料應受到保護是必要的。這包含了儲存在身分證、註冊中心、以及每次使用證件所產生的資訊皆應受保護。故應須對該計畫的目的及使用資料的限制在立法上有清楚的法規定義。[55]

二、 有關隱私權之爭議

關於將廣泛使用生物辨識技術的英國身分證計畫，關於其分析及討論方面，英國內政部近來多只針對其財政及技術方面地問

[54] Gareth Crossman & Caroline Mortimer, ID cards--exposing criminality or invading privacy?, New Law Journal, 9 December 2005.
[55] Janet Paraskeva, Chief Executive's Column: An Identity Crisis, Law Society Gazette, 22 April 2004.

題進行討論。但就法界人士而言，更重要的部份在於其對於人權的侵犯，包括其可能違反歐洲人權公約第八條對於個人私生活的保護，而該人權公約的內容同時在英國亦於 1998 年人權法案中內國法化。

英國內政部 2005 年身分證法案提出了一個不同於其他歐洲國家，甚至在事實上不同於全世界的系統。其主要的特徵在於其創造了一個將擁有所有 16 歲以上個人之特定「註冊資料」的中央資料庫。內政部認爲多數資訊乃是必要的，且可在其他地方公開的取得，故與歐洲人權公約第八條的個人隱私權保護無涉。這樣的看法受到人權聯合委員會(JSCHR)的反對，其指出當公開可得的資訊受到蒐集及保存時，其即牽涉公約第八條的問題(Rotaru v Romania (2000) 8 BHRC 43, para 44)，甚至在該資訊不會在後來揭露的情形亦同(Leander v Sweden (1987) 9 EHRR 433)。

公約第八條表示除非是在民主社會當中爲了達成某些特定合法目的之必要情形下，否則個人有權令其生活不受干涉。該規定同時受到比例原則的支配，亦即身分證計畫的目的必須與個人隱私權受侵犯的程度相權衡。關於第八條更精密的詮釋會是評估該系統就特定個人族群可能的缺失。舉例而言，少有人注意到關於一些由於其生理特徵而無法適用該系統的局外人。像是在英國 150,000 眼睛失明的人士即造成該系統使用高度的困難，更別說還要加上 61,000 其他特定眼疾的患者。生物辨識資料被宣稱爲某種像是金科玉律（gold standard）的辨識方式，但其實此與事實相距甚遠。令人驚訝的，僅僅是長睫毛以及熱淚盈眶的情形，都會影響到虹膜的掃描，而體力勞動、年齡老化、體重增加或者懷孕也都會影響到指紋的掃讀。若將這些生理因素以及失敗機率的情形

列入考慮，不能一貫的利用該計畫辨識身分的人數，將會增加到9百萬到2千1百萬人之間。

支持生物辨識計畫的英國內政部部長 Charles Clarke 和英國首相 Tony Blair 都曾表示，爲了符合科技以及國際護照標準的潮流，英國使用生物辨識系統乃是非常重要的。然而，這樣的主張並非全然正確，就國際民航組織(ICAO)歷經七年的調查後指出，一個可以機器掃讀、電子儲存個人的臉部照片以供面部辨識即已足夠，此亦爲進入美國的要求。因此就國際標準而言，指紋及虹膜的辨識是不需要的。可以看出內政部在主張其身分辨識系統所將達成的利益方面面臨了相當的困境，因此該提議亦有可能違反第八條的要求。[56]

人權聯合委員會（Joint Committee On Human Rights）在二○○五年一月的報告[57]中提出其對法案條款是否遵守歐洲人權公約第八條隱私權保護及第十四條禁止差別待遇的關切，收集並儲存資訊於註冊中心，並使用該資料確認身分或者向其他組織揭露，將會涉及歐洲人權公約第八條隱私權保護的問題，該條規定－

1. 任何人都有私人及家庭生活、其家庭與通訊受到尊重的權利。
2. 公權力對此不得侵犯，除非是依照法律規定且在民主社會中對國家安全、公共安全、國家經濟健全等利益、預防失序或犯罪、保護健康、道德或保護他人自由權利而言爲必要時始可爲之。

[56] David Redmond, License to live?, New Law Journal, 24 June 2005.
[57] Joint Committee On Human Rights, Session 2004-05 Fifth Report, 26 January 2005.

第八條並未阻止任何種類身分證件的發放。歐洲人權法院認爲發放一包含個人姓名、性別、出生日期與地點、目前住所以及配偶姓名的身分證件，其本身並不會在第八條產生爭論。而要求持有或攜帶該證件的情形亦不會涉及第八條規定。

然而，第八條會在收集及儲存個人資料時涉及第八條的問題。使用或揭露有關私人生活的資訊亦同時與第八條相關。在第八條第二項規定中，該侵犯行爲必須在足夠清楚且可預見其施行的法律規定下爲之，且其必須可達到第八條所列出的某一法定目的，同時該行爲須對其目的而言爲必需且符合比例權衡，是一種對於迫切社會需要的回應。故在第八條下合法的干預，必須使在所需程度中對隱私權所做的最小妨害，且其目的無法以其他更不具侵犯性的方式達成。該法案同時可能涉及歐洲人權公約第十四條的問題，其與第八條結合來看，將禁止在保護隱私權方面不正當的差別待遇。在人權委員會的報告當中，其應用這些標準在法案的主要層面審查上。其特別質疑－

- 個人資料會被作爲登記事項儲存於註冊中心的範圍爲何，以及是否該等資料皆如同公約第八條要求的，符合法定目的與比例原則。
- 在相關人士未得知或未同意的情況下登記其個人資料的可能性，在第二條第四款中其容許註冊中心涵括對內政部在其他方面可得的資料。
- 透過選定證件的方式使得註冊以及身分證的使用對某些群眾來說變成實際上強制的可能性，以及其造成恣意或不符比例違反人權公約第八條要求的可能性，並因差別待遇而違反公約第十四條的規定。

- 逐步強制註冊以及施行身分證制度因其未能達成任何合法目的而違反公約第八條要求的可能性，且因其可能對強制採用制度之人造成差別待遇，違反了公約第十四條的要求。
- 在強制的計畫中，第十七條規定在使用公共服務時註冊中心將向服務提供者揭露的個人資料範圍可能違反了公約第八條的規定，且其缺乏在第十七條中防止非必要資訊揭露的防護措施。
- 在強制的計畫中，公家或私人要求要出示身分證或使用註冊中心資訊以締結契約或提供服務的可能，在第十八條中將沒有足夠防護措施，且其有違反公約第八條規定的風險。
- 在第十九條至而十一條的規定下使政府機關得基於寬鬆的目的要求而揭露註冊中心的個人資料，且經由第二十二條的規定無限制的擴大其揭露的權力，令公約第八條第二項對私人生活的侵犯須以一法制化、符合法定目標且與該目標合比例原則的情形始可爲之的要求受到違反。

而身分證法案在二○○五年五月重新提交到國會的版本，與先前的草案大致相同，但有少許的修正影響人權委員會的看法，故雖然在之前的委員會對此法案已有闡述，但仍在後續報告中予以討論[58]。

在先前的報告中，儘管獲得內政部的回應，委員會仍認爲下列問題有侵犯人權的可能－

- 在法案中建立的全國註冊中心，可能會導致強行保存關於群眾的大量個人資料

[58] Joint Committee On Human Rights, Session 2005-06 First Report, 7 October 2005.

- 其資料保存，無論是在自願或強制計畫中，其皆要求在獲得選定證件時必須登記註冊，將會造成未考慮是否能達成身分證計畫法定目標的問題，而違反歐洲人權公約第八條規定。
- 藉由選定證件的發放實際上對某些人會造成強制註冊的行爲，且該選定證件與身分證法定目標並不相關，可能會有違反公約第八條以及第十四條差別待遇的問題。
- 逐步強制註冊的計畫，將有不合比例的干預公約第八條隱私權的風險，並且可能因不正當的差別待遇而違反公約第十四條。
- 法案中應對註冊中心資料的查核有進一步的保護措施，以確保其未違反公約第八條的要求。
- 可揭露註冊中心資料的廣闊範圍，將導致違反公約第八條的風險，且其在法案中亦缺少足夠的保護條款。

在此次重新提出法案之後，有小部分的規定在上次委員會討論之後進行了修正，諸如－

- 國務大臣依照第四條決定選定證件，現在必須經過立法程序（affirmative resolution procedure）。
- 國務大臣可以命令修改何人應可註冊之年齡權利，移轉到立法程序。
- 經由國務大臣之命令可提供資訊的規定，現改變爲須就公共利益而言爲需要時始可。
- 國務大臣可授權在未經個人同意提供資料與公共機構的情況，現在只能在公共利益而言爲需要時始可。

三、 **個人資料庫之爭議**

（一）總論

英國隱私權的守護者，資訊委員會主席 Richard Thomas，曾指出身分證的引入將會造成國家與個人之間關係的重大改變。即使政府表示「如果你沒有什麼可隱藏的，那麼你也沒什麼好害怕的」，但在隱藏犯罪與保護隱私之間仍然有著極大的不同。每個人都有一些寧願保持私人的事宜。

身分證法案同時引進了一副展品─全國註冊中心，該中心將擁有全國人民的個人資料，且有許多政府機關都可以輕易的進入使用。且無論一開始資料庫所包含的是怎樣的資料，一旦全國資料中心建構完成，則其資料都會戲劇性的擴增。如同在戰時身分證法案施行的情況，一開始其目的只在於徵兵、分配資源以及國家安全，但後來卻如雨後春筍的擴展到三十九種不同的作用。在 1952 年廢除該身分證制度後，如同其首相邱吉爾所表示的，此可謂爲人民的解放。[59]

（二）資料取得

對於某些人而言主要的問題在於生物辨識可能會被使用爲一種監控或社會控制的技術，或者生物資訊可能會在未經同意、未積極參與或甚至未能獲知的情況下被使用。由於生物辨識技術的使用僅能容許低程度的侵犯個人隱私，故特定的保護條款乃是必

[59] Gareth Crossman & Caroline Mortimer, ID cards--exposing criminality or invading privacy?, New Law Journal, 9 December 2005.

要的。

關於資料取得及處理方式的部分，亦關係到比例原則的考量。生物資料只應在適當、相關、非過度的情況下在按照其原始目的的情況下處理。此外，在生物資料方面，特別是原始取得資料，其通常涵括其他對於辨識或確認而言不需要的其他資料，擷取樣版技術方面應建構出排除非必要資料的處理方式（任何被收集的非必要資訊皆應被盡速銷毀）。且個人資料只能在該系統目的所需的情況下被持續保存。[60]資料的處理及收集應以誠實公正的方式爲之。資料主體亦應被持續通知特定的例外情況，例如在事關公共安全的時候。資料主體應獲知該系統目的及其管理人之身分。因此在資料主體不知情的情況下收集資料的生物辨識系統應不被考慮。就此方面而言，遠距臉部辨識、指紋收集以及聲音的錄取呈現出高度的風險。而資料主體的同意，其必須是資料主體自主特定地通知其同意資料處理的意願。**[61]**

在政府提案當中其他涉及人權的瑕疵乃是計畫的逐步施行階段。聯合委員會強調該施行階段將有可能違反公約第八條及第十四條的規定。

依各資料取得方式的不同，可能會面臨不同的問題－

[60] Phillip Rees & Marcus Hughes, Biometrics and border control, New Law Journal, 13 August 2004.
[61] Phillip Rees & Marcus Hughes, Biometrics and border control, New Law Journal, 13 August 2004.

1. 經由其他來源進入註冊系統

> 註冊的內容除了經由當事人自願登記提供之外，在第四條第二項的規定同時包括其他可得的資料，例如是未通過審核的難民申請，其生物資料已有留存，故即可登記於註冊中心。但這種資料的使用並未經當事人的同意或知會，首先可能會造成其法律行爲未明確且可預見的問題，當事人將無法經由法律規定確認其私人生活將會受到何種程度的干擾。其次由於該可得資料的不確定性，其亦無法確定與法定目的相關聯且合比例性，可能會導致與法定目的不相干的資料受到保存。上述兩個問題皆會造成對歐洲人權公約第八條的違反。[62]

第二條第四款指出註冊中心可就其他可得的資訊，即使其未提出身分證的申請，亦可未經個人同意或知情而列入註冊資料。內政部就此舉例像是失敗的難民申請者、將要驅逐出境之人或者是申請生物簽證的外國人等。皆可在其未授權登記或尚未授權登記的情況下，基於國家安全的理由，未經其同意而登記其資訊。內政部表示，依照資料保護法，個人將會在其實際能通知的情況下，告知該資料之儲存。但英國人權委員會仍然認爲如此尚有可能在一些該個人無法被通知，而其資料卻還是在其未同意並不知情的情況下被保留，而涉及了違反公約第八條的問題。[63]

2. 經由選定證件進入註冊系統

---

[62] Joint Committee On Human Rights, Session 2004-05 Fifth Report, 26 January 2005.
[63] Joint Committee On Human Rights, Session 2005-06 First Report, 17 October 2005.

第一位被強迫註冊的人士會是那些想要換發護照或者駕照以及那些在身分證法案第六條中被要求註冊的之人。這可能會被不誠實的被稱爲實行計畫中的先行階段而非差別待遇。內政部主張該方式之所以被選擇乃因同時註冊英國所有人口將會是不實際的。這令人想到法國的情形，其身分辨識系統乃是非強制的，但卻約有 65%的公民皆持有身分證。這或許是因爲該卡對於個人的便利性，或者更諷刺的，該卡會被如此虔誠的使用乃因爲若個人不「自願」則其幾乎不可能得以生存。[64]

經由選定證件的申請，將同時使個人資料登記於註冊中心，而該方式將會對某些具有義務使用該類證件之人造成實際上的強制登記。例如須出示居住許可之非國民、例如在生活上或工作上必須持有護照或駕照之人。此種實際上強制登記的作法，特別關係到歐洲人權公約第八條的比例原則。首先，藉由發放或換發護照、駕照此種武斷的標準來迫使其登記個人資料，無法看出其符合任何法定目的。只要求需要發放或換發護照之人爲資料登記，不像是可以解決諸如恐怖主義、不法移民工作、身分詐欺等困境。同時其也看不出要求換發護照之人登記資料是一達成歐洲公約第八條二項要求公益的適當反應。合比例干擾第八條權利的其中一個條件是須先有相關且足夠的理由來支持該行爲，而人權委員會也不清楚依照誰持有護照或誰需換發護照的標準如何會相關且足夠的使侵犯第八條的行爲正當化。[65]

法案第四條容許國務大臣選定特定的證件，在其證件發放時

[64] David Redmond, Licence to live?, New Law Journal, 24 June 2005.
[65] Joint Committee On Human Rights, Session 2004-05 Fifth Report, 26 January 2005.

必須要求登記資訊於註冊中心。先前的委員會曾指出經由選定證件的方式，將會對某些需要該證件的人而言，該登記註冊成爲一種強制的情形，而在此可能會涉及公約第八條的問題。在評估是否合比例的干預第八條權利時，將會必須考慮是否這些證件的選定，與立法目的有明顯的關係。就這點而言，實在無法看出收集申請護照之人的個人資料，將會與諸如國家安全、預防犯罪或是其他第一條所規定之立法目的相關。人權委員會注意到，自從先前委員會的報告對國務大臣選定證件的權力進行評論，現行的規定已將證件的選定透過立法程序進行。人權委員會對此表示肯認。但仍然認爲，經由與法定目的無關的證件強制註冊個人資料，將會是對第八條權利不適當的干擾，必且有可能造成差別待遇而違反第十四條的要求。[66]

3. 經由強制登記進入註冊系統

既然強制登記註冊將會抵觸到公約第八條隱私權的權利，則其必須確定就強制登記之人而言，該手段乃依照法律規定爲之，爲求達成一法定目的，且該手段對該目的而言是必要且合比例的。同時也必須顯示對該強制登記之人而言，其並未違反公約第十四條的規定，而對隱私權的保護做出差別待遇。

因此指定某部份的人強制登記，必須是符合例如防止犯罪、降低身分詐欺等立法目的，具有相關且足夠的理由採取此一手段。身分證法第六條規定必須註冊之人，若其未註冊則可罰處罰

[66] Joint Committee On Human Rights, Session 2005-06 First Report, 17 October 2005.

鍰，且此會在內務大臣（Home Secretary）每次要求其爲註冊而其未爲時重複罰鍰。而忘記換發新身分證亦會被罰處罰鍰。另外，第六條規定須強制註冊之人若未出示發放的身分證件亦會被拒絕使用公共服務系統。其並未享有其他未強制註冊之人的相同保護，而是必須要攜帶並出示身分證件。

曾有提議認爲在第六條之下需註冊之人中，居住於英國的外籍人士應先行強制註冊。但在只有某些人士被要求強制登記時，實在很難認爲此對預防犯罪等立法目的有必要且合比例的關係。且此可能會導致個人在行使歐洲人權公約第八條隱私權時的差別待遇而違反該公約第十四條的規定，該條規定在社會中的每個人其在公約中享有的權利都應受到平等的保護。種族平等委員會相信在計畫的執行階段會對一些在英國長期居住但依其權利未申請公民身分的群眾造成負面的影響。這二階段的方法可能會落實外籍人士是二等公民，且可以二級公民身分對待他們的看法。政府可能會宣稱其令外籍人士先予強制登記註冊將會有助於移民控管等，但即使此一目的符合第八條第二項的要求，但爲了要確定此爲一合比例、迎合社會迫切需要的手段，其必須證明沒有其他較不侵犯人權的手段，例如要求外籍人士持有其他證件，來達到相同的目的。這裡有各種可在全國實行且較不侵犯人權的辨識方式。一個存有各種提議資料，甚至包含電子照片（如此就符合 ICAO 的標準）的獨立智慧卡，可以省下數十億的經費且就該計畫規劃的利益提供一較合比例的反應。故要求外籍人士強制登記，將會面臨到不合比例的侵犯第八條隱私權的問題，以及第十四條差別待遇的疑議。[67]

[67] Joint Committee On Human Rights, Session 2004-05 Fifth Report, 26 January 2005.

事實上在此沒有任何重要的理由認爲外籍人士應先於其他人民註冊。且在非法移民原本即不會被發放身分證且本身亦不想申請身分證的「消失移民」時，該方式亦無法減緩非法移民的問題。若非法移民被要求在 12 天內於警察機關出示其身分證，他們需要做的是不要去出示，而其即能避開該系統。

要注意的是在第六條規定下的外籍人士乃是合法的居住在英國，但一旦將其指定爲強制登記，則將會重複的要求出示其身分證件，而此構成了第八條隱私權重大的侵犯。再者，該計畫的實施亦會造成現已存在的非法移民加倍的地下化。這樣的待遇可能會是在英國居住且工作多年，甚至其小孩出生於此國家中的非法移民變成一下層階級的人民，摧毀所有社會凝聚的希望。

總之，對社會的某些成員而言，生物資料的掃讀、截停並搜查以及民事的處罰將會僅因其社會身分地位而變成司空見慣的情況。以第一階段將在 2008 年到 2013 年完成，該差別待遇將會持續五年之久。第六條所涵蓋的人士以及那些生理上不夠幸運去進行生物掃讀之人，皆將忍受其第八條所保護的隱私權受到不合比例且持續的侵犯。身分證若在現行提議的規劃下被落實，其將對這些人成爲一個證明可爲生存的證件，不停的需要證明他們是誰，需要去確定其在英國居住的權利以及使用公共服務的要求。而大部分的人民，首先，假設該系統將真能在其宣稱的目標有足夠的影響來正當化其對第八條的侵犯，至少在這「自願」的五年之中，則會受到很小部分的侵犯。[68]

[68] David Redmond, Licence to live?, New Law Journal, 24 June 2005.

（三）資料內容

歐洲人權法院將關係私人生活的資訊定義爲關於特定或可特定之人的任何資訊。而公開可得之資訊在其被系統的收集及儲存時，亦同樣涉及第八條保護範圍。故註冊中心系統的收集且儲存資訊的行爲，即使是在其後並未使用時亦涉及歐洲人權公約第八條的問題。更別說該系統會在之後每次使用時登記其紀錄，例如公共服務系統的使用、可能僱主的查詢、犯罪事件的偵察等，其將會建構出私人生活極細節的部份。而其資料的持有將可在其確認目的之下持續爲之，也就是該資訊可能會被持有長達個人一生的時間或至少是個人居住於英國的時間。而此同樣亦增加了對隱私權的干擾。我們已表明，第八條隱私權的干擾必須是在其行爲能達成第八條目的的情況下，其干擾與目的符合比例並以法律爲之。且其手段必須是最小侵害的方式進行。而在註冊中心中所含括的註冊資料，卻有不少是無法理解其對法定目的有任何的助益，例如對於居住狀況的登記，一個人在短暫居留之後獲得公民身分而長期居住，則其之前的居住狀況的登記對法定目的而言有何必要。而除現居住址之外，登記其第二居住地點有有何實益。更別說是在每次註冊資料使用的紀錄登記，其可能在提供給第三人時造成對個人隱私權的重大干預，卻看不出就立法目的而言該記錄有何必要性。[69]

人權委員會認爲註冊中心所持的資料種類將涉及第八條隱私權保護的問題。因此就全國註冊中心的範圍以及其資料的使用將要求政府就其是否對法定目的而言爲必要且合比例的問題審慎評估。特別是，

[69] Joint Committee On Human Rights, Session 2004-05 Fifth Report, 26 January 2005.

就像是先前委員會指出，在表一第九段的使用記錄資訊，隨著時間，將能藉由個人工作、公共服務使用情形等紀錄勾畫出私人的生活，對隱私權的影響尤爲巨大。而註冊中心所登記的廣泛個人資料，有些資料的保留對於法定目的而言並不合比例，因此將可能會有違反第八條的問題。[70]

資訊委員會在 2003 年對於政府的報告當中，其即建議與其建立擁有國內人民廣大資料的全國註冊中心，是否不如尋找是否有其他可辨識身分而較不侵犯人權的方式。其認爲登記如此廣泛的個人資料並要求個人隨時更新變動是過度侵犯且不符合比例原則的。例如其要求個人必須登記所有其曾居住的地址以及未來會居住的地址，但在該身分已經確立，並有生物特徵可辨識身分的情形之下，買了一間新房子並不會影響其身分辨識的問題，是故這樣的資訊登記乃是過度且不必要的。

而註冊中心所涵蓋的資料範圍亦是無保證且侵犯隱私的。此尤其在政府的設想當中，其將會記錄每次註冊資料被使用的情況，紀錄誰使用該註冊資料以及何時使用，此將會詳細的勾畫出個人私人生活的情形，嚴重侵犯私人隱私。而該措施不能僅獨立來看，結合監視器的設置、測速器的紀錄等，將會使國家成爲一個監控社會的情況，若不將各措施對私人干預的程度降到最小，則未來勢必面臨國家權力肆無忌憚的侵犯。[71]

（四）資料使用

[70] Joint Committee On Human Rights, Session 2005-06 First Report, 17 October 2005.
[71] Information Commissioner, concerns about the Identity Cards Bill, October 2005.

資訊委員會同時亦關心政府設定的用途廣泛度。身分證在資訊委員會眼中應該是幫助人民證明身分的工具，且其應該是在個人掌控之下的工具。資訊委員會擔心要求人民證明其身分的要求將會增加，而廣泛的用途設定將會造成某種功能轉移，而使私人的生活無可預見的或甚至不能接受的受到侵犯。[72]

> 主要的重點在於，誰能使用該資料庫。就像是一般可預期的，在國家安全、預防或偵查犯罪或其他由內政部特定的目的之下，該資料庫資料可被揭露。然而，沒有人會去煩惱是否符合這些正當事由，因爲在第 20 條第 2 項中即容許，多不勝數的人可在「任何實現其機構運作的目的」之下使用該資料庫。也就是說英國政府通信部（GCHQ）、安全福利機構、國家犯罪機構等皆可單純宣稱其有此必要而使用該資料庫。
>
> 律師會在法案當中極力禁止對於隨時攜帶身分證的要求。但這樣的努力在國家註冊中心資料可隨時被使用的情況下顯得無關緊要，身分證畢竟只是在註冊中心註冊當時的副本罷了。無可置疑的，身分證及國家註冊中心主要侵犯到了隱私權。目前法律界中認知的法律問題在於，是否這樣的侵犯有因其乃爲針對特定正當的需求作出的合比例反應而合法化。[73]

該疑問就下列不同方式的資料使用進行討論

1. 揭露

---

[72] Information Commissioner, concerns about the Identity Cards Bill, October 2005.
[73] Roger Smith, Rights And Wrongs: Registering Fears, Law Society Gazette, 17 June 2004.

法案第十七至二十條允許內政大臣在某些情況下未經個人同意揭露私人資訊。這些規定的效果如下

- 在註冊中心的所有資料可能將在任何實踐其部門功能的目的下，揭露予保安部門總長、秘密情報局局長、政府通信部部長、重大組織犯罪署署長等。
- 註冊中心的資料，除了先前使用紀錄之外，可能會在國家安全、預防犯罪、或其他國務大臣命令的目的之下，揭露予警察總長。
- 國內稅收或者關稅及消費稅單位可在廣泛的目的下，包括預防偵查犯罪、國安全、確認部門作業資訊等情形下，取得註冊資訊。
- 任何政府部門可在關係其部門功能或主管範圍的目的之下，獲得註冊資訊。
- 而先前使用註冊資料的紀錄，亦可在偵防重大犯罪的情況之下，揭露予警察總長、稅務機關或其他政府部門。
- 註冊資料，當其關係於該選訂機關在本法當中的權力責任或者關係於該選定證件的責任時，亦可能揭露予選定證件機關。.
- 除了使用紀錄之外的註冊資料可被提供予任何關係刑事偵查或訴訟程序之人，無論是在英國或是外國，但國務大臣有權利可限制對海外訴訟程序的資料提供。
- 當公司機構提供資訊確認其是否於註冊中心登記，而其資料被發現與登記資料並不一致時，其可能可取得註冊中心當中相關的資訊。.

未經個人同意揭露私人資料乃侵犯了第八條的權力，尤其是在其所揭露的對象廣泛至所有的政府機關，而且是基於這麼廣泛的政府機關功能目的。如此的規定，其個人資料揭露的對象範圍以及其揭露的

目的，恐怕並不符合歐洲人權公約第八條第二項所要求的確定且可預見。

同時受到注意的是，恐怕不會在容許揭露這些資訊的所有情況，都符合第八條第二項所要追求的目的。例如，這並不能確定所有政府部門的功能都與第八條第二項法定的目的相符合。甚而言之，在關稅機關可請其資訊的情況，包括爲了要落實該機關實行罰則的目的，但此處罰乃關係民事的問題，似乎與第八條第二項所要追求的預防或偵查犯罪並不相干。

即使其揭露目的符合法定目標，但其是否對該目標而言是必需且合乎比例則亦有疑問，在條文中並未要求在揭露之前評估其是否必要或合乎比例。在第二十一條第一項規定，註冊中心資訊只能國務大臣確信該取得資訊之人未有其他合理適用的管道可獲取相關資料時始可爲之。進一步的預防措施可能會以規則的形式在第二十一條下制定，但至少在法案中看不到有限制取得資訊主體或者是需經國務大臣同意後始可揭露資料的保護條款。

註冊資料被使用的紀錄提供部分，則需要更小心的審核。如同歐洲人權法院所主張的，揭露某些特別私人的資料，例如醫療紀錄，必須確定有高度公共利益存在始可爲之。而雖然在法案中並未有揭露醫療記錄的問題，但從註冊紀錄的使用，其可得知個人是否及何時使用醫療系統或其他公共服務、是否申請福利金以及是否申請工作等。這同樣是高度隱私的資料，但在第二十條卻容許國務大臣不需經過額外立法程序即可進一步的提供該項資料，在此有可能有違反第八條隱私權的問題。

人權聯合委員會已經在其對於反恐犯罪安全法案的報告中指出，在第十七條及十八條中，無論該涉案人士在英國或國外，其

> 允許揭露任何與現行或可能的犯罪偵查或訴訟有關之個人資料是可能違反第八條隱私權保護的。而在第十八條卻允許在同樣的情況下，揭露該涉案人士的注冊資料，則其同樣也會有違反第八條的問題。[74]

在先前的人權委員會，對揭露資料的廣泛程度表示嚴重的關切。其注意到在揭露資料之前，其並不會先對該揭露行爲是否對立法目的而言乃爲相關、必要且合比例進行考慮。故委員會認爲，在此隱私權的保護岌岌可危，要求資訊只能在對法定目的而言爲必要的範圍之內始可揭露的法律規定乃爲必要。

而現行的法案在第二十條之下所制定的規則，只能在該揭露對公共利益而言爲必要時始可爲之。類似的要求在第十七條亦可得見，然而，我們注意到在法案中大部分的資訊揭露卻沒有在同樣必要的標準下進行。

例如在第十七條第二項 a 款中規定，資料可在爲落實其機構功能的情況下，揭露予保安部門總長，該門檻相較於必要性是比較低的，而且將容許獲得大部分群眾之資料。同樣的條款亦被適用於秘密情報局局長、政府通信部部長、重大組織犯罪署署長等。

必要性的標準同樣也在下列的情況未受考慮－

- 在第十七條的規定下揭露資訊與警察總長。
- 依照第十七條第五項的規定在關係其部門功能或主管範圍的目的之下，獲得註冊資訊。

---

[74] Joint Committee On Human Rightsm, Session 2004-05 Fifth Report, 26 January 2005.

- 在第十七條第六項的規定下，令選定證件機構在與其功能相關的目的之下獲得註冊資訊。
- 依照第十八條揭露關係刑事偵查或訴訟程序之人之註冊資訊，無論其是在英國或是外國。[75]

2. 查核

在強制登記註冊之後，藉由身分證法案第十三條的規定，國務大臣可制定規則，命相關人士在使用公共服務或獲取福利金時，必須出示身分證件。而在未強制其出示身分證件的情形，根據法案第十七條，公共服務機構可在爲了確定申請服務之個人註冊資料而使用註冊中心之紀錄，在此包括例如現行地址以及前地址、居住狀況以及前居住狀況、可辨認的身體特徵，甚至其也包含之前他人使用註冊資料的紀錄，而此一紀錄如前所述，是非常侵犯個人隱私權的。在此沒有要求公共服務機構只能獲取與其服務相關的資料，例如在健康服務當中，前地址就看不出與其所提供的服務權利有何相關。揭露個人資料會涉及第八條隱私權保護的問題，而我們懷疑向公共服務機構揭露個人資料，甚至包括不相關的個人資料，會能是必需且合比例的干預隱私權之手段。內政部對此保證，依照第十七條提供資訊的情形，將會以規則限制在必要的情形，並且會建立對使用資訊的機構進行審核的系統。但二○○五年及二○○四年的人權委員會都認爲，這樣的防護條款必須與法律明文訂之，而不是以規則的形式爲之。

在強制登記註冊後，在個人與公私機關往來之際，可能會被要求其出示身分證或者同意查詢註冊中心資料。而該機關根據第十二條，將可得到其個人資訊諸如現行即先前居住狀況、照片、簽名等，在此生物特徵並不會被提供，但可被查驗是否與該機關所提供的樣本相

[75] Joint Committee On Human Rights, Session 2005-06 First Report, 17 October 2005.

同，而之前紀錄的使用情況亦不會被提供。但這樣的身分查核可能被廣泛的私人使用，諸如未來的雇主等，雖然說其經過當事人的同意，但這樣提供資料的行爲，是否就其立法目的而言是否爲一必要且合比例的手段則有疑問。且這樣取得資料的情況雖然是經過當事人同意，但此同意可能是事實上的自願或者只是概念上的自願。當事人可能會爲了取得服務的需求、訂定契約的急迫性等，而不得不予以同意。對此內政部表示其機會建立對該資料提供的各機構建立核准的系統。然而人權委員會認爲進一步的保護措施應該藉由立法來確認第八條的保護，確定該查核是在與立法目的相關且在實際情況必要的時候始可爲之。[76]

就像是解釋文指出的，第十二條第四項容許訂定規則限制可能會在該條提供的資料，這可被用來確認不會提供某種人的某種資訊予其他組織，例如對於變性人的原姓名可能對他而言會是敏感資料。此權力甚至可擴及至將第十二條第二項原本可能跟確認目的不相干的資料，限制到僅提供必需的數種資料。該條的規定就符合第八條隱私權的保護而言，可說是十分重要。

3. 交換

第九條允許在國務大臣、選定證件機構、以及其他公司團體間的資訊交換，以確定以被儲存於註冊中心或者提供給國務大臣或從其他來源可得的資料之正確性（第九條第一項）。國務大臣可要求中央政府或者公司機構提供確認的資料。而選定證件機構也可在其需要確認申請發放或修正證件之資料正確性，來要求提供

[76] Joint Committee On Human Rights, Session 2005-06 First Report, 17 October 2005.

確認資料。在第九條之下可要求提供資訊的機構還包括了執行法定功能的私營機構、中央及地方政府、公家機關等。也可能經由國務大臣所制定的規則，包括私人機構亦可要求提供資料（第九條第六項）而此一要求可經由民事程序強制爲之。

在第九條資訊交換的情形明顯的極爲寬廣。可被確認的資訊部但包括註冊中心已有或以被提供的資訊，甚至包括純可由妻他來源取得的資訊。這暗示即使是在自願的計畫當中，個人資訊也可能是在其不知情或未同意的情形被收集。

此外就功能轉移（Function creep）的問題也值得重視，其乃爲某一特定目的所蒐集的資料可能在之後被使用於其他非計畫或非授權的目的。爲了預防此種情況，與原始目的並不相容的資料處理必須備阻止。

四、 **系統技術**

關於生物資料樣板的儲存，依其生物辨識設備的運用情況及樣版的規模大小而定，亦會引發資料保護的問題。舉例來說，樣板被儲存在生物設備記憶當中，可能是在中央資料庫或者是塑膠卡、光學卡、智慧卡等。儲存的方式就系統的目的而言必須爲恰當。當系統目的爲辨識時，只能藉由儲存相關資料於中央資料庫時始能完成，而原則上當系統目的爲確認時則不需要集中儲存相關資料。[77]

[77] Phillip Rees, Biometrics and border control, New Law Journal, 13 August 2004.

生物特徵的技術或許帶來不少便利，但當生物辨識技術出錯時又如何？指紋與虹膜技術仍被認爲存有錯誤的機率，而面部辨識尚在發展之中且該技術需要特定光度、面孔位置、表情的條件配合。則在此科技尚在發展中的情況下，醫院、銀行及其他機構是否會在電腦失靈時關閉；而當辨識技術將你辨識爲他人或者他人竊取該數位身分時又如何？英國瓦立克大學專研生物技術的經濟學者 Jonathan Cave 表示身分詐欺勢將困難化且嚴重化。準確的身分辨識將減少廣泛的錯誤，但當錯誤發生時則將會更爲嚴重且難以改正。因而確保在意外被系統拒絕辨認（例如眼睛受傷）或系統本身錯誤的情形下能有妥善的處理則變得非常重要。

更糟的情況發生在該生物身分遭到竄改或僞造的時候，當該人的虹膜完全與資料庫的紀錄不符，每次掃讀其眼睛時，可能會被其銀行系統、其子女的學校大門、或者機場的櫃檯遭到拒絕。這樣的情形是否可能發生，端視其系統的設計如何。以英國目前將把資料同時儲存於個人身分證及中央資料庫的計畫而言，大多數倫敦經濟學院的研究者皆發現如此太過複雜、技術上並不安全。論者建議在可經當事人同意進入的中央資料庫中，只需儲存非生物特徵的其他資料，而生物性資料，則僅儲存於由個人攜帶的身分證件中。[78]

伍、實行狀況

[78] See Duncan Graham-Rowe, Privacy and prejudice: whose ID is it anyway, New Scientist ：Technology, P. 20, September 17, 2005.

一、身分證

身分證法案規定每位年滿十六歲之人，皆應登記其身分、住址、居住狀況以及包含了指紋或虹膜的生物資料。而在註冊過程中，該人將會被要求前往某地或流動處所確定其生物資料並與登記。該生物資料將會被儲存於全國身分註冊中心 National Identity Register (NIR)以及發放於個人的身分證當中，並僅有授權單位可利用其確認個人身分。

雖然在計畫中，身分證應該於 2008 年發放，但內政部及身分證計劃負責人皆指出，由於各項科技仍處於發展階段，故此一時間表仍有相當的彈性空間。而身分證計畫同時亦與內政部的許多方案息息相關，諸如接下來推動的生物簽證、外國人生物居住許可、生物護照等，其皆同時測試著未來在身分證發放上可能會面臨到的障礙。內含面部辨識晶片的生物護照，在 2006 年 3 月即要開始適用，該護照乃參考 ICAO 所定的標準，以面部辨識爲首要的辨識方式，而指紋及虹膜則爲其備位措施。最新的時間表則在二○○六年內政部所提出的身分證法案執行報告[79]中指出，未來將於二○○八年對英國境內的外籍人士全面發放身分證件，並隨後於二○○九年英國國民於申請護照時可同時申請身分證件，但到了二○一○年每位申請護照之英國國民皆會強制同時發放身分證件。考慮到持護照的英國國民約佔國民總數的八成，且護照一般有效期限爲十年的情況下，估計於二○二○年即有絕大多數的英國國民皆

[79] See Strategic Action Plan for the National Identity Scheme：Safeguarding your identity, Home Office, December 2006.
http://www.identitycards.gov.uk/downloads/Strategic_Action_Plan.pdf

持有身分證件，並於屆時再針對未持證件的兩成民眾考慮修法建立強制發放身分證件之基礎。

爲落實此項計畫，英國結合原本的國家護照服務系統與身分證計畫團隊，建立了新的身分與護照服務系統（IPS）。[80]該系統乃在二○○六年作爲內政部的一執行機關而建立。其將在未來提供護照以及英國、愛爾蘭國民身分證發放的服務，同時也包括了居住在英國境內的外籍人士相關移民證件的核發功能。

身分證計畫要求個人應將其生物資料儲存於全國登記中心，在此生物資料的定義乃爲關於個人外在特徵的資料，特別是包括像虹膜或眼睛部份的特徵等。生物資料的種類多樣，包括指紋、面部、虹膜、視網膜、DNA、走路姿勢、血管紋路等。在此政府表示，在身分證的部份將採用結合十三樣生物資料的辨識系統，包括了十個指紋、兩個虹膜、一個臉部特徵。採用此種多數的生物資料系統，乃基於兩個理由，首先是要使盡可能多數的人民能使用該系統，就像即使其失去雙手，仍有虹膜及臉部可供比對；其次是提供再次確認的機會，例如在指紋辨識出錯時，還尚可以虹膜辨識做第二次的確認。但在不同的情況中，多數仍是會有某種生物特徵辨識較爲合適，例如在航站需快速辨識身分時，虹膜的辨識方式即有此速度上的優勢。

生物資料的比對可以分爲一對一的確認以及一對多的辨識，在身分證計劃當中，生物資料將會儲存在全國紀錄中心以及個人

[80] http://www.ukpa.gov.uk/

所持有的身分證當中，因此內政部長就曾對此表示，一旦有人重複以同樣的生物資料，卻表示不同的身分時，系統即會警告該人以重複出現在資料庫中。

生物辨識在近年來被大量使用，包括在 911 之後美國就簽證部分採用虹膜辨識技術、2003 年 5 月 ICAO 規劃出將生物辨識技術與護照或其他旅行文件相結合的藍圖、2003 年 6 月阿拉伯聯合大公國在國界控管方面採用虹膜技術以及在 2004 年 12 月歐盟通過新的護照必須包括電子面部辨識資料（18 個月內）以及指紋資料（三年內）的規定。

英國針對身分證計畫，分別在 2002 及 2004 年皆有進行相關的研討磋商，第一次的磋商是針對權利卡的使用方式等，第二次則是針對相關立法的問題，包括分享資訊的權力、註冊的單位等等。近來的研討則多針對在技術層面，由於該生物辨識技術與科技發展息息相關，故這方面的研討確是需要的，問題是雖然相關的研討頻繁且多樣，但受人詬病的是其問錯了問題以及搞錯了階段。其多針對獲得該技術的方面，而非真正討論該辨識該不該實施，實施的話應以何種結構爲當等部份。

這份計劃一開始的目的如前所述，在法案中已說明，乃著重於國家安全、執法、移民控管的層面。而隨著計劃的發展，各目的強調的重點開始改變，例如像一開始在身分冒用上的重視，逐漸轉變爲恐怖主義及犯罪部分的反制，爲令社會大眾及相關單位不致無所適從，英國下議院科學科技委員會建議既然該法案已經過皇室御准，則其計畫目的即應該要呈現穩定的狀態。

科學科技委員會於二○○六年八月的研究報告[81]同時亦發現內政部在處理科學上的建議及證詞的部份，在許多層面上乃有極佳的成效。例如在專家委員會的建立、國家商貿部門的審核、與國際專家的研討以及技術上試行的委託等。尤其，委員會對內政部認爲對該計畫應採取審慎的態度，逐步實施的主張予以贊同。內政部目前正在收集建議及資料的階段，如何使用這些資訊將對該計畫有極大的影響。

在這調查當中委員會同時發現一些令人擔憂的問題。首先其發現身分證計畫小組對於生物辨識的專注研究，可能會分散對於其他問題的關注，諸如 ICT 以及社會學上的問題。那同時對於身分證計畫而言是息息相關的問題，但究竟誰應負責去研究討論，卻始終權責不明。而計畫小組對於其他富有相關知識經驗的政府部門亦缺乏合作的互動，這種自我孤立的狀況，在未來亦令該計畫的落實不盡樂觀。

關於科學建議及跡象方面，生物辨識與其他問題的區分被注重的情況乃不一致。在該計畫的某些部份，像是生物特徵的使用種類是被確定的，而其他部分，例如 ICT 系統的問題則留給產業本身決定。這樣不一致的狀況已致使普羅大眾感覺混亂，亦令對於該計畫將規定的範圍亦無法明確。這樣的混亂，由於計劃本身的非透明化而更加惡化。

81 Sixth Report：Identity Card Technologies: Scientific Advice, Risk and Evidence, The House of Commons－Science and Technology Committee, 20 July 2006. http://www.publications.parliament.uk/pa/cm200506/cmselect/cmsctech/1032/103202.htm

而就英國一般人民對於生物特徵應用的觀感部份，一份由TSSI生物公司於二○○六年九月及十月，訪問十八歲至六十歲一千人的調查報告指出，由於近年來英國遭受的恐怖事件頻傳，基於個人安全的擔心，有八成的人士較之前更加支持生物辨識的技術應用。但有關生物辨識對私人權利的侵害仍然是關心的重點，有三成的人士仍然反對由政府統一設置中央資料庫儲存生物資料，有五成人士已被該設置所帶來的利益說服，有二成的人士則尚舉棋不定。[82]

英國人權組織 Liberty 認爲，對於廣泛使用生物辨識技術方面，並未獲得充分的社會共識，普遍而言，對於身分證計畫的疑問通常多過於答案。對於民眾所要達成的目標而言，如此的技術是否必須可能還是疑問。就相關科技尚處於發展階段的現在，技術的現況瞬息萬變，恐怕無法讓社會充分的了解討論後接受之。而對於大型資料庫所帶來的隱私權侵害、身分證計畫預算的不確定性、對少數族群所將帶來更嚴重的騷擾、將來資料可能廣泛應用於其他目的之疑慮等亦是社會各界揮之不去的未解質疑。

二、生物護照

英國生物護照於 2006 年三月開始發行，其乃英國政府對抗身

[82] M2 Presswire, TSSI: Biometrics gains British approval; ...3 in 4 people now say they would welcome its use..., October 17, 2006.

分冒用的一大利器。由於身分冒用的威脅持續的增加，英國政府意識到其必須在護照方面加強安全保護。而以國際民航組織於2003 年五月發表的標準而言，其選擇了面部辨識作爲主要生物辨識方法，並又佐以虹膜及指紋辨識方法作爲後備之用（非強制）。英國生物護照主要有兩種功能，其一爲幫助偵測僞造或篡改的身分證件，另外則爲確定個人的身分。

韋氏辭典定義生物辨識爲，對於生物觀察及現象的統計分析。在近幾年，取得國民的個人生物特徵資料，並安全且有效儲存於個人護照的技術發展，已造成對英國及其他工業國家巨大的衝擊挑戰。通俗的說，生物辨識通常被描述爲區分一個人不同於其他人的個人特徵，例如面部結構、指紋、虹膜以及ＤＮＡ。取得個人的生物資料並將其儲存於護照的晶片當中，其所帶來的安全利益相當可觀。

且全球的恐怖主義盛行，增加了飛航安全以及移民的爭論問題，迫使英國政府重新評估及邊界控管的有效性。英內政部因此推動了生物辨識作爲控制移民及邊界安全的方式。[83]英國政府試圖使用生物辨識技術來現代畫其邊界控管技術的計畫，最先在2002 年二月提出。在其邊界安全白皮書中，開始使用生物辨識作爲監控航線乘客的方式之一。大西洋線的乘客於 2002 年儲存其虹膜資料在一先行挑選並自願爲之的資料庫中，而這是英國第一次試行類似生物辨識的方式，其證明了該方式具有增加邊界安全的潛力，並在該試用中受到了乘客們的好評。在 2003 年八月，該計劃擴展到在英國簽證上亦使用生物辨識技術。在該計畫中，申請

[83] Phillip Rees, Biometrics and border control, NEW LAW JOURNAL, 13 August 2004.

英國簽證的旅客皆將會被要求提供生物資料，來在入境時作爲比對之用，並防止其在英國非法居留。政府同時亦宣佈生物辨識技術將會從 2005 年起遵循國際高峰會的原則使用在英國護照之內。而這將會有六個月的試行計畫，將會記錄超過一萬名參加者的面部特徵、虹膜及指紋資料。

英國護照自從其於英王查理一世在位時被首次引介採用時起，其一直都在持續不斷的發展。在護照每個發展階段中，都會加入安全特徵以防範僞造及濫用的情形。而生物資訊的加入，已將護照的發行帶入了一個新的階段。雖然英國及其他國家已在進行其各自的計畫，但對於生物護照的一般標準同時也已由國際民航組織所制定完成。這當然是一個全新未知的領域，但由於護照將會是國際之間旅行的證件，故這同時也是一個各國政府需要緊密合作的領域。那麼，爲何英國政府決定要投入生物護照計畫？主要的理由是要經由增加證件的安全性以及減少身分冒用的危險，來加入其他國際盟友對於恐怖主義威脅的反制行動。故英國正透過持續不斷的增加護照安全特徵，以及確定申請護照的階段不會被公開濫用，來致力於加強其對恐怖主義的預防。例如，一個新的英國護照組織已在全英各地設立。他們的任務之一，即是去落實對於第一次申請英國護照者的面試規定。

英內政部準備在全英範圍內設立 69 個申辦護照面試中心，並逐步推行面試系統。第一次申辦新護照的成人中將有一些人被要求自費前往這些面試中心接受 10 到 20 分鐘的面試，面試的問題主要圍繞申請人的個人訊息，如過去的地址和銀行賬戶等。但從 2009 年開始，所有申請更新或補辦護照的人都必須接受面試。據估計，屆時每年將有數百萬人被要求前往面試中心，留下指紋和

照片，爲將來簽發生物護照作準備。內政部表示，新的政策會給人們造成一定的不便，但是對於打擊日趨嚴重的身分盜用問題，這一辦法非常重要，因爲有大約 75%的身分盜用發生在第一次申辦護照的人身上。但也有專家表示，對於那些僞造護照職業罪犯來說，面試恐怕不會見效。

但同樣有助於國際生物辨識計畫發展的是美國在２００２年的加強邊境安全及簽證改革法案（Enhanced Border Security and Visa Entry Reform Act），其在２００２年五月由總統簽署通過，當中第３０３條規定，３０２條中之可由機器判讀並防篡改的進出證件，將由２００４年１０月２６日開始，政府組織必須發行可由機器判讀、防篡改的簽證，以及其他使用生物辨識技術的入境證件。進出航站必須使用可進行所有證件中生物辨識比對及確認的儀器及軟體。此外，在２００４年１０月２６日之前，爲了使各國能繼續具備免簽證計畫（Visa Waiver Program）的參加資格，該國政府必須保證其具有計畫發行機器可判讀、防竄之國民護照，該護照還須符合國際民航組織對於生物辨識以及確認的要求標準。在２００４年１０月２６日之後，外國人若要在免簽證計畫當中，尋求入境許可，則除非該人護照是在２００４年１０月２６日之前所發放，否則該外籍人士即必須出示上述護照始可。

因此，美國加強邊界安全及簽證改革法案立下了一個最後期限，其他想要繼續參加免簽證計畫的國家，像是英國，則必須在該期限前在其生物辨識計畫中完成特定的標準。每年有超過四百五十萬的英國護照持有者，經由免簽證計畫進入美國國境。英國及其他二十六個參加免簽證計畫的國家（包括大部分西歐國家、日本、澳洲、紐西蘭等），無法想像在美國免簽證計畫當中的地

位受到質疑的後果。儘管英國政府已盡了其最大努力在美加強邊境安全與簽證改革法案的時間表內發展期生物辨識系統，但很明顯的，其無法在原本的截止期限前完成。

該截止期限被重新談判（第一階段，２００５年１０月２６日前須發放機器可判讀之護照，第二階段，２００６年１０月２６日前，須發放生物護照）。由於如此急迫的必須引進生物辨識技術，使得原本提倡此一技術，甚至在１９９２年即開始討論的國際民航組織，亦有批評，認爲此一行動只是對於９１１事件的反射動作，在對於生物辨識技術充滿迷思的情況以及歇斯底里的環境下所作的匆促決定，缺乏詳盡的考慮。

英國已在２００５年年初在其各政府組織發放機器可判讀之護照。預計在２００６年開始發放生物護照。未來經由使用生物資料所將帶來的改變將會是相當巨大，生物資料將會被收集且儲存於簽證、或在某些高科技單位，未來進出大樓可能皆須經過指紋的掃描。這將會面臨許多挑戰，至少，在安全及隱私之間的平衡即是一項棘手的議題。[84]下列的各個層面都是在實際應用上關注的焦點－

【資料保護】

[84] Graeme Wise，BIOMETRIC PASSPORTS THE UNITED KINGDOM'S RESPONSE TO AN INTERNATIONAL　CHALLENGE，Maryland Bar Journal，July/August, 2006。

對於很多人來說，政府使用生物辨識技術的情況提高了他們對於這方面的關注。在註冊階段當中，原始資料、抽取過程、保護演算技術、樣板選取等問題都會涉入。該收集的資料將會包括敏感的個人資料，其將有可能揭露種族或種源的資訊，甚而可能揭露健康問題。

且隨著生物辨識設備的使用以及選取樣板的大小，個人樣板的儲存問題議會引起資料保護的議題。舉例來說，樣板會被儲存於生物辨識設備的記憶當中，可能是在中央資料庫，也可能是在個人塑膠卡片、光學卡片、智慧卡片當中。該儲存的方式必須就該辨識系統的目的而言符合比例且爲恰當。資料也許只能經由儲存於中央資料庫才能達到辨識身分的目的，但原則上在以確認身分爲目的的系統中，統一的儲存相關資料於中央系統通常是不必要的。

功能的移轉問題也需注意，當資料乃是基於某一法定目的才被收集的時候，必須注意其是否在後續被使用於其他未經授權或者原本不在計畫範圍之內的情況。爲了防止這樣的情形，與原本法定目的不相容的資料處理必須被防止。

另外對於某些人而言的主要問題在於，生物辨識技術是否會被用來作爲一國家監視或社會控制的技術。是否某些生物資料將會在未經同意、未經其個人主動參與的情形下，在資料主體毫不知情的時候被使用。生物辨識技術由於其低侵入性，可能將會沒有限制的被利用，因此，特定的安全防範機制乃是必要的。

類似的問題可能會發生在機關間互相資料分享的情形中。從不同的資料來源所得到的個人資料，可能會被使用在遠超於原始收集目的的情形之下。生物特徵資料的中央儲存系統，作爲一聯繫不同資料庫的核心，同時提升了這種資料濫用的危險，並結合諸項資料，將會能細緻描繪出個人同時在公眾及私人生活的日常習慣。

【比例原則】

此外尚有在資料取得及處理方面的比例原則問題。生物資料只能在對原本收集目的而言爲足夠、相關、非過度的情形下才能被使用。此外，生物資料，尤其是原始資料，通常都會包含一些對於辨識或確認不需要的資料，該生物樣板必須被涉及爲能預先排除此類不需要的個人資料始可（所有被收集但不需要的資料，必須被盡速銷燬）。個人資料只在其法定目的需要的時間內被保存。

當被系統意外的錯誤拒絕（例如眼睛受傷）或者系統本身的錯誤發生時，確保一安全的後續處理程序是很重要的。生物資料的處理及收集必須在一公正誠實的方式下被操作。資料主體除了特定的例外，例如有關於公眾安全的情形之外，應該被持續的通知有關該資訊的應用。該主體應該要知道確切的使用目的，以及關於該檔案管理者的身分。因此基於未通知資料主體之資料而組成的系統，應該被排除。在此方面，基於遠距面部辨識、收集指紋以及錄下聲音的生物資料系統，將會表現出極高的風險。而當有使用或收集的同意出現時，其必須是在自由的狀態下作成，由資料主體特定的通知其同意爲此資料處理。

【安全措施】

管理者必須採取在安全措施上採取適合的技術與組織，以保護個人資料避免意外或不法的破壞、意外的遺失、改變、未經授權的揭露、進入，尤其當生物資料的處理將牽涉到在網路上的傳輸。在資料處理的各個階段都應該備有安全措施，包括儲存、收集資料、比對等。想像中的措施包含有資料樣板的加密、除了存取控制外加密的鑰匙。從樣板中重組原先的資料應該在實際上是不可能的。該安全措施應該在一開始就具備，特別是在註冊階段，當生物資料將被轉化爲某種樣板或典型時。[85]

而英國在實際施行之後亦發現問題，

首先，生物護照有被駭客複製的危險，由於該護照晶片採取射頻辨識（RFID）的技術，其類似超市中的條碼，好處在於可以在短距離內讓掃瞄機器判讀，但其同時也造成安全上的弱點，德國安全專家 Lukas Grunwald 就證明了這一點，經由可輕易在拍賣網站上買得的２００美元掃瞄機器，其可掃描出護照晶片當中儲存的資料，並可複製另一晶片護照。

故該生物護照在實際發行之後，其面臨了收回撤銷的要求。因爲該花費近一百七十四英鎊的生物護照，在面市之後，發現其竟會受到駭客的攻擊並且有複製當中個人資料的可能性。該項發現將勢必使得內政大臣面臨沉重的壓力，並連帶必須重新思考身分證計畫的可行性。對此，英國自由民主黨內政部發言人要求全面的回收，其認爲該生物護照的發行將使人民面臨更甚以往的身

[85] Phillip Rees, Biometrics and border control, NEW LAW JOURNAL, 13 August 2004.

分冒用危險。但英國政府對此表示，該項發現的瑕疵並不重大，經由該瑕疵中能被取得的資訊，都是一般的個人資訊，諸如相片、生日等，而晶片只是生物護照安全設計的一環，能複製晶片並不代表能複製護照，且未來內政部將加強密碼技術的應用，令其即使能從遠距取得晶片資料，但在未破解其加密程式之前皆無法獲得當中內容。該言論當然受到了各方人士的批評，認爲既然該晶片得以被複製，未來使用僞造生物護照的可能不容小覷，政府如此的發言，正反映了其漫不經心的態度。[86]且在此亦有兩項缺失，一爲該加密程式是可讓駭客不斷的嘗試破解，不像銀行密碼的設計，其並不會在幾次嘗試之後即拒絕使用者的進入，另外則爲該加密程式通常有軌跡可循，例如持有者的生日、該護照的到期日期等，該項解開晶片的密碼通常就寫在護照上面，就像是寫在提款卡被面的密碼一樣。

其次，原本計畫使用期限爲十年的電子護照，卻在英國審計部今年二月的報告[87]中指出，當中晶片零件的保證期限相對而言只有區區兩年，而在此一技術如此新穎的情形之下，沒有人知道這些零件會維持多久。內政部對此表示，電子護照已被嚴苛的檢驗測試過，但將來將會在保證問題上加強。該晶片將會儲存生物資料，包括照片等，將會在掃描儀器中被判讀。雖然審計部於報告中讚揚身分與護照系統依計劃時間引進新型護照，並且配合國際標準的努力，但同時亦表示，當中的瑕疵問題可能會使原本預期的安全利益流於空談。故其同時敦促該組織，亦應與晶片生產者研議延長保證時間的問題。審計部表示，雖然其已在研究環境中受到檢驗，但該晶片是否禁得起護照日常生活的使用仍屬未知。在大量人潮時使用判讀機器來檢驗電子護照的影響仍然不確定，包括了該判讀儀器的表現究竟如何，以及其是否會對旅客造成遲延的可能性。該報告同時指出，面對超過十年的變化，該軟體也許會無法在應該比對資料相符時判讀出來。

---

[86] Steve Boggan, Recall demand after cloning of new biometric passports, The Guardian, November 17, 2006.

[87] Identity and Passport Service: Introduction of ePassport，7 February 2007，http://www.nao.org.uk/publications/nao_reports/06-07/0607152.pdf

審計部另外尚對內政部各部門對於引進判讀生物護照掃描器缺乏統一正式聯繫表示關心。其認爲如果外交部、身分及護照系統、移民及國籍局能更緊密的合作，而非個別獨立的購買判讀儀器的話，其將會節省不少的花費及時間。但由於此一現實的問題，目前至少必須要到２００７年三月各航站入口才會有掃描器設立。英國保守黨議員 Mr Leigh 同時也對此表示關注，表示許多英國入境航站都缺乏周全的設備來處理此一新科技的應用，將會增加許多旅客的遲延問題。保守黨 David Davis 亦表示，結合航站設備不全以及零件保固期限甚短的問題，將使度假者以及商務旅客，將面臨更多的不確定性，以及實際被擱淺的可能性。而在較爲單純的生物護照方面就產生了如此多的問題，更遑論複雜程度更甚於此的身分證計畫，此實可證明身分正計畫的推行乃爲一錯誤的決定。

陸、結語

就英國生物辨識議題方面，目前現行相關法案包括 Identity Cards Act 2006、Immigration, Asylum and Nationality Act 2006、Immigration And Asylum Act 1999 及 Anti-terrorism, Crime and Security Act 2001。

就身分證法案而言，其基於方便驗證個人身分之立法目的，可就十六歲以上並屬於英國國民之人取得生物資料，該資料內容包括面部、指紋、虹膜及其他生物特徵等。其將經由身分證或其他指定證件如護照的發放，取得該人生物資訊。身分證持有人，負有義務在其規定的範圍之內，對其個人資訊有所更動或本身已知的錯誤必須在法定期間內通知註冊中心，並當持卡人發現身分證被偷、遺失、遭竄改、毀損的情形時，必須通知註冊中心或其他法定人員，且該身分證則將被取消。而註冊單位以及發放選定

證件部門，可基於確定其將要註冊或已註冊的資訊是否正確之目的，交換其所儲存之資訊。國務卿亦可在當事人同意的情況下，提供他人註冊中心的相關資料。另國安及情報機關、警察首長、稅務管理局等單位，在符合該機關目的的情形之下，亦將可取得相關個人資訊。且設立國家身分計劃委員（National Identity Scheme Commissioner），監督身分證計畫及註冊中心就身分證的應用及對登記資訊的提供。

就移民及難民法部分，定爲查明護照或相關證件的真實性，實行該項查核之人可請求被檢查之人提供外部特徵資料，諸如指紋、虹膜、或其他眼睛部位特徵等。而警官、出入境官員、監獄長官等人對抵達英國國境時，無法提出有效的證件之人、或拒絕入境但例外留置之人、或請求政治庇護者等可在相關時間內取其指紋。取得生物資料的方式則爲書面通知後，由該人提供指紋，或由警察機關在無逮捕令的情況下予以逮捕，強制取得該人指紋。且該指紋必須在一定期間內被銷毀。

另就反恐怖主以法及相關刑事立法部份，司法警察對於定罪、起訴、警告或其他有合理理由認爲其涉入犯罪之人，在未經其同意的情況下採取其指紋。亦可對依該法羈押之人經警察督察長以上層級之授權，採取指紋以確定其是否從事恐怖犯罪，或者教唆、幫助或煽動該類犯罪。在採取指紋之前，必須告知該指紋採取之目的，以及採取指紋之處所等。在強制採取指紋的部份，亦應告訴其授權採取情形、依據理由、所涉犯罪等。爲辨認身分所採取的指紋，無論當事人後來被証明有罪或無罪，皆可保存，但其使用之目的必須與預防或調查、偵查犯罪、進行起訴等目的相關。

雖有上述相關立法，但目前英國就生物辨識的相關討論，多集中於身分證法案部分。首先，侵害隱私權而取得生物資料需符

合特定公共利益爲前提，但在身分證法案當中所提出的公共利益諸如防止犯罪、減少不法工作、身分欺詐等公共利益，皆未能被證實可經由身分證之實行而達成。其次，由於蒐集個人生物資料將有侵犯隱私權的問題，故其是否符合歐洲人權公約第八條的要求，在公共利益的要求下以符合比例原則的權衡標準，非過度的干涉個人權利即爲重點。故在此諸如大型資料庫的設立、諸多資料的蒐集等是否違反比例原則，則爲考慮重點。另由於強制取得身分證將爲階段性的實施，則在此是否會違反歐洲人權公約第十四條禁止差別待遇的規定，亦有疑問。第三，就資料庫的管理部分，涉及資料保護的問題，從資料的取得、內容、管理等皆須小心討論實施，尤其在資料的揭露部分，對生物資料此種敏感資料的使用揭露規定，是否已臻完善，目前在現行英國身分證法當中將有許多機關可在模糊的定義下取得資料的情況下，恐尚有進步空間。最後，就生物辨識技術而言，由於該技術尚在發展當中，其可能會造成的錯誤該如何解決，其技術該限制在怎樣的程度才不會過度蒐集資料而違反比例原則等，皆爲問題所在。

目前英國生物辨識技術的應用，藉著身分證法案的推行，已逐漸展開，未來將於二○○八年對英國境內的外籍人士全面發放身分證件，並隨後於二○○九年英國國民於申請護照時可同時申請身分證件，但到了二○一○年每位申請護照之英國國民皆會強制同時發放身分證件。但在政府不斷保證該計畫爲切合時代潮流且能提升公共安全的同時，諸多反對質疑意見仍然不斷，其對於隱私權及相關人權可能產生的侵害、可能發展爲監控國家的疑慮、甚至在技術上是否能真正實行、是否會造成花費龐大但效用不彰的情況等，皆造成英國社會，甚至政府官員、國會成員對於此項生物技術應用持保留態度。雖然目前英國政府在生物應用上似乎已爲勢所必然，但現實上其反對的呼聲不斷，反對黨甚至明確表示一

旦於下次大選勝利即會停止該身分證計畫的推行，目前英國這樣的道路是走向國家安全提升的康莊大道，或者走向監控社會隱私受限的警察國家，恐怕仍是未知之數。

第五章　德國制度沿革與實踐現狀

壹、導論

生物辨識的技術，以生物特徵來辨識身分制度在德國的討論及運用溯源至 2001 年美國 911 事件之發生後，當時國際間興起基於恐怖主義的防治，而加強安全措施。德國運用生物辨識特徵經過密集的討論，在短期內即在立法上付諸實現。此乃是指以包裹立法〈Artikelgesetz〉的方式在 2002 年 1 月 9 日通過的反國際恐怖主義法（Gesetz zur Bekämpfung der internationalen Terrorismus）[88]，以爲了因應內國治安的問題。在反國際恐怖主義法中，加強對人員及其身分的管控。透過諸如對護照法的修正、個人身份證法的修正、外國人法的修正以及庇護程序法的修正，將生物辨識特徵運用於對人員身分的辨識在這些法律層面上，有了明確的規定，[89]從而行政權在行使運用生物辨識特徵在上述的法律中有成文化的法源基礎—符合所謂的法律保留。另外，在上述的法律中，生物辨識特徵在身分制度的運用之規範目的乃以列舉的方式形成所謂的嚴格的目的拘束〈Zweckbindung〉。即生物辨識特徵運用的目的手段關係中的目的是明確且限定的—表列許可之全部正面目的且亦表列禁止之主要負面目的。生物辨識運用特徵的目的拘束在立法上並沒有採取所謂的例示及概括條款之立法技巧。也就是說生物辨識運用的目的不可以概括條款之方式來立法始合乎憲法

[88] 關於反國際恐怖主義法的立法技術及一般評析，請參見附件一。

[89] 例如擴大情報局的權力、限縮人民的秘密通訊自由，並對於針對外國人之權利〈Ausländerrecht〉有較嚴格的規定。另外德國的基督教民主聯盟〈CDU〉希望警察局與情報局能夠聯手建立恐怖分子的資料庫，惟此還在商議當中。

上比例原則之思維模式而通過最嚴格之合憲的審查，此與我國大法官釋字六 0 三號解釋就生物辨識特徵運用之目的亦需限定且明確始合憲，在憲法的比較層次上恰巧相同。

貳、法規範之基礎

一、 法規範基礎之主旨介紹

反國際恐怖主義法（Gesetz zur Bekämpfung der internationalen Terrorismus） 美國九一一恐怖攻擊事件之發生，使德國警覺必須立即採取全面性安全手段，才能免於成爲國際恐怖組織之下一個受害者。聯邦政府在短時間內以包裹立法之方式，先後擬定二套所謂的「反恐怖主義措施」，送交聯邦眾議院審議。

第一套反恐怖主義措施（Erstes Anti-Terror-Paket）於 2001 年 11 月 9 日通過，其內容要旨包括：

1、 廢除「團體組織法」(Vereinsgesetz)第二條第二項第三款之宗教特權，從此宗教團體將和一般社團一樣受到較嚴格規範。

2、 自 2002 年起提高菸草稅和保險稅，菸草稅分兩階段提高，每階段每支菸加收 2 芬尼之稅金。生命險以外之稅率則由 15%提高至 16%。增稅所得之三十億馬克（15.2 億歐元）將全數用於反恐怖主義措施，如改善通訊、情報和災害防治機關之設備、強化駐外使館查驗簽證申請人身分之能力、增進洗錢防制及危機預防之功能等。

第二套反恐怖主義措施(Zweites Anti-Terror-Paket)於 2002 年 1 月 9 日完成立法，名稱則改爲反國際恐怖主義法（Gesetz zur Bekämpfung der international Terrorismus）。本法內容相當廣泛，

共涉及修正十七個法和五個命令。修法要點如下：

1、 聯邦刑事局法 (das Bundeskriminalamtsgesetz)、聯邦邊防法 (das Bundesgrenz-schutzgesetz) 、聯邦憲法保護法 (das Bundesverfassungsschutzgesetz)、軍事反間諜局法 (das MAD-Gesetz)、聯邦情報局法 (das BND-Gesetz)：擴大相關安全單位之職權，強化其危機預防及洗錢防制之功能。

2、 外國人法 (das Ausländergesetz)：支持恐怖活動者禁止入境及居留。

3、 安全檢查法 (das Sicherheitsüberprüfungsgesetz)：加強對「安全敏感區域」進出人員之查核。

4、 航空法 (das Luftverkehrsgesetz)：民航機得配置武裝警察。

5、 聯邦中央檔案法 (das Bundeszentralregistergesetz) 、社會法典第十冊 (das Zehnte Buch Sozialgesetzbuch)：放寬資料提供之限制。

6、 護照法 (das Passgesetz)、身分證法 (das Gesetz über Personalausweise)：除照片及簽名外，將增錄持證人之指紋、掌紋或面貌等「個人生物特徵」，以提高證件之防偽和辨識能力。

7、 團體組織法 (das Vereinsgesetz)：以財務支持國外恐怖組織之外國團體或外國人社團將被強制解散。

8、 能源安全法 (das Energiesicherungsgesetz)：保護能源供應，避免遭受破壞。

9、 增訂刑法第 129b 條 (§ 129b Strafgesetz)：將聯邦政府打擊對象擴大至國外之犯罪集團和恐怖組織。

10、 難民程序法 (Asylverfahrensgesetz)：難民申請者之指紋、語言別及其他識別資料將保留十年，並與聯邦刑事局資料互作比對。

11、 外國人中央檔案法 (das Ausländerzentralregistergesetz)：除了保留外國人之簽證申請文件，主管機關之批准或駁回文件亦予保

留，並將檔案作自動化處理，供全國警方連線調閱。[90]

二、 法規範之基礎

第七條　護照法之修改[91]

護照法於 1986 年 4 月 19 日制定，於 2000 年 5 月 1 日修改，再來並於 2001 年 12 月 3 日修改。其修改條文如下：

1、　護照法第四條之修正　　其修正之條文如下

a 在第一項第三款後增加第四款，第四款的條文如下“暫時的護照中含有自動解讀之部分，不再適用”

b)第二項後要再增加第三款、第四款。茲分述如下：

(3)護照除了照片以及簽名之外，亦可另外含有其它的生物特徵。護照持有者的手指或是手或是臉。照片、簽名以及其它的生物特徵，可以以編成數碼的方式

來加密，而保存在護照中。第一項第二款，列出的資料亦可以編成數碼的方式來加密在護照中。

(4)生物特徵的種類，其細節、以及按照第三款編成數碼的特徵跟資料的採用，其儲存、建檔、應用的方式仍將由聯邦法律來規定。而全國性的檔案的建立將不被實行。

c)原本是第三、第四項，現在是第五、第六項。

2、　護照法第十六條之修正　　其修正之條文如下：

a〉　第一項第一款刪除

b〉　第五項之後再增加第六項。茲分述如下：

---

[90] 可參 http://npl.ly.gov.tw/do/www/billIntroductionContent?id=7。

[91] 反國際恐怖主義法的包裹立法的第七條，自然在後續的立法中，就會出現對護照法的最近的兩次修正。

(6)護照含有編成數碼之方式來加密之生物特徵以及資料，只能爲了查驗其文件之真僞，以及確認護照持有者的身分，而以讀卡方式作爲上述之檢驗。若護照持有者想知道其編成數碼之方式來加密的生物特徵以及資料的內容，行政機關即有告知義務。[92]

第八條 身分證法之修改[93]

身份證法於 1986 年 4 月 21 日制定，最近的修正經由 2001 年 12 月 3 日的法律中的 25a 來加以修正修改。其修改條文如下：

1、 第一條 其修正成以下之條文

a)第三項之後要再增加第四項、第五項。茲分述如下：

(4) 身份證除了照片以及簽名之外，亦可另外含有其它的生物特徵。身份證持有者的手指或是手或是臉。照片、簽名以及其它的生物特徵，可以以編成數碼的方式來加密而存於身份證中。第二項第二款，同樣上述第一項第二款中的所列出的資料亦可以編成數碼的方式來加密而存於身份證中。

(5) 生物特徵的種類，其細節、以及按照第四款編成數碼方式來加密的生物特徵與資料的採用，其儲存、建檔、應用方式仍將由聯邦法律來規定。而全國性的檔案的建立將不被實行。

b) 原本是第四、第五項，現在是第六、第七項。

2、身份證法第三條其修改如下：

a)第一項第一款刪除。

b)第四項之後再增加第五項。茲分述如下：

---

[92] 此即所謂導論中所提到的嚴格的目的之拘束〈Zweckbindung〉符合所謂的法律保留原則，也是我國大法官所引進的釋字六 o 三號解釋的生物特徵之使用的合憲審查基準。

[93]反國際恐怖主義法的包裹立法的第八條，自然在後續的立法中，就會出現對護照法的最近的兩次修正。

(5)身份證含有編成數碼之方式來加密的生物特徵與資料，只能爲了查驗其文件之真僞，以及確認身份證持有者的身分，而以讀卡方式作爲上述之檢驗。若身份證持有者想知道其編成數碼之方式來加密的生物特徵以及資料的內容，行政機關即有告知義務。[94]

第十二條　政治難民庇護程序法之修改[95]

政治難民庇護程序法於 1993 年 7 月 27 日制定，最近的修正經由 2001 年 12 月 20 日的法律中的第四條來加以修改。其修改條文如下：

1、政治難民庇護程序法第十六條　　其修正如下

a)第一項修正成以下之條文

aa)第一款中的句子“具有無限期的居留許可或是”刪除

bb)第二款之後，增加如下之句子：

“ 爲確定該外國人之屬國及屬地，亦得採用該外國人在正式聽證音源紀錄或資料紀錄以外，所爲之口頭記錄；惟該紀錄必須在該外國人已被事先告知情況下所爲者，方屬有效。該口頭紀錄將由聯邦官署保存之。”

b)第二項中之片語“認識運用之措施經由片語依據第一項之措施”來取代之。

c)原來第四項第一款中的引號中的“項目一”將再加進“第一款”及“第二款”

d) 第五項第一款改成如下：

---

[94] 關於生物特徵之立法規定在身份證法中與護照法有相同之規定，顯見德國聯邦對生物特徵中之規範適用於本國人已有一致的法律規範。

[95]反國際恐怖主義法包裹立法的第十二條，自然在後續的立法中，就會出現對政治難民庇護程序法的最近的兩次修正。

“因刑事訴訟程序或避免緊急危難之目的，而有確定身份或編排證明文件之必要者，得對第一項所取得文件進行加工與運用。該文件亦得應用於失連者或失蹤者之認證上。.”

e)第六項改成如下：

“(6) 依第一項所取得之文件應於不可撤銷的政治庇護程序確定後的十年後被銷毀。所有相關電子資訊亦應刪除之。”

2 政治難民庇護程序法.第六十三條第四項後增加第五項 “(5)此外外國人法的第 56a 準用之。

d) 第五項第一款改成如下：

“因刑事訴訟程序或避免緊急危難之目的，而有確定身份或編排證明文件之必要者，得對第一項所取得文件進行加工與運用。該文件亦得應用於失連者或失蹤者之認證上。.”

e)第六款如下：

“(6) 依第一項所取得之文件應於不可撤銷的政治庇護程序確定後的十年後被銷毀。所有相關電子資訊亦應刪除之。”

2. 政治難民庇護程序法.第六十三條第四項後增加第五項

“(5)此外外國人法的第 56a 準用之。

參、生物特徵在德國法中生物特徵辨識相關法律規定[96]

護照法

[96] 讀者可能覺得這有點重複，那是因爲包裹立法與個別現行法之規定有層次之區別。所以我們將現行的個別法律中有關生物辨識之運用的相關規定再一次統整如下，希望讀者不要以爲是重複而覺得無聊。

護照法第四條　護照的模式

(3)護照除了照片以及簽名之外，亦可另外含有其它的生物特徵。護照持有者的手指或是手或是臉。照片、簽名以及其它的生物特徵，可以以編成數碼的方式存在護照裡。第一款第二句，列出的資料亦可以編成數碼的方式存在護照裡。

(4)生物特徵的種類，其細節、以及按照第三款編成數碼的特徵跟資料的採用，其儲存、建檔、應用方式均以聯邦法律去管制。而全國的檔案不會被建立。

身份證法

身份證第一條 具有隨身攜帶身份證的義務

(4) 身份證除了照片以及簽名之外，亦可另外含有其它的生物特徵。身份證持有者的手指或是手或是臉。照片、簽名以及其它的生物特徵，可以以編成數碼的方式存在身份證裡。第二款第二句，列出的資料亦可以編成數碼的方式存在身份證裡。

(5) 生物特徵的種類，其細節、以及按照第四款編成數碼的特徵跟資料的採用，其儲存、建檔、應用方式均以聯邦法律去管制。而全國的檔案不會被建立。

政治庇護程序法

政治庇護程序法第十六條 身份確認

(1) 外國人申請庇護者，其身份之確認應經主管機關之認證程序爲之，但未滿 14 歲者不適用之。依第一條規定，僅得對手指之照片及指紋進行拍攝。爲確定該外國人之屬國及屬地，亦得採用該外國人在正式聽證音源紀錄或資料紀錄以外，所爲之口頭記

錄；惟該紀錄必須在該外國人已被事先告知情況下所爲者，方屬有效。該口頭紀錄應由聯邦機關保存之。

(2) 前項程序之主管機關爲該外國人所爲申請庇護之聯邦機關，及該外國人依第十八及十九條申請進行紀錄之機關。

(3) 聯邦警政署提供基於身份確認之目的而依第一項取得之指紋分析之官方協助。爲此，亦得行使其爲履行任務時對其所保存之官方認證文件之運用。聯邦警政署爲保管該文件之理由無須告知第二項所指之機關，但其他法律另有規定者，不適用之。

(4)第一條第一項及第二條第一項所取得之文件與其他官方認證文件之分離保管與揀選辨識，由聯邦警政署爲之。關於資料之加工，亦準用之。

(4a)爲確定外國人之國籍與身份，第一條第一項所取得之資料應送達聯邦行政機關;該資料與依居留法第四十九條之二所取得之資料有相同效力。本條亦準用居留法第八十九條之一。

(5)因刑事訴訟程序或避免緊急危難之目的，而有確定身份或編排證明文件之必要者，得對第一項所取得文件進行加工與運用。該文件亦得應用於失連者或失蹤者之認證上。.

(6) 依第一項所取得之文件應於庇護程序之終局決定作成後，經十年後方得銷毀。相關文件亦應刪除之。

德國居留法[97]

---

[97] 居留法是 2005 年 1 月才頒佈生效的法律，它用以來取代 2005 年 1 月被廢止的外國人法。在

反國際恐怖主義法中只談到外國人法之修正，並未提到德國居留法。所以德國居留法乃是最新的法律，其中有關生物辨識運用之特徵的規定可以當作德國法對生物辨識特徵之規定之最新立法，其亦與歐盟關於生物辨識特徵之規定相一致，且是內國法中的最新規定。但是此乃是對外國人的限制而非對本國人的限制。因此在往後的章節中我們會討論到生特徵之辨識在德國法中之規定，內外國人是有所

第四十九條　身分之確定及保證

(1) 任何外國人皆有義務於被要求時，向被委託執行外國人法之行政機關，爲關於其年齡、身分及國籍之必要報告，及在取得返國文件之限度內，作出其原籍國或可能之原籍國的代表機關所要求，或符合德國法之說明。

(2) 於下列情形，若該當外國人之外形、年齡或國籍存有疑問，則應採取爲確定其身分、年齡或國籍所必要之措施：

一、應許可該當外國人入境或居留時。

二、爲實行本法所規定之其他措施所必要時。

(2a) 於依據第十五條之一進行分發時，外國人之身分應藉由鑑定機關之措施予以保證。

(3) 於下列情形，應實行爲確定及保證身分所必要之措施：

一、該當外國人將或已攜帶僞造或變造之護照或護照代替物入境時。

二、基於其他根據，足以懷疑該當外國人於居留被駁回或終止後，將重新以不被許可之方式進入聯邦領域時。

三、該當外國人因爲被驅離或驅逐，而有可執行之出境義務時。

四、該當外國人被庇護程序法第二十六條之一第二項所謂之第三國拒絕入境或驅離時。

五、原籍國存有返國困難性，以及依據第七十三條第四項所確定之情況，其國民申請超過三個月的居留簽證時。

區別的。關於此點請詳見本文之六「就聯邦國民與外國人的差別待遇」

六、依據第二十四條，以及在第二十三條及第二十九條第三項之情況下，提供暫時保護時。

七、確有第五條第四項所規定之拒絕理由時。

(4) 在第二項至第三項意義下之措施，係指拍攝照片及指紋、進行測量，以及類似之措施。上開措施得適用於滿十四歲之外國人。於無法，或不能及時，或僅能在具有顯著困難性下，以其他方式，尤其是藉由詢問其他行政機關，確定該當身分之情形，始得爲確定該當身分而採取上開措施。

(5) 爲確定該當外國人之原籍國或原籍地區，得將該當外國人之口述文字記錄於聲音或資料載體上。於事先就此告知該當外國人之情形，始得進行上開調查。

(6) 滿十四歲，且將因不被許可之入境被第三國攔截，而未被拒絕入境的外國人，其身分應藉由接受捺押全部十支手指予以保證。

(7) 滿十四歲，且於欠缺必要之居留權下在聯邦領域內停留的外國人，於有根據可證明其已向歐洲聯盟之會員國提出庇護之申請時，其身分應藉由接受捺押全部十支手指予以保證。

(8) 該當外國人應忍受依據第二項至第七項所採取之措施。

再者，尚存在若干在歐洲層次上之預先規定，惟其並未就在證明文件中生物辨識資料之整合，對立法者作特別之要求。此外，從歐洲之面向觀之，亦未要求此類整合。

肆、憲法上的基礎暨聯邦憲法法院的諸判決

因爲人們得以藉由生物辨識資料而回朔追蹤系爭當事人的身分

證明，亦即人與事上的關係。因此，由專家的觀點來看這樣的資料。因此，就生物辨識資料的取得、加工、儲存與運用上需注意下列事項：

◎法律基礎不但要合於目的拘束原則，也要合於節省資訊儲存的原則。

前述第一項的內容是：生物辨識資訊指的就特定可藉分之目的被取得與被運用。第二項是說：對必要的儲存空間資源與前作業時間之減少。

在憲法層次上最重要的是資訊自決基本權，是項基本權係由聯邦憲法法院 1983 年的人口普查判決〈Volkszählungsurteil〉所支持。其意爲「對個人的私人資訊無限制的取得、儲存、運用與移轉的保護」。

資訊自決權並不是無限制受保護的，因此依聯邦憲法法所列的項目是可對資訊自決權進行干預。例如人口普查判決的第二要點:

「對此項資訊自決權的干涉只有就大多數的普遍利益才許可。是項干涉需要合憲的法律依據。且此項法律依據必須符合規範明確性底法治國要求。立法者立法時需進一步注意到比例原則。立法者還需針對導致對人格權侵害危險採取組織上和程序法上的預防措施。依規範明確性的原則，不確定法律概念或一般條款在法律中均不得使用。國民也必須得認知，法律就何種行政執行底具體目的規定其屬人資訊。

資訊自決權原則上禁止去取得加工及利用系爭當事人的個人資料。只有在有合於聯邦憲法法院列舉的要求的法律依據下，該禁止才得加以廢棄。在當事人同意的情形下，亦得對資訊自決權進行干涉。不過當事人的同意必需視在自願表達與自主決定的情況。

聯邦憲法法院在人口普查判決中明確強調禁止依不確定的目的

的資訊儲存。資訊的強制取得，依照聯邦憲法法院的見解，必須以立法明確的規定使用目的以及這規定合於本法目的且爲必要時才可。

依照聯邦憲法法院的判決，資訊自決權保障的是「個人的權限，自己就其私人資訊的使用與拋棄去作決定」。個人有權利「去知道何人、何時、何事以及就何種事務對他有所知悉」。

對個人而言，應要求國家資訊處裡的最大可能的透明度。也就是說，對當事人有重大意義的是個人關於他自己的資訊的探問權。相對應於個人基本權利中的管制權，防禦權和形成權等。對於以個人爲基礎建立起得資訊則可行使報告、禁止、刪除與異議等權利。

伍、在反國際恐怖主義法（Gesetz zur Bekämpfung der internationalen Terrorismus）中生物辨識手續展開規定之討論

藉由 2002 年 1 月 9 日的反國際恐怖主義法有多達 21 項法律與行政命令中的條文被修改與新增。在 2001 年 9 月 11 日的恐怖攻擊後的立法活動有如下的發展：

〈1〉多項安保官署的權限被立法者擴大了

〈2〉行政官署間的資訊交換較以往容易 h

〈3〉「在護照及身分證以及外國人身分證明上採用生物辨識特徵」被加以規定。

以下本文的上述〈3〉分析乃著重於：

依照立法者的意思，護照與身分證法基於證件且藉助於電腦對

人所爲的身分確認應再作改良，以求避免產生有人使用其他容貌近似之人的證件。因爲這個原因法律草案乙預見在護照與身分證件上應在照片與簽名之外亦採用其他的特徵。立法者就在護照和身份證上採行生物辨識特徵的作法不僅限於聯邦國民，亦及於在外國人法及庇護聲請程序法中新增的規定。在外國人與庇護聲請人的証明文件上採行生物辨識特徵。

依照舊版護照法第 16 條第 1 項第一句的規定：護照上既不得有護照所有人之指紋，也不得有其他個人密碼。本條的背景乃係在護照和身分證上不得有對每一證件所有人可讀與可理解的資訊。因此，如要藉由反國際恐怖主義法引入取得生物辨識特征及其密碼化的措施，便需修改本法之規定。

考慮到資訊保護法上的重要性，立法者進一步制定了護照法第 16 條第 6 項的規定：護照上的密碼，只得用來判別文件之真僞以及護照所有人的身分。此外，護照所有人也有權獲知密碼內容及要求官署提出說明等等。

在身分法第 1 條第 4 項及第 5 條新增的規定在內容上與護照法第 4 條第 3 項與第 4 項的規定一致。因爲要全面性的保護旅遊文件免於僞造，則不能只限於護照，必須將身分證件也列入。因這些證件爲許多歐洲國家承認爲旅遊文件中，除了護照法的規定外，涉及資訊法上保護的規定尚有：身分證法第 3 條。身分證法第 3 條第 5 項規定的內容如同護照法第 16 條第 6 項也是針對密碼化的特徵之使用目的及相關當事人的詢問權〈Auskunftsrecht〉。

藉由反國際恐怖主義法的制定，使得外國人法第 5 條新增了 6 個條項。以往外國人法並未針對居留項目作規定。新增的條款提供了對居留許可統一的表格樣式。依此方式，在填寫居留許可的表格時採用了多項身分証明特徵：

〈1〉第 5 條第 2 項：在外國人的護照上加貼標籤

〈2〉第 5 條第 2 項：在外國人的護照上附加獨立文件

在上述〈1〉與〈2〉兩種情況下，依據外國人法第 5 條第 4 項的規定得在照片與本人簽名外加上來自本人手指或手掌與臉部取得的生物辨識特徵。在這件事情上，這些特徵得以製作成條碼的安全程序附在居留許可上。本條的內容與護照法第 4 條第 3 項及身分證法第 1 條第 4 項的規定相同。

除了爲居留許可之目的外，生物辨識特徵尙可被運用在不同的外國人證件表上。如：

Ausweisersatz〈外國人法第 39 條第 1 項〉

Duldungsbescheinigung〈外國人法第 56a 條〉

Fiktionsbescheinigung〈外國人法第 69 條第 2 項〉

陸、就聯邦國民與外國人的差別待遇

由於 2002 年 1 月 1 日生效的反國際恐怖主義法（Gesetz zur Bekämpfung der internationalen Terrorismus）有諸多具體的法律基礎被創造出來，這些法律基礎允許在護照及身分證以及外國人的身分證件上採行生物辨識特徵。然而本法的施行仍要依施行細則，此施行細則應就生物辨識特徵的取樣樣式加以規定，在此有一項區分是立法者認爲對於外國人的身分證件上採行生物辨識特徵只要有行政命令爲依據便可。是項行政命令至今尙未被公佈。

緊接在 2001 年 9 月 11 日的恐怖攻擊後，生物辨識系統（biometrische Systeme）在反恐措施中受到了特別的關注，該項系統從事於辨識與證明。舉例如聯邦犯罪局（Bundeskriminalamt）所用於現有生物辨識手續的自動指紋辨識系統（automatisiertes Fingerabdruck-Identifizierungssystem，AFIS）將來自刑事聲請庇

護程序所得之指紋鑑定資料存於資訊銀行中。該系統自 1992 年啓用後將指紋以數位化的方式儲存，且儲存個人資料及全部十隻手指；此外尚包含追蹤（蹤跡）資料暨未歸屬建檔之指紋。AFIS 系統之使用不全爲警察業務，尚及於爲外國人法的目的。自 1993 年庇護程序法（Asylverfahrensgesetz）第 16 條便規定：年滿 14 歲以上及未擁有不限期居留許可的庇護申請人，必須接受鑑識上的處遇。本條的目的在於避免因當事人多次的聲請而必須做不同的身分認定。

上述的作法在以往並不適用於聲請庇護或戰爭難民等，因爲以往依外國人法第 41 條規定，對外國人作身份鑑識只有在對其身分有疑問時才許可。而庇護聲請人與戰爭難民，其依 1997 年新增的外國人法 41a 條地位等同於庇護聲請人。庇護程序法第 16 條此種針對特定群體的立法對當事人資訊自決基本權的保障引進了相當的疑義。

如前所述，對外國人的身分證件上採行生物辨識特徵只需有行政命令爲依據即可。依據外國人法第 5 條第 6 項，是項內政部的行政命令須由聯邦參院批准。這方面的憲法上依據是基本法第 80 條。依基本法第 80 條第 1 項第 2 句法授權之內容、目的與範圍須於法律中明定。聯邦憲法法院爲此發展出許多不同的公式。其中最重要的是針對授權的目的，因爲當授權之目的確定時，授權之內容與範圍則可順利被推導出來。

因此，我們在這裡遇到的問題便是，依照基本法第 80 條第 1 項第 2 句的規定，即令今日對外國人的身份證件上採行生物辨識特徵在外國人法和庇護程序法中有授權以行政命令爲之，然而其目的因爲內容上無法具體而沒有辦法確定。

對資訊自決基本權的干涉，依聯邦憲法法院的裁量需要有合憲的法律基礎，且對基本權限制的要件與範圍依該法是明確的且對

人民而言是可認知的，此外，該項法律基礎要合於規範明確性的法治國家要求。依此看來，雖然聯邦憲法法院並未要求對資訊自決基本權的干涉一定要有形式的法律爲基，然而其必須有事實的理由去對聯邦國民與外國人做差別待遇加以正當化；因此，我們在此看到，就護照何身分證件上採用生物辨識特徵的作法，就聯邦國民而言，需要有形式法律，但對外國人只需有行政命令爲基即可，這項差別待遇是牴觸平等原則的。

柒、生物辨識特徵的種類與其細節之討論

就生物辨識特徵的種類與其細節係規定於護照法第 4 條第 4 項第 1 句及身分證法第 1 條第 5 項第 1 句中。然而上揭條文並未明定個別的生物辨識特徵。上揭條文只規定由哪些身體範圍可取得生物辨識特徵。如手指、手掌與臉部。有疑問的是就立法者所列舉的這些生物辨識特徵是否可替代或增加。由法條的文義來看這個問題並沒有解答。由立法理由來看，依立法者的意思，就這三類身體範圍是可被互相取代的。

實際上立法者的這項限制，亦即只允許上揭身體範圍互相被取代，在生物辨識系統的框架下，錯誤辨識是會造成問題的。在高度安定的要求下，如果僅是限於個別的生物辨識特徵，而不考慮就不同特徵的結合，則在任務上產生的錯誤辨識率不一定能被接受。但是立法者允許的上揭身體範圍限制了其他系統之適用。

例如以虹膜辨識（Iris-Erkennung）爲基之生物辨識邊界管制系統，便不包含在立法者的文義中。

採用生物辨識特徵遇到的另一項問題是護照與身分證的有效期間。證件的效期是法定的，如依護照法第 5 條地 1 項規定護照的效期是 10 年，對於未滿 26 歲之人爲 5 年。立法者就較短效期的

規定的考量即是在於這些群體之人，其身體之發展在這個年紀尚未完成。這樣的情形會導致人的外貌仍有快速的改變，而其戶照上的照片在短短數年內可能與本人不符。同樣的情形在身份證所有人（依照身份證法第二條第一項第二句規定）。對年輕人所爲之臉部辨識也比成年人出現較高的錯誤比。採生物辨識特徵也會遇到類似的問題，也就是說這樣的作法只有再有限的時點內可行。因此採行特定生物辨識特徵時也要注意確保其仍在文件的整個效期內。在十年內的有效期內，是否或多久對生物辨識特徵的採用，有賴於進一步對生物辨識系統的專家研究。對護照與證件效期之縮短可能是不切實際的。就現有生物辨識特徵之使用首先要問的問題是，非生物辨識特徵如照片與簽名等之使用在護照與身份證件上，是否不能達到法律上就採行生物辨識特徵之目的，”審查當事人身份是否與儲存於文件中之原始資訊一致　“。

本人之照片亦購成爲一項生物辨識的特徵。其實技術上也可能做到以照片與本人作比較，只是至今爲止，照片仍不能滿足質上的要求。因爲照片的品質取決於光照的比例。由聯邦印刷場所發展出的驗證〈verifier〉，據稱可將傳統照片以數位圖像方式印在護照尙且在一秒之內便可藉由驗證〈verifier〉加以判讀。

雖然在實際使用上護照照片仍不合於生物辨識特徵，但是我們仍然可以考慮去改良身份證照片的品質以求合於新法上就辨識目的的要求。

捌、由手指或手掌或臉部取得生物辨識特徵之技術與法律之規定

一、 臉部平面圖（Gesichtsgeometrie）

立法者有明示提及臉（Gesicht）這個生物辨識特徵的問題是在

於，高品質的要求在重複辨識上是否仍可達成，在實務上仍有極大的阻礙，例如一項在紐倫堡

機場作生物辨識的駕駛計畫使是失敗的，因爲品質無法達到要求。要達成好的結果需要理想的打光條件以及對臉部正前方做好的掃描。在實務上，這些條件仍未能獲得保障。

二、指紋

指紋是另一個生物辨識特徵。在這裡會面臨的問題是手指受傷的情況。以前便有過，有人的指紋相當難辨識，或由於物理上得原因不適於生物特徵辨識手續。

三、手掌平面圖

在手掌的情況面臨的問題是與指紋類似的。如在手掌受傷的情況。

玖、結語

立法者將取得生物辨識特徵之來源限於"手指"，"手掌"及"臉部"等三項且一開始便排除多項特徵之聯結。此項限制依今日科技水平在考量生物辨識系統的錯誤辨識上並非是沒問題的。而且在計畫使用生物辨識手續上也需考慮到，以今日科技水平，尚未達大量使用的程度。吾人對生物辨識系統的功能要求很高，在運用生物辨識程序常會出現附帶資訊。也就是說，原始資訊（Rohdaten）常會顯示出本人更多的訊息。依比例原則的要求有必要儘量減少採行生物辨識特徵附帶的副作用。

如不儲存原始資訊。考慮到在外國人法中新增的對外國人的生物辨識資訊的使用許可，便有必要注意到不讓這些特徵包含附屬資訊，以求避免對上述資訊之違反目的之利用。

因爲立法者授權可將特徵以制作條碼的方式整合進文件中，也因此產生以下的問題，要採用何種方式也就是說如何將具生物辨識的資訊以電子訊號方式記錄下來。此外，應如何截取電子訊號也是問題。

在資訊保護法中包含一項由資訊自決基本權導出的嚴格的目的拘束原理。就聯邦國民而言，只在爲了辨識文件的真僞及身份確認的情況下，方對生物辨識特徵加以使用，因此合於目的拘束原理。但不同於聯邦國民，對外國人，外國人法第五條第七項所規定的總量處理權限（pauschale Verarbeitungsbefugnis）便不合於憲法上的目的拘束的要求。生物辨識特徵有各種不同的儲存可能。對聯邦國民而言，其生物辨識特徵的集中儲存已由法律上加以排除。反之外國人便沒有而爲外國人的集中資訊設施違反基本法第三調的平等原則以及比例原則。

就外國人的生物辨識特徵之儲存，除了儲存在證明文件之外，可能是只有在地方或中央的外國人事務局（Ausländerbehörde）才可想像，但在這件事情上可能仍必須以法律規定一項完全拘束於資訊儲存的目的。

生物辨識資訊的儲存是專屬於個人的權利。而且只有儲存於護照和身份證上才合於使用目的。同時此等作法才合於比例原則與節省資訊儲存原則。

第六章　歐盟之制度沿革與實踐現狀

壹、歐洲理事會相關公約與報告

一、相關公約與報告

（一）Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data，Oviedo, 4.IV.1997（108）

（二）Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data (2005)

二、公約立法背景

由於在六零年代初期，電腦資訊處理及大型資訊庫的興起，提供了處理個人資訊極大的便利及效率，大量以電子方式儲存個人資訊的應用開始蔚爲潮流。順應時勢，歐洲理事會遂決定建立相關處理原則，以避免個人資訊不正的收集與處理。在 1973、1974 年間首先做出 22 及 29 號決議，建立起公私部門的資訊庫保護原則，但實際運作之後發現唯有將該保護在各內國法中落實，否則很難真正有所建樹。1981 年，在歷經四年的協商談判之後，108 號公約拍板定案。簽約國在其內國法中，必須落實保護個人資訊範圍的原則。此原則特別是涉及公正合法的收集處理資訊、限制法定目的的資訊儲存、其同時關注資訊的性質，特別是必須符合比例原則、正確性、敏感資訊的保密、資訊主題的資訊以及個人的使用及改正權。且在各契約國間的個人資訊，除非有保護程度不一或其中一方爲非會員國的情形，否則一律容許自由流用。該

公約建立一個由公約各會員代表所組織而成之諮詢委員會（T-PD），負責說明公約規定以及確保公約落實的進展。該委員會乃致力於各資訊於不同國家或組織之間的流通互用，包括歐洲共同體、非公約會員國等。

三、公約內容及後續實踐情形報告

關於上述所提到的第 108 號公約，爲了各該不同體系的需要，公約的規定勢必需要更進一步的精緻化，相較於修改公約或是增加協定，歐洲理事會傾向以對各政府的建議形式爲之。這樣的建議有較易起草、採用及落實的優點，以歐洲執委會全體通過的方式取代逐一經各會員國簽署批准的過程。且雖然其不具法律拘束力，但卻提供了無論是會員或非會員國一明確的參考標準。爲了起草各該建議－此除了需要法律經驗外，尚還需要建議主題之專業知識－歐洲執委會在 1976 年建立資訊保護的專家委員會，而此單位隨後演變成爲資訊保護的計畫團體（CJ-PD）。該委員會是由 44 個會員國中負責資訊保護的代表所組成。當處理各領域建議事項時，各代表有時亦會由該領域專門顧問陪同參加。而歐盟在與其權限相關的範圍，亦參加該建議的起草。雖然上述兩個委員會是在相近的研究範圍中運作，但其活動相異：T-PD 乃是公約的守護及推動者，而 CJ-PD 則起草在各領域中較技術及細節的指導方針。

T-PD 最近已對涉及警察單位個人資訊使用的建議以及刑事案件互助資訊的相關報告做出評估。現正準備就監視錄影帶、智慧卡、生物辨識等領域作出報告，並就各該領域評估個人資訊之保護問題。　　此篇報告原於 2003 年由執委會贊助 CJ-PD 研究，並以德生物科技公司 CEO Mr. Marcel YON 之研究報告爲根據而

成。但於其後由 TPD 接手，歷經 2004 年及 2005 年的研究，作成以 Mr. Alexander PATIJN,荷蘭司法部司法總長所擬草稿爲底之報告。並於 2005 年 2 月的會議中公佈，以下將扼要敘述公約與該公約實踐情況報告之內容。

（一）第 108 號公約適用於生物特徵方面之時點

本公約適用於個人資訊之自動處理部分。個人資訊的定義乃是含有特定或可特定人資訊之資訊。但生物特徵是否構成此處的個人資訊，則饒有爭議。有論者認爲我們可能沒辦法從像是不完全的指紋來特定出某人，甚言之，即使是含有生物特徵的資訊，亦不一定即會揭露關乎個人的資訊。另一方面，亦有人反駁生物特徵既然對個人而言是終生獨一無二，則其自然可特定出個人，在未來的科技也許就能很輕易的透過生物特徵來辨認出某人。委員會則認爲上述的爭論乃不必要，只要生物特徵是爲了自動處理而收集的，則其即有與特定或可特定之人相關的可能性，也就是公約所適用的情形。

（二）何者將爲管理人

管理人乃是決定資訊用途、應該收集的資訊種類以及其用法之人。適用公約時必須要有有人負責維護個人資訊保護的原則，而該人即會被稱爲管理人。在生物辨識的情況中，有時並不是那麼容易去確定管理人究竟爲何者。以護照發放爲例，核發機關將有權處理該資訊，但儲存的資訊種類以及其使用皆是由立法者所決定，此時立法者應同時規定究竟何者應承擔相關責任。又或者在有多數管理人的情況，則當中每一個人都應該對公約所規定之責任負責。有時候尚會出現由承包商代表管理人職責的情形，但在此時，管理人的責任並不因此而有所減縮，承包商依 directive 95/46 第二條第 e 項的規定，將被視

processor。在這各式各樣複雜的情形當中，確定何者爲管理人，並讓資訊主體能清楚得知該資訊，乃爲必要的措施。資訊主體有權不須經由複雜且吃力的搜尋，就可知道該向誰提出可能違反資訊保護原則的質疑。而不是讓他們非得經由訴訟才能得知，究竟何者會願意或者會被迫來承擔這項責任。

（三）公正且合法的程序

個人資訊應該公正且合法的取得及處理(article 5, paragraph a.)。公正是個很廣泛的概念，在生物辨識的方面，則是特別反應在須於收集個人資訊時先予告知。資訊主體必須知道該收集成果的用途及管理者的身分。理論上，生物特徵第一次的收集（登記資訊）不是出自法律的強制，就是自願。在私法領域的應用上，則多是以自願的方式爲主，當事人是有選擇要或不要的自由的，例如銀行所發放的智慧卡即是一例。但委員會同時也注意到，隨著此類技術的大量運用，以及相關條款多以定型化契約方式呈現，事實上只要想正常的參與日常生活，即需要選擇接受生物辨識方式，因此所謂的選擇自由實際上可能是不存在的。

至於在其後爲比對原始資訊的後續資訊收集過程當中，要注意的則是非正式資訊、往來資訊或相關資訊等額外資訊的問題，這些資訊通常是會指出資訊主體何時及何地使用該系統的資訊。生物辨識系統通常會被設計一併收集該類資訊，但從該類資訊當中，卻能側寫出該人的舉止以及其他資訊。在此部份，爲符合公平原則，資訊主體應被告知每次的相關資訊收集。且該相關資訊的使用應不能與原始資訊收集的用途互相矛盾。

（四）目的之限定與特定技術之選定

個人資訊的處理用途必須要特定且合法。當決定使用生物辨識系統時，亦應同時確定資訊的用途並令其詳細明確。且一旦選定資訊用途，則即應排除多餘的生物資訊或相關資訊收集。並配合該用途選定確認或者辨識系統。委員會並不特定建議應採用何者爲當。但只要確認的系統技術其實已足以完成該資訊用途，則更進一步選擇辨識系統即需要合理的理由始可。

（五）非過度

生物資訊要特別注意的是，其有可能會包含除了查核或辨識個人身分所需以外的資訊。爲了要避免涉及不需要的資訊處理，故在登記及後續過程中，在儲存及使用資訊部份都針對使用目的而限制其抽取的資訊，此在技術上即稱爲樣版。該擷取的資訊應注意不應涉及不必要的資訊，特別要避免敏感資訊的揭露，例如虹膜的使用即爲一例，整體虹膜的狀況可能會揭露出疾病的存在。擷取樣版的方式就像是從一篇未保存的文章中截取出關鍵字一樣，之後再以同一篇文章比對其關鍵字是否相合即可。以樣版方式進行生物特徵還有一好處，就是如同我們不能從片段的關鍵字拼湊出原文一樣，從樣版的生物特徵資訊也無法重建全面的生物狀況。但此方式對某些辨識用途而言足堪適用，但對類似犯罪偵查等情形可能就無法滿足其需求。另外在相關資訊的處理與儲存也應注意非過度的限制，該資訊之使用儲存不應比該用途所需來的更長。也因爲如此，相關資訊的使用目的應該在系統建構一開始就要確立。

（六）準確性與或然率

個人資訊本身應該力求準確。但如同前述，生物辨識系統有著本身無法避免的或然率特性，即使所得資訊正確，其在處理的過程當中議會發生錯誤，而使某人被錯誤的拒絕或接受。另外雖然生物特徵原則上是終身不變的，但經由年齡、疾病、手術等因素，仍然有改變的可能性存在。是故一旦註冊資訊的準確或相似程度已不符該資訊用途需求時，即應該容許資訊主體修正的要求。

（七）資訊保存

個人資訊的保存不應較其原本收集用途所需來的更長。對於生物特徵資訊，此方面應不大有問題，在第一階段的登記過程中，由於生物特徵資訊本來即是設作爲辨識身分的工具，只要其辨識身分的用途仍在，則即可在儲存工具中保存，使其能完成辨識目的。而在第二階段收集資訊與原始登記資訊比對方面，原則上該後續階段所收集的資訊應立即刪除，除非有特別的情形，例如懷疑有冒用身分等情況發生時才會產生例外。

在此比較有問題的是相關資訊的部份。相關資訊的收集可能是爲了其首要目的，例如在核子建築中，需知道何人進入、何時進入、停留時間多久等資訊，也可能是爲了次要目的，例如在辨識身分的生物辨識中，經由遠距離但短時間的身分辨識，可合理的懷疑有身分冒用的情形出現。但不論是基於何種目的而爲收集，系統皆應配合該用途，令相關資訊的保存時間特定且明確。

（八）敏感資訊

生物特徵資訊可能會揭露疾病或種族等資訊。第六條將此定義爲需要特別安全機制防護的資訊種類，亦即爲敏感資訊。隨著科技的發

展，生物資訊可能會指出某些我們預想不到的資訊。而委員會也承認此種情形可能是無法避免的，就像是從名字能夠看出該人種源的情形。因此選擇生物特徵資訊應盡量避免會與敏感資訊相關的部份。對於未來科技可能揭露無法預料的資訊部分，更應小心此部分資訊的應用，避免造成就長期而言，不樂見且無法逆轉的副作用產生。

（九）資訊安全

第七條的規定乃有關於提供個人資訊保護的適當安全機制。包括硬體及軟體的選擇，在此個人資訊保護機關應配合公約的落實而制定相關技術標準。而另外就人員的訓練及其操作程序也屬安全性中重要的一環。系統人員應對自己在該辨識系統的責任有所認知。

另外系統應定期的受到審核及評估。如果適當的話，最好以一獨立機構，來負責資訊的登記、除存、應用、錯誤率、各階段的加密等部分的監督。而在各階段加密的技術，亦能使他人不法取得及使用資訊的風險降低，令其即使截取資訊，若無破除該密碼，仍然無法使用。

（十）透明化

關於生物辨識系統的存在、該系統的用途、管理人的身分及所在地等皆應向資訊主體以及一般大眾予以公告。特別是系統的用途可能有部份不明的時候，管理人更應主動告知資訊主體及相關大眾該系統的用途、其使用方法及可能風險等。而透明化的原則就資訊請求方面時亦有適用。任何違反透明化原則的情形，都應該建立在 108 號公約第九條的規定之下，亦即必需有立法規定，並基於內國利益如公共安全等考量時始可爲之。

（十一）使用之權利

資訊主體對於與本身有關的生物特徵資訊及相關資訊皆有權接觸使用。資訊主體對於確定及身分的資訊，由於無法排除其竄改或質量不佳的可能性，其仍有核對的切身利益存在。故對其名下的生物資訊，應立刻應其要求而搜尋之。另外由於年齡、意外、手術等情形，資訊主體可能會有發現其登記資訊的準確度已有瑕疵的情形，在此委員會認爲該瑕疵補正的要求乃包含於接觸使用資訊的權利之內，故即使資訊主體並未對此要求提出相當理由，該請求亦需受到重視。而資訊主體所獲得的個人資訊應以易於理解的型態呈現，這意味著相關的工具儀器以及專家講解乃是必要的，管理人不可以缺少是項裝備或人力爲由而拒絕資訊主體接觸資訊。當然這部分亦會有權利濫用的疑義，對此依照公約第八條第 b 項之規定，對於太過頻繁的資訊使用要求乃是可以拒絕的，在此只需提供在合理間隔之下要求的資訊。而對於有理由懷疑其冒用身分的情形，資訊管理人亦應盡其最大的努力予以調查。

委員會基於資訊保護的觀點，對於生物辨識進行初步的討論。許多的問題仍然懸而未決。但委員會發現，儘管從公約起草以來科技大量的改變，但許多原則在生物辨識系統使用部分仍然有其適用。此報告反映了法律原則與這些新技術的關連，並希望能促成關於國際與國內間關於人權及生物辨識之間關係更多的討論。未來委員會將會隨時進一步更新報告，並在發展成熟時起草法律文件。

（十二）改正與消除之權利

生物或相關資訊可能會有不正確的情形，資訊主體應可請求對其改正或消除。

在生物辨識系統當中，其準確度乃基於該目的要求，由管理人選擇出適當的標準採行。資訊主體不能一味要求要達成絕對的準確程度。在此由於該系統無法避免的或然率以及生物資訊仍有隨著年齡、疾病或手術改變的可能性，該資訊將有錯誤的機會存在，故改正的權利乃是必要的。而與改正的權利相關的，是在該生物資訊儲存違法時，資訊主體將有請求其刪除的權利。

關於生物資訊，管理人及資訊主體可能會對該系統錯誤率的接受程度產生爭議。原則上，如果資訊主體要求要進行新的登記，即使管理人不承認該登記資訊存在錯誤，在不致於過度花費的情況下，基於資訊主體的改正權利，都應容許其再次登記。這在生物特徵原本正確，隨著年齡等因素而有出入的情況亦應適用。隨著時間的經過，生物資訊可能會逐漸的變得不盡正確。

（十三）有效的救濟

每一個人在其上述接觸使用資訊或改正消除資訊等的權利未受滿足時，皆應有權得到一有效的救濟。該原則在生物辨識部份，由於該系統本身的或然率特性，而顯得更加重要。選擇使用生物辨識是管理人應對此風險負責，而不應由資訊主體承擔其不便。故隨著情況的不同，資訊主體應該可以尋求立即的救濟管道，或者得到盡速的複查。

在現階段，委員會特別強調：

1. 生物特徵被視爲從人體取得的一項特別資訊種類，在不同的系統，以及終其一身皆會相同不變。然而，它們仍有改變的可能性，例如經由年齡增長、疾病或外科手術等。

2. 在決定依靠生物特徵之前，管理者應一方面衡量其對資訊主體私生活所產生的優點及缺點，一方面衡量其預期的用途。並考慮其他對私人生活較不侵犯的選擇。
3. 不能僅因便利而選擇採用生物特徵。人性尊嚴也同樣會影響到生物特徵的使用與否。社會文化以及對於將深以當作器具使用的抗拒都應該考慮在內。
4. 生物資訊及其他系統所生相關資訊，皆應基於合法、特定且明確的用途上處理。其他與原本用途不相容的處理，均爲不被容許。
5. 資訊對該用途而言，應須適當、相關且不應過度。系統在技術面應排除對該用途而言非必需的生物或相關資訊收集。當部分的樣板收集及已足夠的時候，整體狀況的收集或儲存即應避免。
6. 在選擇系統結構方面，管理者應衡量對資訊主體私人生活所造成的優缺點以及預設的用途。合理的選擇應注意資訊安全考量，在儲存於個人器具、分散的資訊庫或中央資訊庫間抉擇。
7. 生物辨識系統的結構不應與該處理用途不成比例。因此，一旦確認的結構即已足夠，則管理者就不應該進一步選擇辨識的方式。生物特徵若只供確認之用時，則最好應儲存於個人儲存工具中，例如智慧卡，其僅由資訊主體持有。
8. 除非資訊主體已知，否則該系統用途以及管理人身分都應對其告知。至於在確保系統公正性的情況下，應告知其被處理的個人資訊以及該資訊可能被揭露的對象。
9. 資訊主體對與自己相關的資訊，皆有權使用、改正、阻止、或消除之。此權利延伸到自身權利的處理過程方面，包括相關資訊（例如使用該系統的時間及地點），以及流傳的對象。

10. 管理人應就保護生物及相關資訊不受意外或故意的刪除、進入、修改或不法使用部分，預見其適當的技術及組織措施。
11. 核定、監控以及管理的程序，如果適合由一獨立組織爲之，則應設立，特別在大量適用的情形，包括軟硬體的標準、負責登記及配對的人員訓練等。建議應固定週期對該系統進行審核。
12. 如果因爲生物辨識系統，資訊主體被拒絕認可時，應依其要求重新檢驗，並應在需要時提供其他恰當的選擇。爲防所謂系統錯誤的情形，該程序應該適當且令資訊主體得知。

四、小結

由上揭公約內容及報告內容可知，本公約適用於含有特定或可特定人資訊之個人資訊之自動處理部分。其目的乃是規範各會員國必須遵守上揭規範，包括在取得個人生物辨識特徵時，應於收集個人資訊時先予告知，且資訊主體必須知道該收集成果的用途及管理者的身分，而個人資訊的處理用途也必須要特定且合法；而在蒐集生物辨識特徵的過程中，有可能會包含除了查核或辨識個人身分所需以外的資訊，此時該擷取的資訊應注意不應涉及不必要的資訊，特別要避免敏感資訊的揭露。

此外，各會員國也應容許資訊主體，對於與本身有關的生物特徵資訊及相關資訊皆有權接觸使用。資訊主體對於確定及身分的資訊，由於無法排除其竄改或質量不佳的可能性，其仍有核對的切身利益存在，原則上，如果資訊主體要求要進行新的登記，即使管理人不承認該登記資訊存在錯誤，在不致於過度花費的情況下，基於資訊主體的改正權利，都應容許其再次登記，以爲救濟。

貳、歐盟制度沿革與實踐現狀

一、前言

近年來隨著科技的進步，國家掌握人民身分的技術也隨著日進千里，英國日前通過身分證法，將建立一個儲存各種人民的生物特徵，主要包含指紋(fingerprints)、虹膜(retinal pattern)、DNA等資訊的資訊庫。

而除了英國之外，歐盟在其個人資訊保護指令(Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data)後，也陸續發布不少與生物特徵相關之法令，以下將先列舉其主要內容涉及生物特徵之歐盟法令，並依各法令的主要規範領域爲區分，將下揭各法令區分爲三大部分—涉及航海員部份的生物辨識特徵法令、涉及護照簽證與中央簽證資訊系統的法令、以及涉及申請臨時避難所與都柏林會議的法令；其次方就分別就涉及指紋之法令一一爲介紹，惟應予說明者係，目前歐盟似仍無以「虹膜」此項生物特徵爲辨識方法或搜集此項生物特徵之法令。

（一）涉及航海員部份

1. 2005/367/EC

2. SEAFARERS' IDENTITY DOCUMENTS CONVENTION (REVISED), 2003

（二） 涉及護照簽證與中央簽證資訊系統

1.Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and

travel documents issued by Member States

2.2004/512/EC

（三）申請避難相關程序與都柏林會議

1. 2006/188/EC

2. Council Directive 2005/85/EC of 1 December 2005 on minimum standards on procedures in Member States for granting and withdrawing refugee status

3. Protocol to the Agreement between the European Community and the Republic of Iceland and the Kingdom of Norway concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Iceland or Norway

4. Agreement between the European Community and the Kingdom of Denmark on the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in Denmark or any other Member State of the European Union and Eurodac for the comparison of fingerprints for the effective application of the Dublin Convention

5. Commission Regulation (EC) No 1560/2003 of 2 September 2003 laying down detailed rules for the application of Council Regulation (EC) No 343/2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national

6. Council Regulation (EC) No 343/2003 of 18 February 2003

establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national

7. Council Regulation (EC) No 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No 2725/2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention

8. Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention

9. Decision No 1/98 of 30 June 1998 of the Committee set up by Article 18 of the Dublin Convention of 15 June 1990, concerning provisions for the implementation of the Convention

二、相關法令介紹

（一）在涉及航海員部份的生物辨識特徵法令中，主要規範在航海員的身分證明文件上所必須包含的資訊，其中包括身體各部份特徵，特別是指紋此一生物辨識特徵。且該生物辨識特徵的紀錄與留存，必須在符合一定條件下，諸如不侵犯航海員的人性尊嚴及隱私權，且能兼顧航海員與政府機關的便利，方得爲之。

1.SEAFARERS' IDENTITY DOCUMENTS CONVENTION (REVISED), 2003

如上所述，本法後來經 2005/367/EC 決議授權歐盟各會員國批准相關內容。

第 3 條(目錄與格式)

第 8 項規定主要規範那些符合本法 Annex I 所列清單的生物特徵樣本或其他樣品之持有者，也應該被包含在航海員的身分證明文件上，並以同條項下之各款條件都被滿足爲前提，該各款條件包括：

(a) 該生物特徵能夠在隱私權不被侵犯、或並未造成身體、健康上不適、或並未損及尊嚴的前提下被獲得。

(b) 該生物特徵能夠在文件上直接以目視的方法知悉,而無法從該樣本或其他樣品中被重組。

(c) 用來確認生物特徵的採樣器材必須是容易使用的,且必須能夠以低價讓政府獲得。

(d) 用以確認生物特徵的器材必須在那些有權機關經常用來確認生物特徵的地方,像是港口或包括船板在內的其他地方，能夠很方便且可靠的被操作。

(e) 使用生物特徵的系統(包括器材、科技、及程序)必須被用來提供一致且可靠的結果用以作爲身分確認。

而附件 1 的 III 係規定航海員必須提供：

(a)航海員全名

(b)性別

(c)出生日與出生地區

(d)國籍

(e)任何有助於辨識航海員身分的身體特徵

(f)簽名

(g)期滿日

(h)文件種類或名稱

(i)獨特文件號碼

(j)個人身分證號碼(非必要)

(k)指紋樣本

(l)一個機器可辨識、且符合在上述文件 9303 中所提到的國際民航組織(ICAO)表格的地區

2. 2005/367/EC: Council Decision of 14 April 2005 authorising Member States to ratify, in the interests of the European Community, the Seafarers' Identity Documents Convention of the International Labour Organisation (Convention 185)

本決議主要係賦予各歐盟會員國，爲了歐盟整體的利益，批准國際勞工組織的航海員身分文件協定。

第 3 條(目錄與格式)

第 8 項部份主要規範那些符合本法附件 1(Annex I)所列清單的生物特徵樣本或其他樣品之持有者，也應該被包含在航海

員的身分證明文件上，並以同條項下之各款條件都被滿足爲前提，該各款條件包括：

(a)該生物特徵能夠在隱私權不被侵犯、或並未造成身體、健康上不適、或並未損及尊嚴的前提下被獲得。

(b)該生物特徵能夠在文件上直接以目視的方法知悉，而無法從該樣本或其他樣品中被重組。

(c)用來確認生物特徵的採樣器材必須是容易使用的，且必須能夠以低價讓政府獲得。

(d)用以確認生物特徵的器材必須在那些有權機關經常用來確認生物特徵的地方,像是港口或包括船板在內的其他地方，且必須能夠很方便且可靠的被操作。

(e)使用生物特徵的系統(包括器材、科技、及程序)必須被用來提供一致且可靠的結果，用以作爲身分確認。

而附件 1 的 III 係規定航海員必須提供：

(a)航海員全名

(b)性別

(c)出生日與出生地區

(d)國籍

(e)任何有助於辨識航海員身分的身體特徵

(f)簽名

(g)期滿日

(h)文件種類或名稱

(i)獨特文件號碼

(j)個人身分證號碼(非必要)

(k)指紋樣本

(l)一個機器可辨識、且符合在上述文件 9303 中所提到的國際民航組織(ICAO)表格的地區

（二）在涉及護照簽證與中央簽證資訊系統部分，主要規範部份在於護照簽證及其他文件上，爲了辨識與確認申請人的身分，所必須留存的生物辨識特徵。而在留存這些申請者的生物辨識特徵後，其儲存的方式、程序與使用的目的，必須被妥善的預先規劃。而在涉及中央簽證資訊系統的部份，主要係規範衛了發展中央簽證系統，各歐盟會員國所應具備的軟、硬體及制度上之要求。

1. Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States

第 1 條

第 1 項規定會員國所頒發的護照或其他旅行文件應遵守附件 1 所規定的最低安全標準。

第 2 項規定護照或其他旅行文件上，應包含臉部特徵等儲存媒介。會員國也應將指紋納入可共同操作的格式。這些資訊必須被妥善保存，而儲存媒介必須有足夠的空間與能力以確保資訊的完整性、真實性、以及可信性。

第 2 條

護照或其他旅行文件上，關於下述內容的額外科技清單必須依照第 5 條第 2 項所規定的程序被建立，清單內容包括：

(a) 額外的安全特徵與必要條件，包括加強防僞與竄改的標準。

(b) 生物特徵儲存媒介的技術性說明及其安全性，包括避免無權使用。

(c) 還有(爲了維持)品質的必要條件與臉部特徵及指紋的普遍標準。

第 4 條

第 3 項規定爲了本規則的立法目的，護照及旅行文件上的生物特徵只能被用來作爲確認身分使用。

第 6 條

本規則應於公佈於歐盟官方期刊後第 20 日起生效。

(a)關於臉部特徵的規定，會員國至遲應於 18 個月內施行；

(b)關於指紋的規定，會員國至遲應於 36 個月內施行。

2. 2004/512/EC: Council Decision of 8 June 2004 establishing the Visa Information System (VIS)

第 4 條

爲了發展中央簽證資訊系統(Central Visa Information System)、每個會員國的國境交界處，以及兩者之間的通訊基礎設施所必要之措施，凡涉及下列事項者，必須按照第 5 條第 3 項的程序才能被採用，這些事項包括

(a) 該系統物理結構的設計，包含通訊網路。

(b) 與個人資訊保護相關聯的技術層面。

(c) 與各會員國預算相關的財政事項或與各會員國本國系統相關的技術事項的技術層面。

(d) 關於安全必要條件方面的發展，包括生物特徵。

（三）在涉及申請臨時避難及 Eurodac 此一系統的建立時，首應說明者係這個科技資訊系統的概念，產生於 1997 年生效的都柏林協議，並在 2000 年 12 月 11 日，由 Council Regulation (EC) No 2725/2000 所通過，其目的係用以比較申請避難者及非法移民者的指紋，並希望能夠便利都柏林決議的適用情況，而能進一步決定審核申請避難者的責任歸屬問題。這個系統並在後來的 Council Regulation (EC) No 343/2003 中被加以修正、取代。

因此，下述規定多半是關於歐盟各會員國在面對申請避難者的情形時，所應採納的檢驗程序，及該程序中所應紀錄與留存的申請者生物辨識特徵，以及在記錄與留存生物辨識特徵後，應如何進行後續儲存與交流的工作，以便能更安全、更有效的達到比較申請避難者及非法移民者的指紋的目的。

1. 2006/188/EC: Council Decision of 21 February 2006 on the conclusion of the Agreement between the European Community and the Kingdom of Denmark extending to Denmark the provisions of Council Regulation (EC) No 343/2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national and Council Regulation (EC) No 2725/2000 concerning the establishment of Eurodac for the comparison of fingerprints for the effective application of the Dublin Convention

   第 1 條

   系爭使 Council Regulation (EC) No 43/2003 條款及 Council Regulation (EC) No 2725/2000 之效力亦得拘束丹麥的歐盟與丹麥間協議，自此爲了歐盟的利益而被通過。前者係涉及建立一套標準與程序，用以決定歐盟會員國如何審核由第三國公民所提出、請求暫住在任一會員國中的避難所的申請；而後者係涉及 Eurodac 此一系統的建立，該系統係爲了比較指紋，以便能更有效率的適用都柏林協議。

2. Council Directive 2005/85/EC of 1 December 2005 on minimum standards on procedures in Member States for granting and withdrawing refugee status

   第 23 條(檢驗程序)

第 4 項規定會員國亦得按照本指令第 2 章的基本原則與保證條款，規定一套優先或加速進行的審核程序，如果有下述情形發生的話：

(a) 申請者在繳交申請單及呈現事實時，在面對其是否符合 Directive 2004/83/EC 所規定的難民資格的審核時，只提出不相關或低度相關的事實。

(b) 明顯不具難民身分，或不符合會員國在 Directive 2004/83/EC 底下的難民資格。

(c) 避難所的申請是沒有事實根據的：

(i) 因爲申請者來自於第 29、30、31 條定義下的安全國家。

(ii)因爲申請者來自於非會員國以外的安全第三國。

(d) 申請者透過提供假資訊或文件，或藉由保留與其個人身分和國籍相關、可能對其申請產生不利影響的資訊或文件，來誤導行政機關。

(e) 申請者前已在另一份避難所的申請文件上填寫其他個人資訊。

(f) 申請者就其身分或國籍，並未提供足夠合理的資訊，或他/她可能不誠實地銷毀或棄置足以證明他/她身分或國籍的身分證或旅行文件

(g) 申請者表現出不一致、矛盾、不可能、或不足的陳述，使他/她在宣稱自己受到 Directive 2004/83/EC 中所提到的迫害的主張，明顯不具說服力。

(h) 申請者在關於他的個人環境或其來源國的情況沒有其他新的變化產生的情形下，另行繳交一份的申請書。

(i) 申請者在有可能，卻沒有正當理由的情形下，未能使他/她的申請早一點被受理。

(j) 申請者的申請只是爲了延遲或撤銷先前已通過或即將生效的遷移令。

(k) 申請者於不具正當理由的情形下，未能遵守 Directive 2004/83/EC 第 4 條第 1 項、第 2 項的義務或本指令第 11 條第 2 項(a)款和(b)款以及第 20 條第 1 項的義務。

(l) 申請者非法進入或延長他/她滯留在會員國的時間，以及在考量他的入境情形下，申請者沒有正當理由即未與權責機關聯繫，和/或盡速申請避難所。

(m) 申請者將對會員國的國家安全或公共秩序造成危害，或申請者業已因嚴重危及公共安全或公共秩序的理由被強迫驅離。

(n) 如果申請人拒絕按照相關歐盟及各國立法之規定，提供他或她的指紋的話。

(o) 申請者係第 6 條第 4 項 c 款所規範的未成年之未婚者所提出，而其父母的申請已經被駁回，且申請者的個人環境或其來源國的情況又沒有其他新的變化產生。

3. Protocol to the Agreement between the European Community and the Republic of Iceland and the Kingdom of Norway concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Iceland or Norway (Text with EEA relevance)

第 6 條

每一個簽約國都可以藉由對保管處提出書面聲明，以終止本議定書。這種聲明就會在其對保管處提出後六個月生效。

如果歐盟與丹麥間的協定被終止，則本議定書將停止生效。

本議定書也將停止生效，如果歐盟或冰島及挪威宣布廢止之。

(1) 2003 年 2 月 18 的(EC) No 343/2003，涉及建立一套標準與程序，用以決定歐盟會員國如何審核由第三國公民所提出、請求暫住在任一會員國中避難所的申請

(2) 2000 年 12 月 11 日的(EC) No 2725/2000，涉及 Eurodac 的建立，用以比較指紋，以便能更有效率的適用都柏林協議

4. Agreement between the European Community and the Kingdom of Denmark on the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in Denmark or any other Member State of the European Union and Eurodac for the comparison of fingerprints for the effective application of the Dublin Convention

第 1 條(目標)

第 1 項規定，本決議的目標在於適用 2003 年 2 月 18 的

(EC) No 343/2003 規則和 2000 年 12 月 11 日的(EC) No 2725/2000 規則，前者係涉及建立一套標準與程序，用以決定歐盟會員國如何審核由第三國公民所提出、請求暫住在丹麥或其他會員國的避難所的申請；而後者係涉及 Eurodac 此一系統的建立，該系統係爲了比較指紋，以便能更有效率的適用都柏林協議(Eurodac 規則)以及他們在歐盟和丹麥之間，按照第 2 條第 1 項及第 2 條第 2 項規定，所實行的措施。

5. Commission Regulation (EC) No 1560/2003 of 2 September 2003 laying down detailed rules for the application of Council Regulation (EC) No 343/2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national

第 1 條(掌管請求的準備措施)

第 2 項係規定，在比較過避難所申請者與按照(EC) No 2725/2000 第 8 條規定，於先前所採集、傳遞到 Central Unit，並經按該規則第 4 條第 6 項核對過的指紋資訊後，當 Eurodac Central Unit 基於比對後的正面結果，按照該規則第 4 條第 5 項提出請求後，該請求也應該包含 Central Unit 所提供的資訊。

第 2 條((收回請求的準備措施)

該請求也應包含那些被 Eurodac Central Unit 按照(EC)

No 2725/2000 規則，在比較過申請者與按該規則第 4 條第 1 項、第 2 項於先前所採集、傳遞到 Central Unit，並按該規則第 4 條第 6 項核對過的指紋資訊後的正面結果。

對於那些在 Eurodac 開始運作前所提出的請求，應備份該指紋乙份並附加於表格上。

6. Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national

第 21 條

第 2 項(c)款規定第 1 項所提到的資訊可能包含其他爲建立申請者的身分所必要的資訊，包含按照(EC) No 2725/2000 所處理過的指紋。

7. Council Regulation (EC) No 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No 2725/2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention

第 1 條(定義)

爲了本規則的立法目的，

(a) 所謂 Central Unit，係指在 Eurodac 規則第 1 條第 2 項款所稱的單位。

(b) 所謂資訊庫，係指 Eurodac 規則第 1 條第 2 項(b)款所稱的電腦化的中央資訊庫。

(c) 所謂「對照」係指審核在資訊庫裡被記錄的指紋資訊是否符合會員國所傳遞的指紋資訊的程序。

第 2 條(傳遞)

第 1 項規定指紋必須被數位化的處理，以及以附件 1 中所提及的資訊格式被傳遞。Central Unit 應建立會員國與 Central Unit 間互相傳遞資訊格式的必要技術條件，只要那對於 Central Unit 有效率的運作是必要的。Central Unit 必須確保會員國所傳遞的指紋資訊能夠被電腦化的指紋辨識系統所比較。

第 3 條(完成比較與傳遞結果)

第 1 項規定會員國應確保指紋資訊以一種適當的品質被傳遞，以爲了經由電腦化的指紋辨識系統來進行比較。Central Unit 應界定被傳遞指紋資訊的適當品質，只要那是爲了確保經由 Central Unit 所比較出來的結果可以達到非常高的準確率所必須。Central Unit 應儘可能審核被傳遞的指紋資訊的品質。如果指紋資訊無法透過電腦化指紋辨識系統來比較，Central Unit 應儘可能要求會員國傳遞適當品質的指紋資訊。

8. Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention

第 1 條(Eurodac 的目的)

第 2 項(b)款規定，爲了比較避難所申請者的指紋資訊，以及在第 8 條第 1 項及第 11 條第 1 項所提及之外國人分類，Eurodac 必須由一個電腦化的中央資訊資訊庫所組成，以處理在第 5 條第 1 項、第 8 條第 2 項及第 11 條第 2 項所提及的資訊。

第 3 項則規定，在不損及各會員國按其本國法所建立的資訊庫之資訊使用下，指紋資訊以及其他個人資訊僅得爲了在都柏林決議第 15 條第 1 項中所列舉的目的，在 Eurodac 中被處理。

第 2 條(定義)

第 1 項(e)款規定「hit」意指者經由 Central Unit 比較記錄在資訊庫的指紋資訊和那些透過會員國所傳遞、關於個人的指紋資訊所建立的比對紀錄，而未損及會員國依照第 4 條第 6 項應立刻審核比較結果的要求。

第 3 條(Central Unit)

第 1 項規定 Central Unit 應設立於委員會中，負責代表各會員國運作第 1 條第 2 項(b)款所提及之中央資訊資訊庫。

Central Unit 應配備有電腦化指紋辨識系統。

第 3 項(e)款規定 Central Unit 應每季就其工作起草統計資訊，其中(e)款表明 Central Unit 必須再度請求各會員國的指紋資訊數目，因爲被傳遞的原始指紋資訊並未同意使用電腦化指紋辨識系統。

第 4 條(指紋的搜集、傳遞、比較)

第 1 項規定每個會員國應立即將每個 14 歲以上的避難所申請者所有手指的指紋採集下來，並應立刻將第 5 條第 1 項(a)點到(f)點所提及的這些資訊傳送到 Central Unit。採集指紋的程序應按照各會員國的實踐情形以及歐洲議會在人權方面及聯合國會議在兒童權利方面所設下的保證措施。

第 3 項規定 Central Unit 應比較在第 5 條第 1 項(b)點所提及而被各會員國傳遞的指紋資訊，與被其他會員國所傳遞、且已經儲存在中央資訊資訊庫的指紋資訊。

第 4 項規定 Central Unit 應在各會員國的要求下，確保在第 3 項所提及的比較，除了其他會員國所傳遞的資訊以外，將覆蓋先前被該會員國所傳遞的指紋資訊。

第 5 條(資訊紀錄)

第 1 項規定只有下列各點的資訊嬰被記錄於中央資訊庫，包括

(a)避難所申請者的來源會員國、地區、與日期

(b)指紋資訊

(c)性別

(d)來源會員國的紀錄識別碼

(e)指紋採集日期。

第 6 條(資訊儲存)

每一組在第 5 條第 1 項所提及的資訊，從指紋被採集的那一天起，都應該在中央資訊庫被儲存十年。

第 8 條(指紋數據的搜集、傳遞)

第 1 項規定，按照歐洲議會在人權方面及聯合國會議在兒童權利方面所設下的保證措施，每個會員國應立刻採集每一個 14 歲以上、非法橫跨該會員國陸、海、空邊界，而被該國有權機關逮捕的，從第三國而來且未被遣返的外國人指紋。

第 2 項規定相關會員國應立即傳遞下列各點在第 1 項被提及、涉及任何未被遣返的外國人之資訊至 Central Unit，包括

(a)被逮捕者的來源會員國、地區及被逮捕日期

(b)指紋資訊(c) 性別

(d)來源會員國的紀錄識別碼

(e)指紋採集日期

(f)資訊被傳送到 Central Unit 的日期。

第 10 條(資訊儲存)

第 1 項規定每一組在第 8 條第 1 項所提及關於外國人的資訊，從指紋被採集的那一天起，都必須被儲存在中央資訊庫兩年。在期滿後，Central Unit 應自動將這些資訊從中央資訊庫中銷毀。

第 11 條(指紋資訊的比較)

第 1 項規定爲了審核非法出現在國境內、先前暫住其他會員國避難所的外國人，每個會員國得將任何可能關於該 14 歲以上之外國人已經被採集的指紋資訊，連同該會員國的紀錄識別碼傳遞到 Central Unit。

第 2 項規定當會員國參加第 1 項所提及的程序，他們應將第 1 項所提及的外國人所有、或起碼索引卡上的手指指紋傳遞到 Central Unit，以及如果這些資訊被遺失的話，所有其他手指指紋的影本。

第 3 項規定在第 1 項所提及的外國人指紋資訊，只有當其他會員國爲了比較避難所申請者的指紋資訊且已經儲存在中央資訊庫時，才應被傳遞到 Central Unit。這些外國人的指紋資訊不應被記錄在中央資訊庫，也不應依第 8 條第 2 項的規定，被拿來和傳遞到 Central Unit 的指紋資訊做比較。

第 4 項則規定，在比較按本條規定下被傳遞的指紋資訊，與被其他會員國所傳遞、業已儲存於 Central Unit 中有關避難所申請者的指紋資訊時，應適用第 4 條第 3 項、第 5 項以及第 6 項，以及其他按第 4 條第 7 項所設置的規定。

第 5 項(a) 款則規定一旦比較結果已經被傳遞到來源會員

國時，Central Unit 應立即銷毀指紋資訊以及其他在第 1 項規定下被傳遞的資訊。

第 13 條(資訊使用的責任)

第 1 項(a)、(b)、(e) 款分別規定來源會員國應負責確保指紋是被合法的採集、指紋資訊以及其他在第 5 條第 1 項、第 8 條第 2 項以及第 11 條第 2 項所提及的資訊是被合法的傳遞到 Central Unit、以及被傳遞到 Central Unit 的指紋資訊比較結果是被合法的使用。

第 18 條(資訊擁有者的權利)

第 1 項規定來源會員國應告知任何受本規則拘束的個人下列事項：

(a)控制者的身分，以及他的代理人，如果有的話。

(b)處理 Eurodac 內資訊的目的。

(c)資訊的收受單位

(d)在採集關於被第 4 條或第 8 條所拘束的個人指紋時，所應盡的義務。

(e)使用以及更正關於自身資訊的權利。

第一次項(subparagraph)所提及的資訊，應當在受第 4 條及第 8 條所拘束的個人的指紋被採集時被提供。在第一次項所提及關於受第 11 條所拘束的個人的資訊，至遲應當於關於該個人的資訊被傳遞到 Central Unit 時被提供。當此資訊的規定被證明不可能或將牽涉到不適當的結果時，這個

義務將不生效，

第 7 項規定任何基於第 2 項及第 3 項的請求，應包含所有關於辨識資訊對象所必要的細目，包含指紋。這些資訊必須被專門用來允許第 2 項及第 3 項所提及的權利行使，且應在之後立即被銷毀。

第 19 條(國家主管監督機關)

第 2 項規定各會員國應確保該國監督機關得從擁有足夠指紋資訊知識的專家獲取建議。

第 20 條(聯合監督機關)

第 5 項規定聯合監督機關應得從擁有足夠指紋資訊知識的專家獲取建議。

9. Decision No 1/98 of 30 June 1998 of the Committee set up by Article 18 of the Dublin Convention of 15 June 1990, concerning provisions for the implementation of the Convention

第 2 條(在決議第 15 條下的指紋交換)

第 1 項規定在不損及任何都柏林決議條款或其他議會決定的前提下，各會員國得於有理由追求關於第 15 條第 1 項所提及之目標時，從其他會員國那請求都柏林決議第 15 條第 2 項之指紋資訊。

第 2 項係指對於按第 1 項所提出之請求，指紋資訊規定應

受提出請求之會員國國內法及適用於歐盟的資訊保護原則之拘束。

三、近年實踐情況

在 2006 年 5 月 31 日，歐盟執委會對歐洲議會及歐洲理事會針對 Common Consular Instructions(CCI)所提出之修正案，提出一份建議，在其解釋備忘錄中，提到本提案的主要目的是爲了提供各會員國對申請簽證者強制採納其生物辨識特徵(包括臉部外貌及十根手指的指紋)的法律基礎，以及爲了履行簽證資訊系統(Visa Information System，以下簡稱 VIS)所設立的各國領事辦公室的組織基礎。爲了避免所有的會員國都必須在每個領事辦公室準備所有爲了蒐集生物特徵所必須的設備，設立聯合申請中心(Common application Centres，以下簡稱 CAC)的想法就產生了。CAC 有兩個優點，因爲資源能夠被集中且分享，所以得以強化各地區領事辦公室的合作，且使各會員國各有效率及節省成本的處理這些事務。在這個脈絡底下，各會員國爲了安排申請程序以降低使用生物特徵的花費，也將討論其他可能的選擇方案，例如代表制與外包制(outsourcing)。

VIS 是設計用來增進聯合簽證政策的履行，透過便利簽證發放程序、避免買賣簽證、便利邊境查核與加強打擊僞造，以及在各會員國境內協助辨識與遣返非法移民，便利 Regulation(EC) No 343/2003 的應用，以及協助預防對任一會員國的國內安全威脅。隨著採納生物辨特徵將成爲申請簽證程序的一部份，CCI 也必須爲上揭措施提供法律基礎而進行修正。

在影響評估的部份，由於 VIS 實施前已進行過影響評估，本次提案並未提出額外的影響評估。而在先前所提出的評估意見中，資源的匯集被認爲是一項正面的因素，即使領事辦公室可能難以處理這麼多的申請簽證案。CAC 的優點也在先前的影響評估案被提及，包括遏止簽證買賣、降低成本、更容易符合資訊保障的要求，以及有助於聯合簽證政策的履行。在關於外包制度時，一些會員國已經在尚未有共同法律框架的情形下，開始採用這種方法。由於在某些領事處申請簽證的數量逐年增加以及預算的限制，必須引入新方法以面對這種挑戰。外包制度並不被建議當作一種普遍的解決方案，而僅在特定領事處被使用。這種法律框架下的好處是，在 Directive 95/46 第 16 條及第 17 條的意義下，各會員國仍保有控制者的角色，而外部服務提供者則是加工者的角色。

爲了能完整的履行 VIS，盡速建立法律框架是必要的。在涉及 VIS 以及在會員國間交換短期停留簽證資訊的諸項規定構成法律框架的核心時，一份關於採納申請簽證者之生物辨識特徵的補充性法律文件是必要的。這份提案包含了 VIS 法律文件中所未提及的幾個領域。這份提案處理生物特徵的搜集，而 VIS 提案則涵蓋了資訊的傳遞與交換。將簽證申請者的受理與生物特徵資訊的搜集外包給外部服務提供者的可能性則落入這份提案框架中。鑒於整體政策是爲了便利簽證發放的程序，執委會恢復了每位簽證申請者僅需出面一次的原則：關於簽證申請僅需停留一次的系統：將簽證申請表格與生物特徵辨識之紀錄在同一地點與時間完成。然而，在個別案例中，爲了確認發放簽證的情形，特別是關於短期停留的合法目的，第二次會面訪談將無法避免。

因此爲了確保對簽證申請者身分確認與辨識，處理 VIS 系統(2004 年 6 月 8 日所通過的 2004/512/EC 的理事會決議中所建立)中的生物特徵資訊是必要的。除此之外，VIS 的履行也要求要有受理簽證申請者的新格式。而將生物辨識特徵整合入 VIS 系統，對於對簽證持有者與護照間建立更可靠的連結以避免錯認身分而言，是一個重要的步驟。

除了現存的代表制度框架，爲了便利簽證申請者的登記以及降低各會員國的行政成本，也必須預想新的組織可能性。首先，一種僅限於受理簽證申請者以及辦理紀錄生物辨識特徵特殊的代表型態，應被加入於 CCI 之中。其他的選擇，像是聯合辦公場所、聯合申請中心以及外包制度，也應該被引入。相對的，就符合上述各項選擇機制的法律框架，也應該考量特殊資訊保護的問題後被建立。在法律框架底下，各會員國應得自由選擇他們要在每個第三國家內，要使用何種類型的組織結構。

在會員國的中央權責機關決定將部分簽證處理過程外包給外部服務提供者時，制訂條文以規範這種情形是必要的。這種安排必須嚴格的遵守發放簽證的一般原則，並尊重歐洲議會與歐洲理事會爲保障個人資訊與傳遞這些資訊，在 1995 年 10 月 24 日所通過的 95/46/EC 指令。各會員國應與外部服務提供者訂立契約，契約中必須包含關於他們確切責任、中止或結束契約的條件與程序。

會員國也應該基於人道或其他原因，允許部分簽證申請者直接進入他們的領事辦公室。爲了便利任何後續的申請程序，按照 VIS 規則中所訂定的保留期限，在 48 個月內自第一次申請簽證時，影

印當時所留存的生物特徵資訊，應該被容許。一旦這段時間經過，生物特徵就應該重新被記錄。

執委會應自本規則生效後兩年，繳交一份報告，報告內容應包含生物辨識特徵紀錄的履行、第一次申請的原則、以及收理簽證申請申請的組織與程序。按照比例原則，爲所有履行申根條約(Schengen Convention)的諸會員國完成引入聯合標準與可相互使用的生物辨識特徵的基本目標，制定一套規則是必要與適當的。

根據歐盟條約後附錄的丹麥地位議定書(Protocol on the position of Denmark)，丹麥並不參加系爭規則的適用，也不受其所拘束。按照上揭協定第 5 條，丹麥應於系爭規則被採納後六個月內決定是否將系系爭規則納入其國內法的領域內。而對於冰島、挪威以及瑞典，本規則的適用情形也各有不同。

基於上揭原因，歐洲議會及歐洲理事會因此採納系爭規則，系爭規則的第一條內容如下：「

第一條

CCI 被修正如下：

(1) 在第 II 點，第 1.2 點被修正如下：

(a) 在(b)增加下列段落：

會員國僅能爲受理申請以及紀錄生物辨識特徵的情形下，代表一個或兩個以上的其他會員國。1.2(c)及(e)的相關條文也應適用。

代表受理與檔案資訊傳遞的領事處應遵守相關的資訊保護及安全規則。

(b)　(d)點被下述內容所取代：

當統一簽證被按照(a)和(b)點發放時，應該在附錄 18 中所規定的統一簽證發放表中被反映出來。

(2)　在第 III 點，第 1 點被下述內容所取代：

1.1 簽證申請格式—申請格式數量

外國人應填寫統一簽證表格。申請統一簽證的申請者必須使用與附錄 16 中的範本相符應的表格。

起碼將一份申請表格的影本歸檔，以便供中央權責機關商議之用。只要各國行政程序如此要求，簽約的各方均得請求數放申請書的影本。

1.2 生物辨識特徵

a)　各會員國應按照在歐洲人權公約(European Convention for the Human Rights and Fundamental Freedoms)以及聯合國兒童權利公約(United Nations Convention on the Rights of the Child)所設下的保衛措施，從簽證申請者身上蒐集生物辨識特徵，包含臉部影像與十指的指紋。

在呈遞他/她的第一次簽證申請時，每個申請者均應親自出現，以

便在那時搜集下列生物特徵：

- 一張在申請當時所掃描或拍攝的照片。
- 十指指紋，須平坦地以數位方式留存。

對於任何後續的申請，只要是在離上次入境後 48 個月之內，上揭生物辨識特徵均得使用第一次申請時所留存之資訊影本。在這段期限過後，任何後續的申請均應視爲第一次申請。

拍攝相片與按捺指紋的科技設備，應按照 ICAQ 文件 9303 第 1 部份(護照)第 6 版所訂定的國際標準。

生物辨識特徵應被合格的與經充分授權的領事處職員所記錄；或在他們的監督下，由第 1.B 點所提及的外部服務提供者所記錄。

資訊應當且僅能由按照 VIS 第 4 條第 1 項、第 5 條及第 6 條第五項、第六項之規定，所充分授權的領事處職員輸入 VIS 中。

b) 例外情形

下列申請者得免於按捺指紋的要求：

- 低於 6 歲的幼童。
- 生理上不可能按捺指紋的申請者。然而，如果僅有部分手指無法按捺，其餘手指指紋仍應按捺。

任一會員國得對外交護照、軍用/公務護照以及特殊護照的持有者，得免除其提供生物辨識特徵的義務。

在這些情形中，任何不適用本規則的入境情況都應該在 VIS 中被引入。

(3) 在第 VII 點，第 1 點被下述內容所取代：

1A 受理與處理簽證程序的組織

每個會員國應負責成立受理與處理簽證程序的組織。

各會員國應使其各地的領事處均具備合格的機器設備，以蒐集生物辨識特徵；或決定與一個或一個以上的其他會員國合作，無偏頗的選擇使用上述其他代理方法。任何合作方式應使用聯合處所、或建立聯合申請中心(CAC)、或與外部服務提供者的合作方式。

a)當聯合辦公處所的地點被決定時，各會員國領事處或大使館的職員，在其他會員國的領事館或大使館處理呈遞到他們面前的申請案(包括生物辨識特徵)，並共用該會員國的機器設備。聯合辦公處所的各會員國應就終止聯合辦公處所的期限與條件，以及行政成本由領事處或大使館所在地的會員國收取的部

份達成共識。

b) 當聯合申請中心被建立時，兩個或兩個以上的會員國的領事處及大使館將被集中於同一棟大樓，以便受理呈遞上來的簽證申請(包括生物辨識特徵)。申請者必須告知負責處理他們簽證申請的會員國。會員國應就終止這種合作方式的期限與條件，以及由各會員國分攤費用一事達成共識。會員國之一必須負責關於與地主國之間的物流與外交關係的契約。

c)按照第 1.B 與外部服務提供者的合作

1.B 與外部服務提供者的合作

當有與涉及當地情形的理由認爲領事處不適合配備紀錄或搜集生物辨識特徵、組織聯合辦公處或聯合申請中心時，會員國之一或數個會員國得與外部服務提供者合作受理簽證申請(包括生物辨識特徵)。在這種情形下，涉及的各會員國仍應遵從資訊保護法中關於處理簽證申請的規定。

1.B.1 與外部服務提供者的合作形式

與外部服務提供者的合作應採取下列幾種方式：

a)外部服務提供者作爲客戶服務中心，應提供有關申請簽證所必要之條件的一般資訊，並負責會面制度。

b) 外部服務提供者提供有關申請簽證所必要之條件，從申請者那收受申請、證明文件、與生物資訊，收受處理費用(就像在第 VII 部分、第 4 點及附錄 12 中所提及的)，並將已完成的檔案與資訊傳遞給有權處理申請程序的會員國所屬大使館或領事處。

1.B.2 會員國的義務

各會員國所選擇的外部服務提供者，應足以確保所有技術上與組織上的安全措施，以及各會員國所要求的技術上與組織上的適當措施，以保障個人資訊免於意外或非法的破壞，或意外遺失、變造、非經授權的揭露或使用，特別是在透過網路傳遞資訊或向領事處接受與傳遞檔案時，並對抗所有其他非法形式的處理。

當選擇外部服務提供商的時候，會員國大使館或領事處應詳細審核該公司的償付能力及可信性(包括必要的證照、商業登記、公司章程、銀行契約以及確保沒有利益衝突)。

無論基於任何理由，外部服務提供者均不得使用 VIS。使用 VIS 的權利必須僅保留給充分授權的大使館或領事處職員。

涉及的各會員國應按照 95/46 指令 的第 17 條之規定，與外部服務提供者簽訂契約。在簽訂契約前，涉及的會員國大使館或領事處應向其他會員國的大使館或領事處以及執委會代表說明，爲何簽訂這種契約是必要的。

除了 95/46 指令 第 17 條所規定的義務之外，契約尚應包含下列各款內容：

a) 定義服務提供者的確切責任。

b) 要求外部服務提供者按照權責會員國之規定行事，且僅能按照 95/46 指令的規定，基於處理簽證申請者的個人資訊之目的，代表權責會員國傳遞資訊。

c) 要求外部服務提供者提供簽證申請者 VIS 規定下所必要的資訊。

d) 提供領事處職員得隨時進入服務提供者營業處所的管道。

e) 要求服務提供者遵守機密規定(包含與簽證申請者相關的資訊保護)

f) 包含中止與結束條款。

涉及的各會員國應監督契約的履行，包括：

a) 外部服務提供者提供給簽證申請者的一般資訊。

b) 技術上與組織上的安全措施，以及技術上與組織上的適當措施，以保障個人資訊免於意外或非法的破壞，或意外遺失、變造、非經授權的揭露或使用，特別是在透過網路傳遞資訊時，並對抗所有其他非法形式的處理或向領事處接受與傳遞檔案。

c) 生物辨識特徵的保存。

d) 確保符合資訊保障條款的措施。

外部服務提供者處理簽證申請的總花費，不應超過附錄 12 所規定的費用。

會員國的領事處職員應訓練服務提供者，使其具備提供簽證申請者適當服務與充分資訊的知識。

1.B.5　資訊

各會國的大使館及領事處應對一般大眾公開，關於如何進行會面與呈遞簽證申請的確切資訊。

1.C　簽證申請者與各會員國大使館或領事處的溝通管道

和選擇的合作類型無關，會員國得自行決定是否繼續維持允許簽證申請者直接在大使館和領事處提出簽證申請的可能性。會員國也應確保在突然終止與其他會員國，或任何與外部服務提供者的合作時，能繼續受理與處理簽證申請。

1.D　決議與出版

各會員國就每個所屬領事處，將如何安排收受與處理簽證申請一事，應通知執委會。執委會將確保適當的公開。

會員國應將他們所簽訂的契約提供給執委會。

(4) 在第 III 點中，第 5.2 點修正如下：

a) 標題被取代如下：

5.2 各會員國的大使館及領事處與商業仲介者的合作

b) 下列內容被補充於標題與第 5.2(a)點之間：

爲了第 III 點中所提及的重複申請

1.2 各會員國應允許他們的大使館或領事處與商業仲介者合作。(換句話說，私人行政執行代理商、運輸或旅遊業者，包括遊覽業者及零售商)

第二條

執委會應在規定生效後兩年，向歐洲議會及歐洲理事會呈遞一份關於履行本

規定的報告。

第三條

本規定應於公佈在歐盟官方公報後翌日生效。」

針對上述修正案，首先要提及的是，歐洲資訊保護監察員(European Data Protection Supervisor，以下簡稱 EDPS)Peter HUSTINX，在 2006 年 10 月 27 日，就歐洲議會以及歐洲理事會針對涉及外交任務之護照簽證上之生物特徵，包括在簽證申請過程中所留下的生物特徵的組織與接受機構，所提的 Common Consular Instructions(CCI)修正提案(以下簡稱系爭提案)，提出一份建議，是近日內關於生物特徵資訊之應用在歐洲地區實踐情形的最新資訊。

該建議提到，CCI 的修正案有兩個主要的目標，這兩個目標都是爲了履行簽證資訊系統所建立，一是要提供歐洲特會員國要求簽證申請人提供生物辨識資訊的法律基礎，二是提供各會員國設立領事辦公室組織的法律框架，特別是在各會員國的簽證申請過程間提供可能的合作。然而這兩個目標都在資訊保護這個議題上，引發不同的問題。

CCI 是在 2000 年所發布，包含簽證申請的審核、審核決定的程序等相關事項。根據 2004 年 12 月 28 號的提議，各會員國基於辨識與確認身分的目的，應在 VIS 系統中引入指紋及相片等生物特徵。而目前歐洲議會及歐洲理事會針對修正 CCI 所提的建議就是爲了提供一個搜集生物辨識特徵的法律基礎。而 EDPS 早在 2005 年 3 月 23 日就發布一份意見書，強調生物特徵的敏感特質，將使得使用這種資訊前，必須謹慎評估它的風險以及必須遵循一允許

民主監控的程序。

EDPS 反對將規定特定個人或團體是否得以免除提供指紋的義務此事，規定在 CCI，而非 VIS 中。理由如下：首先，這些條款對很大一群人的隱私權將產生重大的影響，因此應該以較爲謹慎的立法程序來處理。特別是在關於按捺指紋的最低年齡與最高年齡的設定上，是一個政治問題而非單純的技術問題。其次，法律體系的透明化將使其更容易爲人所接納。

在免除按捺指紋義務這個議題上，採納幼童指紋的容許性必須基於 VIS 本身的立法目的來進行討論。換句話說，強迫或免除特定範圍的的人們按捺指紋，必須在簽証政策的框架中，是一個合乎比例原則的手段。這種比例性必須經由民主程序去評估。它也應該被以採納指紋的實際用途來評估，一般說來，生物特徵若非被用於證實身分，就是被用來分辨身分。傳遞低於 14 歲的幼童指紋通常僅被視爲用以證實身分。

總之，EDPS 強烈建議，基於一致性與透命性的考量，免除採納指紋義務這件事應該嚴格規範。搜集生物特徵的規定，特別是指紋，應被視爲附屬於主要的法律文書，而因此應在主要文件中提及。

而在申請簽證應採納指紋的最低年齡限制上，EDPS 廣泛的採納幼童指紋不能被視爲僅僅是一種技術性手段，而應該經過嚴肅的民主辯論。這種決定不能僅基於技術可行性，而也應該基於履行 VIS 所可以帶來的利益上。然而，因爲少數會員國的反對，這種

公共辯論似乎沒有舉行，這是很令人惋惜的。

EDPS 也提醒我們，制定 VIS 的目的是基於便利真誠的旅行者所必須的簽證申請過程，因此，便利性與合乎人體工學是不可或缺的。無論是在簽證過程或邊境控管上，使用生物特徵不應該使遵從簽證過程這件事，對幼童而言過度困難。

最後 EDPS 提到，生物特徵辨識系統有其技術上的局限。低於 14 歲的幼童指紋，在像 VIS 這種大規模的資訊庫中，應透過研究以証實其正確性與實用性。當然，上述提及的部份，不只牽涉到幼童，也及於老年人。指紋的準確性與實用性會隨著年齡增長而遞減，而便利性與合乎人體工學也是格外重要的。

照片部分也有一樣的問題，幼童時期的照片，是否在成年後仍然可以達到辨識的或確認身分的目的，都是令人質疑的。即使面部辨識的技術有顯著進步，軟體的進步也很難追上幼童面孔在其成長後所帶來的改變。因此，必須在 VIS 規則中說明的是，只要面部辨識技術仍未足夠可靠，照片僅能用於作爲分辨身分或證實身分的輔助因素。

EDPS 因此建議，對於上述兩中生物辨識特徵，應給予嚴肅的考慮以衡量打擊非法移民或幼童走私等利益，是否高於上述提及的弊病。

就生理上無法採納指紋的個人而言，有高達百分之五的人無法被

記錄指紋。EDPS 因此建議應有其他有效率的應變程序，這些程序應尊重那些無法成功的進行按捺程序的人的尊嚴，且避免將系統的缺陷轉嫁於這群人身上。因此，對於無法按捺指紋的人，自不應直接導致無法獲得簽證的結果。

爲了減輕各會員國的負擔(特別是指那些購買與維持機器設備的耗費)，系爭提案提出幾個合作機制，包括共用機器設備、聯合辦公場所、或透過外部服務提供者(external service provider)。就外部服務提供者而言，系爭提案強調只有可靠的外部服務提供者可供挑選，且這些服務提供者都必須盡一切努力保護資訊免於意外或非法的破壞、或意外移失、變造、非經授權的揭露或使用。對此，EDP 特別強調以下幾點：一、外部服務提供者的員工背景可能難以或不可能被審核；二、同樣的，對於破壞隱私的服務提供者或其員工的處罰未必是有效的；三、私人公司可能被政治動盪或改變所影響，而無法履行渠保護傳遞資訊過程安全無虞的義務。四、有效的監督可能是困難的。

因此，任何與外部服務提供者的的契約均應包含必要的安全措施以確保資訊保護無虞，包括外部審核、定期查對、報告，以及確保外部服務提供者破壞隱私時的責任機制，包含因該外部服務提供者洩漏隱私所遭受損害的個人補償義務。

事實上，儘管有上述契約條款之規範，外部服務提供者仍可能將屈服於第三國的本國法下。除此之外，這還可能涉及一項重大風險，也就是在某些第三國家裡，政府可能急切的希望知道他們的國民向何國申請簽證，特別是基於控制那些反對者或異議者的政

治企圖。私人公司的職員(多半是當地員工)將無從抗拒來自政府或執法機關的壓力。和將資訊存放於領事辦公室或外交單位比起來，這會是個主要的缺陷。因此，EDPS 強烈建議不要採取將資訊存放於外部服務提供者的作法。

綜上所述，EDPS 提出下列幾項建議：

一、 爲了確保透明化與一致性，免除按捺指紋義務應規定於 VIS 中，而非 CCI 中。

二、 提供指紋與相片的年齡限制應謹慎處理，並將倫理性、便利性、正確性與可行性一併納入考慮。

三、 相片不應被視爲獨立的辨識手段，而僅僅是一個輔助因素。

四、 將處理申請簽證一事外包給私人公司僅在該公司位於外交保護之處，且契約條款能提供有效的監督與責任。

除了上揭與涉及簽證申請的相關生物特徵規範外，歐盟執委會在 2006 年 2 月 21 日及 2006 年 9 月 22 日，也分別通過 2006/188/EC 及 2006/648/EC。2006/188/EC 係歐盟與丹麥間的協定，雙方將 2003 年 2 月 18 日所通過的(EC) NO 343/2003 的理事會規定及(EC) NO 2725/2000 理事會規定之效力擴張適用於丹麥。(EC) NO 343/2003 係涉及建立一套標準與程序，用以決定歐盟會員國如何審核由第三國公民所提出、請求暫住在任一會員國中的避難所的申請；而(EC) NO 2725/2000 係涉及 Eurodac 此一組織的建立，該組織係爲了比較指紋，以便能更有效率的適用都柏林協議。

在 2006/188/EC 中，歐洲理事會提到，在考量到歐盟條約部分規

定、歐盟執委會的建議以及歐洲議會的意見後，決定通過下列決議：「

第 1 條

系爭使 Council Regulation (EC) No 343/2003 條款及 Council Regulation (EC) No 2725/2000 之效力亦得拘束丹麥的歐盟與丹麥間協議，自此爲了歐盟的利益而被通過。前者係涉及建立一套標準與程序，用以決定歐盟會員國如何審核由第三國公民所提出、請求暫住在任一會員國中的避難所的申請；而後者係涉及 Eurodac 此一組織的建立，該組織係爲了比較指紋，以便能更有效率的適用都柏林協議。

第 2 條

關於協議(4)的第 10 條第(2)項中的相關準備事項，歐洲理事會主席應公告週知。

第 3 條

本決議應公告於歐盟公報。」

而在 2006/648/EC 係涉及在 2006 年 9 月 22 日所通過的執委會決議，該決議發布與發展簽證資訊系統(Visa Information System，以下簡稱 VIS)相關的生物特徵標準的科技清單。

歐盟執委會在考量歐盟條約部分規定及在 2004 年 6 月 8 日建立 VIS 的 2004/512/EC 理事會決議後，基於 2004/512/EC 理事會決議所建立的 VIS 是爲了在各會員國間交換簽證資訊，並授權歐盟執委會發展 VIS，包括中央簽證系統(Central Visa Information System)、在各會員國國內的 National Interface，以及兩者之間的通訊設備。而在發展 VIS 的最後階段中，納入與生物特徵相關的必要準備措施是適當的，且爲了使各會員國能夠使國內系統與中央簽證資訊系統相連結而事先進行相關準備措施，設定用於發展 VIS 的生物特徵清單也是必要的。

況且，生物辨識特徵的品質與可信性是最重要的。因此，有必要界定能夠符合品質與可信性的設備的科技標準，這對各會員國來說，將成爲嚴肅的經濟上與科技上指示。因此歐盟執委會通過了下列決議：「

第 1 條

與 VIS 發展相關的生物特徵標準的科技清單，被規定在本決議的附錄中。

第 2 條

本決議係向比利時、捷克、德國、愛沙尼亞共和國、希臘、西班牙、法國、義大利、賽普勒斯、拉托維亞、立陶宛、盧森堡、

匈牙利、馬爾他、荷蘭、奧地利、波蘭、葡萄牙、斯洛維尼亞、斯洛伐克、芬蘭以及瑞典提出。

」

參、結語

在過去一年內，歐盟在生物辨識特爭這個領域內所做的規定，主要是圍繞著資訊簽證系統(Visa Information System)打轉，如上所述，VIS 的出現，主要是爲了是設計用來增進聯合簽證政策的履行，透過便利簽證發放程序、避免買賣簽證、便利邊境查核與加強打擊僞造，以及在各會員國境內協助辨識與遣返非法移民，而爲了達到上揭目的，收集、留存相關生物辨識特徵便成爲最佳的手段，然而這個手段仍有許多值得檢討之處，從紀錄及留存生物辨識特徵的對象及其限制—包括最高與最低年齡、生理上無法採納者—，到簽證申請的過程、及在這過程中應遵守的程序，以及各會員國所得採取的執行方式，以及各種執行方式—包括聯合辦公處所、外部服務提供者等—所應注意之事項，均有所討論；我們也同時見到歐洲資訊保護監察員機於人權保障的立場，所提出的四項建議，包括爲了確保透明化與一致性，免除按捺指紋義務應規定於 VIS 中，而非 CCI 中；提供指紋與相片的年齡限制應謹慎處理，並將倫理性、便利性、正確性與可行性一併納入考慮；相片不應被視爲獨立的辨識手段，而僅僅是一個輔助因素；將處理申請簽證一事外包給私人公司僅在該公司位於外交保護之處，且契約條款能提供有效的監督與責任。由上揭情形，顯見在歐洲，運用生物辨識特徵的討論及實踐，正處於方興未艾的狀態。

第七章　日本制度沿革與實踐現狀

壹、前言：日趨嚴重的日本型監控社會

自從 2002 年日本政府開始全面施行「全國住民基本台帳網路」等基本政策後，每一個國民都被賦予一個號碼，並且將國民的姓名、地址、性別、出生年月日等基本資料登錄在電腦網路上，進行全國性的統一管理運用。到 2003 年 8 月，甚至只要有人申請，政府便提供內藏晶片的住民基本台帳卡。

這些事情意味著什麼呢？就是一億三千萬的日本國民所有的基本資料，將被電腦所聯繫，而形成巨大的 data base 資料庫。如果這些資料外洩或者是被非法使用的話，那麼這個被害的規模跟程度，可以說超乎國民的想像。此外，所謂的住民號碼，實際上會將各種各樣的個人資訊，透過不同的行政機關而結合在一起，使國民的生活完全失去隱私。我們可以預測：未來這個住民基本卡會被當成一種身分證，廣泛的被使用，甚至成爲國內版的護照，而且更有可能被賦予隨身攜帶的義務。

除此之外，在目前日本各大都市主要的幹道，有千百個地方設有能夠完全拍攝經過車輛所謂的「N 系統」[98]，無論是在鬧區、商店街、車站、超級市場、便利商店、學校等等，都裝上了這種監視錄影機，連與犯罪無關的一般國民也都會被拍攝進去。而全國的自治團體也相繼制定「生活安全條例」，甚至也有政府機關的幕僚提議導入「共謀罪」，對市民的監控越加強。一般國民的言論

[98] 桜井光政「N システム訴訟の現状」田島泰彦ら編著『住基ネット監視社会』、日本評論社、2003 年、216 頁以下。

自由或媒體的取材等等，也會被官僚機構介入，甚至取締，就好像在日本的個人情報保護法中所顯示的一樣。『週刊文春』雜誌兩度被法院命令禁止出版，使得表現自由受到很大的限制。甚至媒體對於派遣到伊拉克的自衛隊的取材或報導，也被政府統一規範，幾乎像是戰爭期間的整個資訊管控[99]。如果加上美國的 911 事件後，全球各國對於國民監控的強化與全面化，換言之即是對於各國國內中央集權的監控傾向，甚至全球化監控的合作，所造成的「反恐立法」等抑制國民自由的趨勢越來越嚴重。因此我們不能把監控片面的了解爲「爲了治安的必要之惡」，而要知道：所謂的監控社會，乃是同時具有人權保障與管理統馭的兩義性。

不過，日本國內的這種監控社會傾向，倒未必是從受到美國 911 事件的影響才開始。實際上，在 1995 年的東京地下鐵沙林事件，就已經形成國家決定全面監控的契機。甚至在當年一月所發生的阪神大地震，也有很大的影響。像這類的恐怖攻擊或是天災，給予日本政府的唯一教訓竟然只是「危機管理出現很大的漏洞」，因此反而強化了既存的監控社會型態[100]。雖然受到 911 影響，日本的監控社會也有全球化的傾向，但是在日本有更具體、更傳統性的問題，也就是所謂的「local globalization」這種地域性的全球化問題。比方說日本對於朝鮮半島出身的在日朝鮮人，從戰後就一直進行監控[101]，這就好像西班牙的巴斯克分離主義者、以色列的巴勒斯坦人、法國的阿爾及利亞人或者是香港的中國人等等。這些人都被國家或殖民地宗主國視爲潛在的恐怖主義者而加以監控。但是我們也不能不注意到，從這一系列監控社會的趨勢

[99] 梓澤和幸・真田範行「週刊文春差止め事件」田島泰彦ら編著『表現の自由とプライバシー――憲法・民法・訴訟実務の総合的研究』、日本評論社、2006 年、249 頁以下。

[100] デイヴィッド・ライアン『9・11 以後の監視――「監視社会」と「自由」』田島泰彦監修、清水知子訳、明石書店、2004 年、242－249 頁。

[101] デイヴィッド・ライアン前引書 242 頁。

也產生了許多的抵抗。許多的職業工會、個人甚至社區、NGO 等等都不斷的向嶄新的社會安全體制提出抗議甚至抵抗，同時也質疑這些新科技的有效性以及妥當性、合法性。

貳、日本監控社會的傳統

二十世紀伊始，日本的行政機關的規模就已經急速成長，同時也開始對於國民的生活展開綿密的調查。日文所謂的「世代調查」──也就是人口普查或者是家庭調查──只要每隔一兩年，警官就會拜訪一般家庭，調查居住者、人口結構以及鄰居是否有可疑人物等等。而調查所謂的「反政府活動」更是被等同調查犯罪，經常進行電話的竊聽。因此在 1960 年代，日本就已經透過所謂「創立情報社會」的概念，進行對國民的監控[102]。

「監控」一辭，或許可以如此定義：「以管理或統馭資訊操作爲目的，進行集中而且組織性的對個人資料的詳細調查」[103]。因此監控本身其實未必一定需要網際網路等電子媒介。只不過電腦軟體以及網際網路的使用，確實使得監視的範圍越來越擴張，監視的手段也越發的「便利」。原本近代西歐的市民社會，其內在邏輯就是爲了要進行資本主義的發展，因此本質上即可稱之爲一種資訊社會。然而這裡所謂的資訊，幾乎都是以個人資訊爲主，因此我們也可以說近代社會就是一種監控社會[104]。有趣的是，日本的資訊社會與其說是市民社會自行形成，還不如說是公家機關主

---

[102] 斉藤貴男「監視社会の動向と背景」前引『住基ネット監視社会』4－6 頁。
[103] デイヴィッド・ライアン『監視社会』河村一郎訳、青土社、2002 年、序章を見よ。
[104] 經常有人會把監控型社會和喬治．歐威爾的名著『1984』並論，但這個看法有盲點。歐威爾的未來社會一切均由統治者(行政機關)「老大哥」監控，而如今活生生的監控社會，卻是由行政機關與私人團體聯手，甚至國民之間也互相監視。我們姑且名之以「匿名監視者」──亦即：到處都是受害者，卻不知誰是加害人。

導。因此，對於一般國民而言，政府所稱「透過新科技以進行行政的合理化」，是不可輕信的政治諾言，有著太多的陷阱。其中最令人憂心的，當然是隱私權可能會受到侵犯。國民的隱私權與社會的治安孰輕孰重，正是資訊社會所蘊含的兩難。

舉例而言，日本的各部會與警察體系，利用整個監控系統而共同享有國民的個人資料。而處理個人資料的方法極爲多樣，因此往往會從一種監視聯結到另一種監視。舉例而言，一般的消費者監控或者資料庫的商業化等等，原本均是由民間的企業所進行，但是因此而得到的資料，總會讓行政機關或者警察「產生興趣」進而試圖分一杯羹。過去警察便曾利用保險公司調查保險的優先順位而進行的風險評估資料。相對的，基於官商互利，企業的行銷部門，也會使用警察製作的資料，避開高危險性的地區[105]。但過去無論是由政府進行對國民的監控，亦或公司行號在職場進行對職員的監控，一般而言都比對消費者所做的監控來的更加肆無忌憚。不過因爲網際網路的普及，以及行動電話在社會上造成的熱潮，使得電子交易急速成長，尤其是在日本使用行動電話所進行的電子交易蔚爲風潮，因此這同樣能擴張未來監控的領域[106]。

除此之外，日本與其他的歐美各國的社會監控的樣貌也未必全然相同。英文所謂的 privacy──隱私權，在日文中其實並沒有能夠相對應的語彙。因此在抵抗監控型社會的時候，往往會造成一些概念上的困擾[107]。此外，日本的「公共圈 public circle」，其實也不如歐美發達而且自給自足。一般而言，日本社會對於文官組織的信賴，其實竟然勝過媒體，所以這點來說是一個很奇妙的

[105] 船越一幸『情報とプライバシーの権利──サイバースペース時代の人格権』北樹出版社、2001 年、129－152 頁。

[106] 船越前引書 191-194 頁。

[107] 勉強可解釋爲隱私權法源的，是日本憲法第 13 條「個人尊嚴」。參照 1964 年 9 月 28 日下民集 15 卷 9 號 2317 頁東京地方法院判決。

特例[108]。

參、日本型監控社會素描

日本戰後的經濟發展以及立憲民主主義的成功，雖然在許多人的眼中是一個民主化的證據，但是日本國內仍然有許多人不一定完全認同。他們毋寧特別重視在政策擬定過程背後所潛在的政治性的腐敗，以及經濟性的，也就是財團或官僚的權力過份肥大。而且日本因爲從明治時代開始，爲了進行由上而下的nation-building，國家便透過教育體系創造出一個「單一民族的神話」[109]，對於日本國內的外國人，尤其是對於傳統的競爭對手如中國、韓國人都有相當的歧視，甚至對最近大量流入日本的阿拉伯人、拉丁美洲或其他國家的人也一樣。在這樣的傳統社會條件之上，出現更嶄新的監控技術，只不過會促成監控社會不斷的成長。現代的監控社會，監控的是所有國民的日常生活，因此政府便在法律或行政規範上訂定一個「視覺、聽覺的議定書」（audio visual protocol），或「視覺、聽覺的共通規則」，將視覺的、聽覺的乃至一切可以數位化的個人資料全部整合建檔運用[110]。

像這樣的嶄新監控，有兩個非常重要的特徵。第一是監控的自動化以及資訊整合。整個監控的自動化能夠確定人的身分，檢查個人資料並且 manipulate 動作、行動或者是遷徙移動。另一方面，所謂的整合是把各種各樣的資料庫進行橫向的聯結，記錄更

---

[108] 關於日本公共圈的討論，請參照拙文「『大正民主』與治警事件」（『輔仁法學』24 期）。

[109] 小熊英二『単一民族神話の起源——「日本人」の自画像の系譜』新曜社、1995 年を見よ。

[110] ジル・ドゥルーズ「追伸——管理社会について」『記号と事件』宮林寛訳、河出書房新社、1992 年、296 頁。

詳細的個人資料與動向，可以連結完全不同種類的資訊。其中犖犖大著者，就是用監視錄影機全面的追蹤市民的生活。1986 年日本警察就設立了所謂的 N 系統（N system）[111]，可以全面掌握道路交通狀況。根據公元２０００年的統計，在全國各主要交通地點，至少有 550 台的攝影器被設置，而且能夠自動的讀取汽機車的車牌號碼。爲了尋找贓車或嫌犯所乘的汽車，只要調閱監控攝影機設置地點的所有車輛的詳細資料，立刻就會自動的送到東京警視廳本部，然後與其所保管的資訊進行對比。除此之外，當然也包括超速攝影或是 ETC 等功能[112]。

這種超大規模的 N 系統究竟帶來了什麼好處呢？又有那些缺點？事實上至今並無定論。儘管如此，該系統卻已經被使用了這麼久，而且今後顯然會等比級數的擴大，不再只是爲了舉發違反交通規則或是竊盜，而將應用在更多樣的目的之上。比方說，N 系統所攝影拍到的影像因爲是數位化的影像，所以能夠去搜尋乘客人物的容顏，如果和汽車駕照上的照片互相比對之下，就等於是一個嶄新的手段可以去監控國民。的確，乍看之下本來是一個管理交通的手段，但是結果變成警察辦理其他案件時一個非常有效率的工具[113]。

此外，在鬧區以防止犯罪爲目的所設置的監控攝影機，在 2001 年之後也快速增加。比方說，在東京一些治安狀況比較差的地區，例如新宿歌舞伎町，光是在 2002 年 2 月就增加了 50 台的監視攝影機，因爲這附近的暴力犯罪大概是東京其他地區平均的一百八十五倍。民間企業或是商店街的人們也大量使用這種街頭攝影機，而警察往往會要求要得到這些攝影機所拍攝下來的數位攝影

[111] N 是車牌號碼。
[112] 參見日本警察廳網站 http://www.npa.go.jp/seisaku-hyoka/kekka-h13jisseki/2.4htm。
[113] 在 1995 年奧姆真理教事件發生的時候，日本警方便曾使用 N 系統追蹤嫌犯。

資料。事實上，日本警察非常獎勵民間設立這樣的攝影機[114]。

N 系統所使用的新科技既然是一種數位化的科技，因此它不單使得監控能夠自動化，而且也容易使它成爲一個 network 形成一種網絡。易言之，從這些街頭攝影機所得到的資料經過整合之後，很容易就能夠與其他資訊來源的資料庫互通有無，甚至組合在一起。而這樣的整合系統基礎結構，其實在 2002 年到 2003 年之間已經被確立，這就是前述的住民基本台帳的 network。透過給予每個國民十一個數字的「國民號碼」[115]，將所有日本國民的姓氏、住址、出生年月日、性別等等所有上線的資料全數網羅。依照日本政府的構想，此後日本的一億三千萬國民就可以利用這個簡稱「住基網」的網絡，和行政機關輕鬆愉快的打交道。無論申請簽證、護照，或者是申報所得稅，以及各式各樣的行政服務，都將既快速又方便。這就是日本政府最是心嚮往之的「電子政府」「網路虛擬政府」[116]。

網路虛擬政府，目前是由日本總務省所營運，和中央部會以及地方自治團體各個行政單位聯繫在一起。每一個國民「得到」一個識別登錄號碼，從此與電子政府你儂我儂，密不可分。

然而上述的國民登錄制度，其實在監控社會裡面是非常非常重要的一環。因爲透過這種制度，就提供了政府機會，可以很簡單的進入蓄積個人資料的超大型資料庫，甚至從各種各樣的資訊來源搜尋國民的個人資料，同時資料庫與資料庫彼此之間也可以互相整合或者是產生新的排列組合。比方說住民基本台帳卡，可以搭載個人生物特徵的資料，也可以加入所謂的銀行業務或其他

---

[114] 『警察白書』2002 年版，84 頁。

[115] 日文稱之爲「國民總背番號化」，亦即每個國民都好像棒球選手一樣，球衣的背後都有一個號碼以供辨識。

[116] 小倉利丸編『監視社会とプライバシー』インパクト出版会、2001 年、61－62 頁。

的金融服務。這就像馬來西亞或香港大量發行的智慧卡或 ID 卡的系統一樣，可以多目的的使用。表面上住民基本網路建構一個電子政府，使得行政機關原本繁瑣的行政手續得以更有效率，但是現在電子政府已經擴張使用到出入境的管理政策，也就是反恐的措施上面。這種個人資料範圍的不當擴張可能性，我們可以推想而知，有許多的個人、團體甚至自治體都不可能忍受國家肆無忌憚的入侵隱私權聖域。不過在論及國民的批判與抵抗之前，我們必須先對日本據以反恐的幾個法律修正案談起。

肆、「反恐」的迷思

在外交政策上一向隨著美國亦步亦趨的日本政府，近年來更以反制恐怖主義行動爲理由，對日本社會以及入境日本的外國人進行更嚴苛的監控。其中最重要的措施有三點：第一點是修改日本的「入出境管理以及難民認定法」，第二點是晶片護照的實施，第三就是準備在刑法中增設可處罰預備犯的「共謀罪」。除了第三點的共謀罪，雖然違背傳統的刑法理念，但因爲與生物科技及追蹤監視科技尚無直接關係，在此略而不論。以下僅就入出境管理法以及晶片護照略作說明。

一、出入國管理及難民認定法的修正

平成十八年（2006 年），日本國會通過修正入出國管理及難民認定法的一部分，並在該年五月二十四日公佈。本法主要有三個目的：第一，設置防範恐怖主義於未然的法制。第二，增添使入出境管理更加順暢的規定。第三，藉由「結構改革特別區域法」對全國實施特例措施的規定。而這三點之中，第一點與第二點尤其重要。

（一）首先，關於這些防止恐怖主義行動的修法，日本國會在法

案修正的說明文上指出：目前國際恐怖行動仍屬猖獗，爲保障國民的生命與安全，必須加強對恐怖主義防範之對策。因此，政府（國際組織犯罪、國際恐怖主義對策推進本部）在 2004 年 12 月便草擬了「防範恐怖主義於未然的行動計畫」。該行動計畫包含以下幾項內容：

1.法務省在對於外國人（特別永久居留權者例外）入境審查時，可以強制採取其指紋以及要求攝影。爲了得到法源基礎，法務省在 2006 年的國會中提出出入境管理法的修正案。

2.在同案中，法務省並加入（由各相關機關協議而認定的）恐怖主義者之入境，可以將之阻止或強制遣送出境等規定。此處所謂的外國人，除了具有特別永久居留權者或者未滿十六歲的青少年，以及其他與外交或者是國家招聘的特殊人員之外，都必須提供指紋等個人的生物識別資訊。如果外國人不願意負擔此一法定義務，提供指紋等的個人生物識別資訊，日本政府得將其強制驅逐出境。而海關所採取的指紋資訊以及其他的生物特徵都將 data base 化，亦可利用於外國人在日本居留時的管理與犯罪搜查[117]。

（二）入出國管理法的修正在日本國會之中，也因爲牽涉外國人之人權與隱私權，甚至個人資料自我決定權的保障等等問題而引發爭議。主要的爭議亦可分成以下幾點：

1.指紋等個人生物特徵資訊的提供範圍以及利用目的。

關於指紋等個人生物資料的提供是否屬於一種義務，有無違反憲法之虞等顧慮，已經在 2000 年日本政府廢除「外國人登錄法」

[117] 藤乘一道「テロの未然防止のための規定の整備」『立法と調査』254 号、2006 年、22－25 頁。

中強制按捺指紋的規定上，看到一點端倪[118]。同樣的疑慮也在國會中被提出。相對於此，日本法務大臣則回答道，如同最高法院的判決，國家機關若無正當理由強制按捺指紋的確是違反憲法第十三條；但另一方面，憲法第十三條也同時如此規定：爲了公共福祉，該權利也必須受到某種限制。爲了要公正的管理入出境以及保護國民的生命財產──簡單說就是爲了要防止恐怖主義行動──而要求外國人入境時必須有義務提供其指紋，乃是具有充足合理性與必要性的立法，同時也符合最高法院判例所言的「公共福祉」[119]。

2.誰應該提供這些生物特徵資訊？

以美國爲例，凡是具有永久居留權者即可免除按捺指紋之義務。但是在日本則只有具特別永久居留權者才得以免除該義務。法務大臣針對這點如此回答：

關於個人識別情報的提供義務，可以有兩種基準。一種是危險性程度較低者，第二種是需要做特殊考量之程度較高者，而政府就根據這兩種基準去處理決定什麼樣的外國人得以免除按捺指紋之義務。所謂特別永久居留權者，也就是在日朝鮮人，因為有其歷史背景，必須要對其法律地位特別加以保障，因此可以免除該當義務。相對的對於一般永久居留權者，他們並沒有這樣的歷史背景，所以不適用於所謂的入管特例法，從而亦無法免除提供個人生物資訊的義務。而且很遺憾的是，有許多的非法入境之外國人利用種種不法手段獲得永久居留權。目前擁有永久居留權而長期居住在日本者有三十萬人以上，如果這些人被恐怖主義或犯

[118] 當時日本全國律師公會（日辯連）就曾經指出，強制外國人在日本國內居留時按捺指紋，違反憲法第十三條以及違反公民與政治權利國際公約第七條。
[119] 第 164 回国会衆議院法務委員会会議録第 8 号 1 頁（2006・3・22）。

罪者利用或者竊取其護照等等，將會對於我國造成很大的困擾[120]。

3.使用的目的。

關於個人識別情報的使用目的，根據行政個人情報保護法的第三條第一項規定，行政機關在保有個人情報之際，其使用僅限於法律所規定之職務範圍內，並且使用目的必須加以特定。而在入管法修正案當中，法務大臣的理由便是在入境之際爲了確定其身分，的確有明確的使用目的，因此並未違反第三條第一項。同時在該法中也提到這些個人的識別資訊，在必要的情形之下也可以提供給外國政府[121]。

4.保管期限。

日本政府究竟打算保管這些個人生物特徵資訊到什麼時候，或者是什麼時候應該要刪除？國會中曾有意見認爲，應該在法案上明記個人生物資訊的保管期限。但法務副大臣則辯解道，如果在法案中明記保管期限，比方說五年，那麼恐怖主義或者是受到強制遣送出境之犯罪者，在五年後就有可能捲土重來，而這違反了入管法的修正目的，因此對外我們並不公開告知這些生物特徵資訊的保管期限。甚至他又說，指紋是辨識真假護照最重要的個人資訊，因爲指紋會伴隨人的一生而不改變，因此如果說有保管期限的話，就是該人的生存期限。假如從本法中的規定，十六歲以上的外國人入境必須採取指紋，那麼「我們希望能夠保管七、八十年」[122]。

5.恐怖份子如何認定。

---

[120] 第 164 回国会衆議院法務委員会会議録第 15 号 9 頁（2006・5・9）。
[121] 第 164 回国会衆議院法務委員会会議録第 15 号 7 頁、17 号 5 頁(2006･5･16)。
[122] 第 164 回国会衆議院法務委員会会議録第 15 号 2－3 頁（2006・5・9）、7 号 4 頁（2006・3・17）。

過去入出境管理法並無對恐怖主義做出任何的定義與規定。此次修正法第二十四條第三項之二也僅止抽象的規定:「除有相當理由被認爲有可能進行以脅迫公眾爲目的的犯罪行爲，或以脅迫公眾爲目的的犯罪行爲之預備行爲，以及有助於脅迫公眾爲目的之犯罪行爲實行之行爲」而已。但是這些抽象規定仍有可能被行政機關恣意濫用。法務省則回答，濫用是不可能的，因爲法務大臣在認定外國恐怖主義者的時候，會根據二十四條之二第一項的規定，必須「經由外務大臣、警察廳長官、公安調查廳長官以及海上保安廳長官」的意見，而這些行政機關均是極爲專業並具有調查權限之單位。

最後的疑慮則是這些個人資料是否可能外洩，法務大臣則信誓旦旦的保證，一定會徹底管理[123]。

二、晶片護照

根據日本外務省的網站上說明，從 2006 年 3 月 20 號開始接受申請新的護照，也就是所謂的 IC 護照、晶片護照。該護照上將植入晶片，除了持照人的國籍、姓名、出生年月日等事項之外，也在護照中嵌入晶片，晶片內儲存上述各類基本資料，還存有各項生物特徵資料，如臉部特徵，甚至未來還可能包括護照本人的指紋及虹膜等[124]。

日本的執政黨在 2005 年 4 月 13 日由法務省提出，修正「關於護照法以及組織性犯罪處罰以及犯罪收益的監視監控等法律修正草案」，並建議使用晶片護照。2005 年 6 月 3 日，參議院表決通過護照法的修正，並在同年 6 月 10 日公佈。因此，日本外務省

---

[123] 第 164 回国会衆議院法務委員会会議録第 15 号 12 頁（2006・5・9）。

[124] 到目前日本晶片護照的生物特徵資訊部分，只限於臉部特徵，也就是相片。關於日本晶片護照的官方說法，請參見日本外務省網站 http://www.gao/cgi_bin/getrpt?GAO-07-208T。

便向全國國民公佈引入新型晶片護照。不過目前爲止，並未強制人民立即更換護照，原來的護照在有效期間內仍可繼續使用，算是仍設定了一段緩衝期。

和出入國管理法的修正案一樣，護照法修正案的目的仍然是爲了要抑止犯罪，尤其是抑止恐怖主義。不過日本法務省並未提出任何具有說服力的說明，儘管政府一再強調這種生物特徵辨識技術（biomatrix）的應用足以阻擋犯罪，但針對政府蒐集個人資料所造成非常嚴重的隱私權侵害如何避免，則並未正面回覆。同時亦有日本國會議員直接提出法務省引進晶片護照基本上是受到美國壓力的看法，亦即認爲日本政府因外交的壓力而導致無視本國國民的隱私權，等於是政府本來應該進行對本國國民的權利保護義務有所怠忽，反而以美國的利害爲優先，甚至與入管法修正案相同，日本政府所累積的本國國民個人資料，日後也有可能流入美國政府之手[125]。

伍、民間對於反恐迷思的質疑

入管法以及護照法的修正案在國會審議的之前與之後，日本國內各界對於這兩個法案是否侵犯國民基本權，均提出很大的質疑。其中以日本全國律師公會（日辯連）以及國際特赦組織日本分部所提出的意見最爲具體。

一、日辯連「對於構築新體制，強化外國人的出入國、在留管理之意見書」

[125] 日本社民黨眾議員保坂展人的發言，請參見 http://www.jimbo.tv/videonews/000262.php。

（一）早在 2005 年，日辯連就對日本政府反恐以及監視外國人犯罪的諸多行動提出警告。同年 12 月 15 日所提出的意見書之中，日辯連舉出以下五點理由，希望政府必須謹慎評估，不可一意孤行。試略述如下：

1.日本政府對於所有的外國人賦予其義務，要求在入出境時提供指紋資訊以及顏面資訊等生物特徵資訊，並據此確實確認持照者是否爲本人，以及其是否過去曾遭受強制遣送出境者，甚至是通緝犯。像這種將個人生物特徵資料之提供予以義務化，不啻是限制隱私權以及自我資訊管理權。而且，這樣的作法究竟是否真能防止恐怖主義或者是犯罪？有無其他的替代方案？均應更審慎評估。再者，此制度牴觸憲法第十三條以及公民與政治權利國際公約第七條，因此不應該採用。此外，所謂例外對象也不應只限於特別永久居留權者，凡是已經經由入境審查取得居留資格的外國人，縱使暫時出境後再回到日本，也不需要提供個人的生物資訊。

2.政府將外國人入境時必須提供個人生物特徵資料制度化，而在外國人入境之後仍然保管其所取得的資料，並使用在外國人的居留管理以及犯罪搜查之上。換句話說，所有入境日本的外國人儘管沒有任何的嫌疑，仍然成爲犯罪搜查的對象，明顯違反無罪推定的刑法大原則。而其被數位化的生物資訊，也被日本政府其他部門所接收，列爲管理與監視的對象。如此一來，可謂是對外國人的基本人權進行積極的侵害。特別是行政機關所保有的個人資料，是否會提供給其他行政機關（甚至是民間企業），在目前經常僅由行政機關首長一念之間的判斷。何況若一味強化對外國人的管理與監視，反而會阻礙與外國人共生的日本社會的安定。因此，日辯連建議在入出境審查時，只要確認持照人並非恐怖主義者，或過去曾被強制遣送出國者，所有得到的資訊應當場立即刪去，更不可以在外國人入境之後持續保管上數的個人資料。

3.政府雖然在 2000 年時修法，已將外國人登錄制度中的強制按納指紋條款廢除，但如今卻想另外發給外國人晶片型在留卡，並預備將此「新身分證」之取得與攜帶義務化，甚至對於外國人的工作地點、學校等均課以報告義務，甚至打算將外國人的出入境資料、在留資料、警察廳與外務省所提供的各種資訊集中管理。凡此種種，均是明顯侵犯外國人的隱私權與自我資訊管理權，對於外國人而言是一種歧視性的待遇，也違反國際人權法的慣例。

4.政府強制旅館業者在外國旅客住宿之時必須確認其身分，但此一措施必須由法律明確規定，不應由行政機關片面決定。而且爲了保護外國人的隱私權與自我資訊管理權，護照的影印本不可強制旅館業者保管或者提供給警察。

5.政府在修正法案中僅以各相關行政單位的協議即得認定誰爲恐怖主義者，並拒絕其入境，或強制遣送出境。然而，以反恐之名所進行的這種任意解釋非常危險，不但違反國際難民公約等國際人權法，甚至也有可能否定了難民的民族的自決權。因此，對於恐怖主義者的定義必須更明確、更嚴格，且不得違反正當法律程序。

（二）以上五點意見中，值得更加深入探討的，是有關於個人生物特徵資料的保護，比方說在有關指紋資料的保護方面。指紋是隱私權的一部分，而隱私權不分本國人、外國人都應該受到同等的保障。最高法院於 1995 年 12 月 15 日的判決之中就曾經指出，憲法第十三條規定，國家權力的行使不得侵犯國民私生活上的自由，因此任何人均不可任意被強制按納指紋，國家機關若無正當理由強制按納指紋，即違反同條意旨。而上述自由的保障亦及於居留我國的外國人。此外，在日本的法律當中，基於公權力的發動，人們必須提供指紋的情形，只限於刑事訴訟法的二百二十八條，由法院發出身體檢查令狀或者是受到羈押的嫌犯。因此，如

果將提供指紋資訊予以義務化，便傷害了該人的尊嚴，也就是違反公民與政治權利國際公約第七條。

（三）事實上，有關個人容顏的資訊保護，最高法院早在 1969 年 12 月 24 號判決即指出，未得本人承諾不得對其容貌姿態加以攝影；即使是偵查機關進行的持續性自動性攝影、錄影，也必須要舉證證明使用該手段的必要性與緊急性以及比例原則等，方得受到承認（東京高等法院 1988 年 4 月 1 號判決）。總之，政府所設想的各種方案，根本是毫無根據的將外國人視爲犯罪的溫床。如果如此的偏見影響國民對外國人的觀感，並助長了對外國人的歧視，就違反了國際人權公約上人種歧視廢止公約的第一條第一項以及第二條「禁止人種歧視的行爲以及習慣」。根據 2004 年法務省入國管理局的統計，現在每一年大概有六百七十五萬的外國人進入日本，其中約有一百九十七萬人已進行外國人登入在日本居留。本制度如果得以實施，去除具有特別永久居留權者四十七萬人之外，已進行外國人登錄的一百五十萬人的生物資訊，被將完全被日本政府取得並保管，而以犯罪搜查爲目的進行使用。這不但會助長上述所說的，將外國人視爲潛在的犯罪者與進行恐怖行爲的歧視，甚至也會使外國人疏離日本社會之外[126]。

二、國際特赦組織日本分部的意見

在上述入管法以及護照法的修法過程中，日本政府最常提出的修法理由就是「反恐」。但是恐怖主義或恐怖份子如何認定，卻說得非常抽象。從國際政治與國際法的觀點而言，每一位被某國

[126] 以上日辯連「對於構築新體制，強化外國人的出入國、在留管理之意見書」，請參見日辯連網站 http://www.nichibenren.or.jp/ja/opinion/report/2005_69.html。

另外，關於 IC 晶片在留卡的取得與攜帶義務化，也值得深入討論。因爲登記在晶片在留卡上之資料，勢必與電腦網路相結合而加以使用。因此，非常有可能這些個人資料會在瞬間並且無限制的外洩。尤其是日本政府強迫居留在本國的外國人必須要隨時攜帶該卡片，因此上述個人資料外洩的可能性非常高。而強迫外國人隨時攜帶這種身分証，基本上也是一種明顯的歧視，與殖民地無異。

認定爲恐怖份子者，從另一方面而言，也大有可能是一個國際政治難民。舉例而言，從事新疆獨立運動的維吾爾人，或者是西藏獨立運動的西藏人，最有可能被中國認定爲恐怖主義者。而這樣子的人進入到日本的時候，究竟算是難民或者是恐怖份子呢？

有鑑於此，國際特赦組織日本分部便從國際法的觀點，對於入管法的修正案進行嚴密的批判。雖然這些批判並未直接討論到日本政府所使用的晶片護照或者是其他生物特徵取得之問題，但入管法修正案畢竟是日本政府蒐集本國人與外國人生物特徵的基本前提之一，因此有必要略加介紹。

國際特赦組織日本分部首先提醒道，日本是 1951 年國際難民公約以及 1967 年議定書的締約國之一，因此有關難民保護的國內法必須要符合該公約以及議定書的規定。此外，對該公約與議定書的適切解釋，均須考慮起草時各國的立法意旨、聯合國高等難民事務官事務所（UNHCR）執行委員會（EXCOM）的結論，以及日本所簽署的國際人權法規（A 公約、B 公約、禁止酷刑條約等）。

然而，此次的入管法修正，就牽涉了三點有違反國際人權法與國際法之虞。第一，是新創設的居留資格規定；第二是暫時居留許可的問題；第三個是強制遣送出境的程序。

首先，新法第六十一條第二項之二，設定一個歧視性的法案，也就是「居留資格受到承認者可以定居於日本，如果不受承認者就必須強制遣送出境」。但是審查標準所設定的四項要件中，卻有兩個要件是非常抽象且不合理的。第一是「入境後經過六個月才申請者」，就不符合要件。第二是，（雖然從有可能遭受迫害之虞的地域前來日本，但）「並非自母國直接入境日本者」也不符要件。

日本政府針對該兩個要件提出解釋，認爲是爲了要「避免難民認定制度的濫用」以及「證據的散失造成審查認定的困難」。可

是難民之所以成爲難民，其理由各不相同，現實上有許多的例子顯示，許多難民之所以經過六個月的期限而仍未申請庇護，往往是因爲愧於個人捨棄祖國的精神上困擾，或者是對於境管局的恐懼等等。何況難民所以成爲難民，並未必然已經遭受到迫害，而是未來有可能遭受到迫害。政府不能因爲其尚未受到迫害，便認爲其無證據證明其爲難民。另外，關於未直接從本國進入日本之難民被排除在外的規定，也非常不合理。根據 UNHCR 東京事務所的統計，過去十年之間被認定爲難民的七十七個人之中，直接從本國來到日本的只有九位，可見此要件與難民性的關係可以說風馬牛不相及（相同的，在難民認定申請之前暫時居留的許可，也發生同樣的要件問題）。而且日本政府千萬不要忘記，６０年前的世界人權宣言第十四條中早就規定，人民有向他國要求庇護的權利了[127]。

三、其他的批判

總之，對於入管法修法以及晶片護照制度，即使在法案已經通過的今日，仍然深受國民的懷疑與批判[128]，簡單整理如下：

（一）目前日本每年有超過七百萬的外國人入境，而日本政府卻打算對這些所有外國人採取指紋，根本是自討苦吃，貽笑國際。而且入管法修正後，日本就成爲世界第二個要求外國人留下指紋的國家，僅次於美國。

（二）耗費數十年的爭議與努力，日本國內好不容易廢止了在日朝鮮人指紋強制納印的規定，現在等於是一個人權大退步；而且

---

[127] アムネスティ・インターナショナル日本「国際法の観点から見た入管法改正案(政府案)」難民政策提言シリーズ NO.2，2003 年 5 月、http://www.amnesty.or.jp/ を見よ。

[128] 參照ネットワーク反監視プロジェクト(NaST)小倉利丸 2005/4/13 的意見，http://list.jca.apc.org/public/aml/2005-April/001177.html。

指紋資訊的保存期限、日後是否刪去、目的之外的利用是否應該有限制等等，這些最重要的部分完全沒有明確的規定，只是一味的追隨美國，一味的要去抵禦從未在日本發生過的國際恐怖主義。

（三）美國的指紋採取以及管理系統的設計者，與日本如今管理系統的設計者是同一家公司（ACCENTURE COMPANY）。這不但有圖利單一廠商的嫌疑，更重要的是，此後日本與美國的入國資訊是否會相互流用，以及是否會被一家私人公司掌握所有的入境兩國的外國人個人資訊呢？

（四）晶片護照簡單而言，就是凡是所有出國的日本人的生物資訊之一的容顏也被國家所管理。另一方面，我們的指紋資訊雖然目前仍然是「只要不犯罪就不需要受到政府管理」，但這項權利何時淪陷，恐怕也只是時間問題。因爲當日本人進入美國境內時，必須要被強制按納指紋，而這些資料從美國還流到日本政府的可能性是非常大的，尤其兩國的管理系統是交由同一家公司進行的。

總而言之，這些入管法護照法的修正以及共謀罪的新設，甚至是與單一公司締約，最終均指向日本型監控社會的完成。甚至從此以後日本人或日本國的基礎資料，也有可能被美國人所完全掌控。而日本政府真的有必要對美國政府的反恐政策亦步亦趨嗎？現在巴西等國已對美國這項強力措施產生極大的反彈，而採取報復性行動——凡是入境巴西的外國人，「只有」美國人會被強迫按納指紋，可見世界上有許多國家對美國的作法相當反感，日本人難道也要步上美國的後塵嗎？

最後，對於恐怖份子的定義過於曖昧，也是一大隱憂。根據法律規定，只要有「相當的理由」認定某人有可能是恐怖主義者，便可對其進行強制遣送出境。基於過去累積至今的經驗，只要對於日本政府的政策或方針看法不同的人，就有被認定爲恐怖主義者的可能，極可能並不是過於誇張的看法。

陸、市民社會的全面抵抗

爲求取行政上的方便及效率所進行的國民登錄制度、入管法修法、晶片護照，或者是新的 ID card 的創設發展等等，當然會引起許多國民／外國籍住民不安與反對的聲浪。其實在過去，日本也發生過相同的事情。60 年代到 70 年代之間，當日本政府開始將國民個人記錄全部交由行政機關內部的電腦處理時，就曾引起不少抗議。而如今則有許多律師、媒體工作者、學者、工會、市民團體或個人，竭盡全力抵禦政府入侵私領域的做法。其中 NGO 團體的力量最爲強大[129]。1999 年，日本的「通信傍受法（其實就是監聽法）」草案曾引起大規模的論爭。這個法律的草案，基本上是要國會承認檢調單位對於毒品、槍械犯罪、幫派殺人或者是大規模的不法移民等等犯罪組織有權進行電話或傳真的監控、監聽，甚至也旁及於電子郵件的監視。而值此社會譁然之際，日本全國律師公會、新聞媒體人以及工會、NGO 團體等群起抗爭，提出超過二十萬人的反對連署。最後法案雖然仍在國會中通過，不過因爲受到如此沉重的壓力，而被迫修改多處[130]。

在 2002 年到 2003 年間，則有兩次更大規模的，抗議政府監控政策的抗爭。第一次發生在 2002 年。導火線是該年 5 月日本防衛廳居然無視「政府情報公開法」中明白賦予人民向政府請求資訊公開的權利，暗中收集資訊請求人的個人資料，而且還做了一份請求人清單。原本資訊自由（freedom of information）必然是民主國家資訊政治的基本方針，從「政府有說明義務」的觀點來說，幾乎所有的民主主義國家都非常重視資訊自由。但是防衛廳這種「監控系統的整合」行爲，卻完全違反資訊政治的基本方針。他

[129] 例如上述「network 反監視 project（簡稱叫 NaST）」就是非常具有代表性的運動組織。
[130] 小倉利丸前引書 28 頁以下。

們千方百計想要了解的是,「誰」對於特定的內閣部會或者是行政機構有特別的「關心」,甚至幻想著透過這樣的資料蒐集,讓防衛廳能夠掌握是哪些個人或團體會對各個不同的行政機構進行「挑釁或脅迫」。

一般而言,各個行政機構最關心、最想知道的資訊就是有媒體人、反戰團體、NGO 的成員或市民團體的個人資料。日本防衛廳雖然也承認這些清單有可能被誤用濫用,但是實際上他們仍然當成家常便飯一樣的進行個人資料的搜集,等到在被媒體揭露之後,防衛廳才趕緊把廳內所揭載的請求情報者的名單消除。其實防衛廳的各部門,根本就是組織性的蒐集這些資訊公開請求者的資料,而且在上面記載請求人的職業、所屬團體、與自衛隊的關係甚至其思想信念等等。這個醜聞爆發之後,中谷元防衛廳長官不得不出面向全國國民謝罪。

防衛廳醜聞,讓國民開始對政府機關「有沒有能力慎重保護國民的個人資料」產生極大的懷疑。但是到第二年,也就是 2003 年防衛廳又被爆料,發現他們這十數年來都在偷偷蒐集十八歲左右、有資格可招募至進入自衛隊的,所有男性女性的個人資料。防衛廳透過 550 個以上的自治團體,接受這些團體所提供的居民資料,而本來應該有責任保護個人資料的地方行政機關,不但怠忽職守,甚至還違法主動提供居民的個人資料給防衛廳[131]。

其實,規模最大的抗議,發生在 2002 年住民基本網絡的國民登錄制度以及所謂的 ID card 系統開始運作之時。這種以「提供公共服務的網路電子合理化爲目的」的電子政府,所引起的抵抗之強烈,完全出乎日本政客意料之外。根據朝日新聞的輿論調查

[131] 日弁連編『プライバシーがなくなる日』明石書店、2003 年、第 2 章 1－2、1－3 を見よ。

[132]，國民之中有百分之七十六要求住民基本網絡的營運應該要延期，而且主張在營運之前，必須要立法創設隱私保護的法律加以配套。從最近防衛廳的惡例或其他侵害個人隱私的事例來看，日本人絕對不相信政府已經有能力或者有意願保護國民的隱私。

在以東京杉並區爲例，杉並區區長山田宏做了一個問卷調查，發現百分之七十以上的居民根本就反對住基網絡[133]。當時的一個口號就是「我不想變成一組號碼」，因爲居民們認爲新的居民登錄制度，乃是威脅人民自由的恐怖象徵。而反對住民基本台帳網絡的理由如下：第一點，就是根本欠缺一個國民隱私的保護法律。第二點，從過去的案例可知，連公務員都不可信任了，遑論一般民間企業，更有可能流用或洩漏國民的基本資料。第三個理由是，這些基本資料很可能被使用在所規定的目的之外。當時政府辯解說這是杞憂，因爲當時原本規定住民票的號碼只能用在三類的行政服務上。然而短短幾年不到，現在已經擴大到二百六十四種行政事務了。可見日本政府在蒐集人民個人資料上的綿密程度和對人民個人隱私的漠視，較之東亞諸國未遑多讓．

安東尼•紀登斯曾指出，監控是現代型統治的必然產物[134]。因此像前述的竊聽、資料的比對查證、國民登錄制度、ID 卡、晶片護照等等政府的行爲，必然會引起反對運動的發生。雖然塞繆爾•杭亭頓認爲亞洲社會不太可能轉變成西歐式的市民社會，但是實際上這些日本社會的抵抗行動，已經證明了杭亭頓的說法是大有問題的。從 1995 年的阪神大地震以來，無論是政府危機管理的失敗，或是對個人基本資料貪婪的搜集，均已使日本人不再能容忍國家政策的暴走，而且也不再壓抑自己對於社會正義的要求。因

[132] 朝日新聞 2002 年 7 月 21 日的問卷調查結果。
[133] 杉並区「住基ネットに関するアンケート中間集計結果」(2002 年 7 月 31 日)、http://www2.city.suginami.tokyo.jp/library/file/enq_half_jnet.pdf。
[134] アンソニー・ギデンス『国民国家と暴力』松尾精文ら訳、而立書房、1999 年。

此日本人不斷的形成各式各樣的 NGO 團體，參加這些組織以表明自己的要求，使得國家或政黨政客在侵犯國民人權時，都必須付出慘痛代價。

柒、結語

與國家理性主導一切的近代社會一樣，現今的日本也是一種監控社會。有人擔心歐威爾預言的「一九八四老大哥」社會即將夢魘成真。相對的，幾乎所有的監控社會，也都試圖把官僚制度的合理化以及其業務的效率化相結合在一起，就像前述日本政府所想要推動的電子政府一樣，可以簡化繁雜的手續，以提高效率。因此如何在行政效率與隱私權之間保持合於憲法精神的平衡，便顯得特別重要。不幸的是，規範這些電子政府的 guideline（指針、行動方針）或法律的限制既不明確也不完備。因此在這種情形之下，一味追求所謂的電子政府，事實上是一種不負責任而且違反民主精神的行動。這正是日本人對於各級政府或防衛廳等內各各部會的非法蒐集資料，甚至住民基本台帳網絡感到危疑恐懼的原因。

監控社會的統治，會不斷的追求監控系統的自動化以及整合。而這種監控的強化無論多麼的有效率，無論具有如何的目的正當性，仍然會引起統治者其他的邪惡欲望。一言以蔽之，監控必然成爲取得政權者最難抗拒的誘惑。同時，國民則因政府對資訊的操作、統治、管理，而被監控、被追蹤、被識別。不止如此，既然監控及於所有的日常生活，因此必須要透過所謂視覺、聽覺的，甚至是數位的把國民做鉅細靡遺的分類，分爲各種不同的極端，然後交由不同的機構來管控。問題是這種所謂的 social sorting（社會性分類）的監控新系統的設計，在過程中幾乎沒有經過法

律的、倫理的或者是開放性的討論，整個過程是完全不透明的，傳統官僚政治的黑箱作業惡習才是主流。

日本政府（警察）現在所進行的管控，實際上在 911 之前很早就已經計畫開發了。另一方面，爲了要跟美國合作以及反恐，如今又更加速「填補」監控的「漏洞」。結果，只有在技術上不斷的更新加強，使監控成爲一種預防型的監控，甚至純粹爲了監控而監控．而且這種國家性的監控同時也會影響民間公司行號，甚至學校的上行下效，使得過去純粹的、行政的、警察的監控慢慢地走進誘惑型的監控，也就是說對消費者資料的監控。還好對於這樣子的監控社會進行抵抗的文化，在日本已經有百年的歷史，而且也在日益壯大之中，值得我們繼續觀察、學習。

第八章 生物辨識身分制度所引發的社會風險及辯論

壹、生物辨識的效益取向

生物辨識技術是運用人體的生物特徵和行爲特徵，進行身分辨認的技術，可分爲行爲特徵與生物特徵兩種。行爲特徵是透過聲音、筆跡等方法來進行身分辨識，會隨著時間或心情而有所改變，如唇部動作模式、敲打鍵盤的方式、步態辨識:走路時身體各部位之間角度的變化等；生物特徵則採用臉部、指紋、虹膜、掌型、DNA、靜脈模式、耳型辨識(外耳特徵的幾何型態) 體溫辨識等方式來進行身分辨識，不會隨著時間或心情有大改變。它具有以下優點:

一.迅速與便利

使用方便，不用擔心遺失或損壞、密碼遺忘的問題，可用於簡化入境的手續。使用生物檢查可使旅客從報關到櫃檯、通關、登基等多個關卡的檢查，簡化到只要幾分鐘即完成，避免排隊久候查驗之不便，但若要達到全面性的安全網絡，則必須靠各國籍國際犯罪防範組織將資料互通有無[135]。

二.具有廣大市場與商機

適用性廣泛，可依安全性需求做適當的調整，且生物認證技術擁有廣大的市場，其應用領域主要有：

---

[135] 郭錦萍，生物檢查通關 航協將試用，聯合報，2001/10/15.

1. 門禁系統:運用於需要高度安全防護地方的門禁管理，如政府機密部門、銀行及金融中心、化驗室、私人住宅、航空站、運動場等場所等。可作爲工作出席狀況之紀錄。

2.身分鑑定:如自動提款機作業、電子商務。可於金融機構、自動提款機等財務處理的提款卡或信用卡上嵌一小片內存有生物特徵資料的晶片，以補強原本的安全防護措施。並可協尋失蹤老人或小孩。

3.電腦使用開機(Login)、行動電話、PDA 等個人資訊用品使用的身分確認

4.自動安全監控(工廠、社區、大樓)、

5.打擊犯罪，執法單位用於鎖定嫌疑犯、逮捕犯人

6.海關通關檢查，出入境身分的確認[136]。

7 其它還包括人性化機器人之製作、醫學上用途等，但相對地缺點是技術層次高、須較多的軟硬體支援、費用較傳統安全系統高。

三.防僞造與辨識率高

生物測定技術辨識率據稱可達百分之九十七到九十八，若應用於護照製作上可降低護照僞造問題。這種晶片新護照乍看之下外觀似乎與傳統護照區別不大，差異點在於它的防僞功能，故贊成電子護照的人認爲，電子護照很難被僞造或變造，因爲晶片上的所有個人資料都能和護照紙本部分比對[137]。美國希望使用生物辨識技術乃爲國家安全考量，它可有助於防止可能構成危險的恐怖分子入境。新式護照不只能提高護照的完整性和安全性，還有助於

[136] 參閱:〈「生物認證」技術〉，工研院資訊與通訊研究所，2004 年 5 月.
[137] 郭無患，美國開始核發電子護照 有人擔心資料被竊，Yahoo!奇摩新聞，2006/08/05

偵測僞造或竄改資料等罪行，生物測定技術運用每個人的特徵，使用這些資訊對照持有人和護照的資料，無疑能提高安全性[138]。晶片護照亦有抑制護照冒名申請、冒領之功效，透過機器自動、大量且快速的比對處理，輔助人工查驗經驗及設備不足問題。

但因爲科學本身的不確定性特性所致，生物辨識技術並不如宣稱中安全，它可能產生許多相對的風險面，包括有:違反基本人權的風險、資料外洩改造和散佈風險、人類與非人類因素造成的風險、引發新的犯罪機會、增加犯罪機會風險、全球化與文化背景的社會風險、個人和家族污名化及社會歧視風險等。

貳、遲滯型的風險意識

就風險的語源學說，風險原本就是指發生在未來的危險與令人恐懼的情況。按照這個定義，建立生物特徵資料庫或建立全民指紋資料庫，在現在或許看不出對個人有什麼具體的危害，但是我們可以設想一些情況，它們現在只出現在想像中，可是未來也許真的會發生，這些情況包括：除了指紋，我們還要交出其他的個人生物特徵供國家使用與管理，例如眼睛虹膜或 DNA。我們一旦交出這些個人生物特徵，對這些私密資訊就不再具有管控權，那麼後果會是什麼[139]？

從在地的社會風險角度，台灣社會回應基因食品、換發身分證按捺指紋、biobank 到生物特徵辨識制度等生物科技的特殊脈絡來看，都蘊含著政府風險管理的怠惰，造成台灣高科技社會蘊生了遲滯型態的社會風險與危機。換言之，長期以來技術官僚獨大

[138] 廖玉玲，生物測定護照 向冒牌貨說拜拜，經濟日報，2006/03/08

[139] 周桂田、張淳美，生物特徵、指紋資料庫風險，科學發展 398 期，2006 年 2 月

的科技與風險決策，雖然面對國際相關風險管制規範的發展，但無論在管制政策（風險評估）或風險溝通上仍然遲滯與隱匿，相關本土社會生物辨識制度資訊的嚴重缺乏，使得台灣的風險社會脈絡從全球化風險運動中缺席。

生物特徵辨識制度的設立不僅是法律基本權利（如基本人權、隱私權）的問題，還涉及資訊保存、複製及保密的科學不確定性所衍生的各種重大社會風險。換句話說，依照數位科技所發展的生物資料系統所構成的不再是科技不確定性的風險本身，更直接關連到國家監控、隱私權侵犯、資料暴露後之個人與家族社會歧視等巨大風險，而這一部分就是後常態科學的領域中科技發展對社會衝擊的不確定性，已經外溢到非科技的領域，而構成對社會多元的挑戰[140]。

今年 2007 年初中國時報報導[141]，爲因應大陸觀光客「大舉入侵」，移民署已購買二十二套生物特徵辨識系統分散於桃園機場、高雄小港機場、金門與馬祖服務站，預計於七月一日上線啓用，全面防堵大陸人滲透國境；移民署署長吳振吉表示使用生物特徵辨識系統是國際上防患未然趨勢，將率先對中國旅客和中國配偶實施臉型辨識[142]；移民署副署長吳學燕進一步指出何以專挑大陸客通關查驗，是因爲大陸人民僞造、變造身分入境的情況，比其他外國人來得嚴重，因此率先對大陸人士實施臉型辨識，未來將逐步擴及入境來台的外國人[143]；而其實外交部領事局早已緊鑼密鼓規畫「晶片護照」[144](國外稱之爲「生物護照」或「電子護

[140] 周桂田，2006，〈遲滯型高科技風險社會下之典範鬥爭:以換發身分證按捺指紋案爲分析〉,《政治與社會哲學評論》，第十七期，頁 135

[141] 大陸客來台，通關辨臉伺候，中國時報，2007 年 1 月 1 日

[142] 藍營：生物特徵辨識把中國新娘當恐怖分子，中央通訊社，2007 年 1 月 3 日，http://tw.news.yahoo.com/article/url/d/a/070103/5/8wy7.html

[143] 移民署:陸客僞造身分入境較嚴重，中國時報，2007 年 1 月 2 日。

[144] 參閱:晶片護照年底發行，中國時報，2007 年 1 月 15 日。

照」)，以因應國際民航組織聲稱 2010 年前發行機器可判讀型護照的趨勢，外交部並編列生物護照業務費及軟硬體設備接近十億元，將把本國人的臉部生物特徵及基本資料，植入護照封底一小塊晶片內，預計今年底完成生產設備、開始小量發行，晶片內除了儲存護照上各項基本資料，如護照本人電子檔、臉部影像，未來還可能包括護照本人的各項生物特徵資料，如指紋及虹膜等。

這種使用生物特徵辨識系統快速地通過航空站、過境關卡，給人一種未來派的感覺，但故事更大的部分是在於景象背後，關於真實身分背後的秘密應該是一個健全的科技設施，畢竟，作粗工的生物特徵辨識科技是所謂翻譯、運送和捕捉形象的過程，它藉由比對先前捕捉的形象和儲存資料在巨大的資料庫中，來確認一個人是否就是他所宣稱的身分。

從不確定性科學的角度來看，生物特徵資料庫的保存、複製、認定應用、保密等問題，涉及相當龐雜的、以資訊科技爲基礎的資訊資料蒐集與管理程序，涉及的問題已脫離了生物特徵資料庫的單一學科問題，而進入系統性的、異質的科技風險與由其衍生的巨大社會風險。由於資訊科技對於相關資訊資料的保存、複製、認定應用、保密等的確定性，在當代資訊連結技術與複製技術的高度發展中已面臨了挑戰，因而產生了科技風險。一方面在龐雜資訊系統的技術運作使用上，可能面對精確性的不確定性，比方說指紋辨識完成後的推理過程，要是資訊連結出了錯，就會產生誤認的風險。另一方面，這些資訊資料可以隨時被複製儲存，密碼破解，連結、認定改造、散布，資訊系統整體運作的安全性因而受到破壞。整體來說，資訊科技系統運作將不再容易確定其安全性[145]。

而資訊系統運作的安全不確定性，不僅侷限在科技層面上，

[145] 周桂田、張淳美，生物特徵、指紋資料庫風險，科學發展 398 期，2006 年 2 月

同時會直接外溢，造成整個社會的安全不確定性問題。首先，一旦在龐雜資訊技術運作認定的精確性上，產生模糊狀態或錯誤，將可能隨機地引發社會巨大的爭議。尤其針對高度敏感性的政治或社會爭議標的，科學精確性往往反過頭來受到挑戰，而形成兩極的反應。 其次，資訊系統的連結安全，由於加密與破解密碼技術日新月異，有可能導致資訊資料被侵入改造、複製儲存與不當散布，發展成具有高度爭議的社會事件。諸如個人、家族或族群生物特徵資料的暴露，造成相關的權利侵害與歧視問題，演變成世代、家族或族群的歷史事件。上述這兩個科技系統風險與社會系統風險，正是 J.R. Ravetz 所強調的後常態科學高度不確定性狀態。整個科技系統的安全不確定，造成的問題不只是停留在科技系統本身，還會外溢到社會系統，而產生不可估計的或未意圖的後果[146]。

生物辨識身分制度涉及個人與集體人類安全、個人行蹤、生物特徵資訊曝露等問題，風險包括法律上違反程序正義的風險、政治上形成警察國家、國家至上的風險、社會上階級汙名化、倫理的風險，以及資訊管理上被冒用、被洩露的風險等社會後果[147]。

事實上，這些社會後果也會進一步解構科學系統安全性的問題。假設在商業高度激烈競爭或全球科技研發激烈競爭中，研究人員或管理人員在相關利益的考慮權衡下，在某個模糊的倫理或管理規定或範疇上進行傾斜式的運作（例如故意遺留資料空間、侵入管道），將回過頭侵害到科學系統安全性問題，而進一步循環性地衝擊到社會面向的爭議與風險。也就是說，人類生物特徵資料系統的控制、相關技術，不斷地研發、破解與再研發，可能使

[146] 周桂田、張淳美，生物特徵、指紋資料庫風險，科學發展 398 期，2006 年 2 月
[147] 周桂田，2006，〈遲滯型高科技風險社會下之典範鬥爭:以換發身分證按捺指紋案爲分析〉，《政治與社會哲學評論》，第十七期，頁 131。

整體社會系統逐步滑向國家監控、商業監控、犯罪、侵犯人權、社會歧視等的循環，而造成不可回復、不可估量、不可控制的歷史後果。當然，我們可以看到在這個滑坡效應下，任何形式的法律與社會制度或程序正義的保障設計，將敵不過逐步朝向系統性、複雜性演化的趨勢，最後造成監控社會（每個人民都受到監控的社會）。歐威爾在《一九八四》一書所描述的老大哥監控世界，或許會是人類不久的未來[148]。

即使民眾一般認爲隱私的期待與社會目標應相互妥協，然而以立法來控制生物測定科技的使用和保護隱私權並不是萬靈丹，它並不足處理其他議題，如科技、資訊分享規則，可能與生物測定科技使用一同發生，而這往往不被民眾了解[149]。

民眾常「無知」的「忽視」生物辨識身分制度將構成風險的潛在嚴重性與不可欲的後果，原因包括:1.民眾不了解生物資料系統遭竄改、傳布造成的犯罪、詐騙，對隱私空間的威脅、社會歧視等一發不可收拾的風險。2.科技系統風險的複雜性，使得社會公眾存在著知識與資訊判斷上的困難性，而導致風險感知選擇上的貧困 3.以及長期技術官僚政策片面擷取科技系統的利益論述，以便宜行事的取得民眾的支持[150]。

探討生物辨識身分制度所引發的社會風險還必須研究風險感知與風險溝通面。普遍的社會氛圍、社會議題扮演了型塑風險承擔人風險感知的角色[151]。大眾在評定風險和科技的不確定性上，

---

[148] 周桂田、張淳美，生物特徵、指紋資料庫風險，科學發展 398 期，2006 年 2 月

[149] Kristen Batch, Lynette I. Millett, Joseph N.Pato, Editors，〈Summary of a Workshop on the Technology, Policy, and Cultural Dimensions of Biometric systems〉，p21-22，2005

[150]周桂田，2006，〈遲滯型高科技風險社會下之典範鬥爭:以換發身分證按捺指紋案爲分析〉，《政治與社會哲學評論》，第十七期，頁 167-169。

[151] 參考 Robin Mansell and Brian S. Collins，〈Risk management in cyberspace〉，p351－356, 2005

風險感知的變化，依賴是否有質詢進信任和值得信任的議題，而這又牽涉到個人對個人、對人對系統或系統對系統的信任[152]，而信任和可信度是被那些過去被傳遞訊息的人所給予的，故大眾會以過往管制機構的風險管理作爲信任的參考來源。

此外，風險溝通的組成不只是個團體的資訊交換，亦鑲嵌於更寬廣的制度和文化的背景中。風險溝通中，被信任的來源是重要的，至於詳述或稀薄乃依在地的脈絡氛圍而定[153]。就生物辨識身分制度所引發的社會風險綜合如下，包括違反基本人權的風險:隱私權、國家監控、人權問題、資料外洩改造和散佈風險、人類與非人類因素造成的風險、引發新的犯罪機會、增加犯罪機會風險、全球化與文化背景的社會風險、個人和家族污名化及社會歧視風險。

參、社會風險的種類

一、違反基本人權的風險:隱私權、國家監控、人權問題

從科技讓人無所遁形的隱私權侵犯面來說，若人們將一天到晚的所有活動詳細記錄，會發現自己在偵監科技產品與管道下無所遁形，比方通過幾座電子收費站、刷了幾次信用卡、何時登入或退出即時通、Skype、收發多少封 E-MAIL、於 Google 和 Yahoo 上搜尋了何種內容、走在路上與進入商店購物時，當天被明或暗的攝影機捕捉到的次數、手機與何人的通聯紀錄、幫忙標示地標

有關 NIMETBANK 的研究。

[152] 參考 Robin Mansell and Brian S. Collins，〈introduction〉，《Trust and crime in information societies》，p.6－7, 2005

[153] 參考 Robin Mansell and Brian S. Collins，〈Risk management in cyberspace〉，p351－356, 2005

有關 NIMETBANK 的研究。

與資訊的車上「全球定位系統」，而這樣的無所遁形將在生物辨識技術大量運用後，我們的個人資料會在所有使用生物辨識系統的公共場所中反覆出現、反覆地被知悉，而且只要是使用生物辨識系統的公共場所也都將留存出入民眾的紀錄，透過這些紀錄，我們的行蹤可輕易地被有意得知的人知悉，也會得到國家對人民更全面和徹底的監控，儘管自己的一切都禁著起檢驗，但儲存資料的辨識系統與資料庫卻可能出錯，更可能被濫用。

管制單位認爲要有好的治安、強壯的國家安全體制就必須加強身分概念的執行和服務功能，所以官方認爲生物特徵辨識有利於法律執行，但只單是以「全民拚治安」這一點說法還是不夠的，利益面仍是不清楚的，在管制單位的宣稱與人民的預期仍有不同，尤其是這類資料會牽涉到個人隱私權和國家安全，資料的管理就成了一個難關，如何防止資料外洩或盜取遭詐騙集團利用，防止駭客破壞生物特徵電腦資料庫、不法份子竊取資料去從事壞事、或遭臥底、恐怖份子侵入進而得到國家機密，危害國家安全是現今非常重要的課題。

維護治安利益在大多數公眾感知下認爲大於侵犯隱私權的風險，這種風險的抉擇，相當程度是公眾認爲現行制度保障人民身家安全的不足，寧願犧牲部分個人隱私爲代價的風險個人化選擇，而這樣民眾風險感知不足的遲滯型風險的文化結構，或說是反身現代與簡單現代的典範轉移困境，將不利於一個身處全球化科技競爭、知識與科技複雜風險快速變遷的社會，因爲愈是隱匿、遲滯愈是缺乏反省批判的風險，愈容易被篤信科技安全的確定性、加強犯罪預防的簡單化約、工具性的現代化論述所操弄[154]，而形成國家機器社會，忽視科技系統可能產生的不可控制性、不

[154] 周桂田，2006，〈遲滯型高科技風險社會下之典範鬥爭:以換發身分證按捺指紋案爲分析〉，《政治與社會哲學評論》，第十七期，頁 165.176

可彌補性、不可回復性效應。

再者參考 2005.3.15 及 16 日在華盛頓舉辦的專題研討，此研討會的內容乃探討生物檢測系統(Biometrics)的科技、政策和文化層面，其中與人權相關的議題還包括以下可供思考[155]

1. 這類收集資料的方式可能是先例，而類似這樣的政策可能也被使用在電腦、網路和 E－mail 上嗎?
2. 因爲個人可能不會知曉這樣的生物測定資料的收集，尤其是遙感的裝置，那是不是應該或可以被通知呢?
3. 當生物測定資料可能與其他資料庫連結，而這被涉及的利害關係又如何，以及被收集的資料應該可以被保存多久?
4. 個人有被給予機會檢查他們的生物測定資料是否正確嗎?這又該如何做?
5. 誰有資格收集資料，而資料的整合、保護和告知的責任歸屬又是哪些?

除了以上思考點外，生物特徵辨識系統較傳統確認系統安全，這同時也意味連結過程的完整(integrity)必須要高，而這仰賴四個階段的安全操作，這四個階段分別是登錄、儲存、獲得、配對[156]，此四步驟必須確保過程中無任何人類或非人類因素造成的差錯，而這樣的生物特徵辨識科技的安全性絕對比管制單位所宣稱的可靠還來的低，比方指纹辨識完後的推測過程，要是資訊連結出了錯，就會產生誤認的風險，此外，這些個人資訊資料可以

[155] Kristen Batch, Lynette I. Millett, Joseph N.Pato, Editors,〈Summary of a Workshop on the Technology, Policy, and Cultural Dimensions of Biometric systems〉, p9-10, 2005

[156] Roberto TAVANO、Pr. Juliet Lodge、Ronald Huijgens、Kamini Aisola、Marc Flammang,《Biometrics in Europe》, European Biometrics Portal Trend Report 2006,June 2006 2.2.3

隨時被複製儲存、連結、散佈、改造，所以它並不能絕對百分之百地保證安全，正如同其它的辨識技術一樣，資訊系統整體運作的安全性可能遭破壞，縱使生物特徵辨識系統頗有用處，大部分的產品卻仍有尚待突破的阻礙。

二、資料外洩和散佈風險

自進入電腦資訊時代後，資訊、金融、消費、教育、娛樂的網路化提供了人們日常生活更便利的方式，但也面臨了更多駭客入侵及個人外洩的資訊風險，資訊風險並未必全由資訊科技所引起，不使用任何資訊科技也同樣地存在著資訊風險，重點在於國家愈依賴資訊科技時，資訊風險就隨之增加。回想當處在使用紙張紀錄時代，業務上的資訊，如消費者的個人資料等都存在著遺失、遭竊取、竄改等風險；更別說使用網路普及化後，每天電腦一開機連結上網，都有防毒軟體、防毒軟體防不甚防的病毒與駭客攻擊，及層出不窮的資料外洩、犯罪、詐騙等行爲了。

以我國而言，在個人資料保護上一直有很大的漏洞，消基會於 2003 年 12 月 24 號指出，民眾竟可透過入口網站，進入中央健保局網站，查到個人病史、身分證號碼、親屬姓名、電話、住址等及醫生個人資料、實驗室檢驗報告等機密資料[157]；此外根據消機會在 2004 年 6 月 2 日指出，逾 2000 萬個人資料外洩，資料外洩的單位包括政府機關、電信事業、及金融事業單位等[158]。又誠如李德財所述:「2004 年的蕭榮祥案牽涉到警察、海巡人員、還有電信業者集體盜賣客戶資料。接踵而來的 2005 年假退稅和假綁票等詐財案層出不窮，這些詐財案都肇因於個人資料外洩，讓歹徒

[157] 參考廖瑞宜，中國時報 2003 年 12 月 25 日；李宗衡/陳伯因，蘋果日報 12 月 25 日。
[158] 參閱消基會，2004 年 6 月 2 日，消費新聞。

有機可乘。可以說，由於保護個人資料的觀念和作法不足，業者在個人資料管理上有漏洞，社會付出了相當慘痛的代價。資訊安全科學的研究早就已經指出，人員的管理問題，是資訊系統的安全罩門。所謂防護周詳的資訊系統，也難以因應人員的管理問題，更何況資訊管理鬆散的單位呢？ 2004 年資訊安全科學最大的消息，是一套幾乎所有系統都賴以保護使用者密碼的一套機制，被幾位中國浙江大學的教授所破解。這項消息令全世界的資訊安全人員，人人自危。[159]」。

諷刺的是，當晶片護照發佈的同一天(2007/01/15)，新聞就報導了發生了刷卡消費資料外洩的事件[160]；同一月份也有多起資料外洩的新聞發生，比方 1 月 5 號有報導指出聯邦銀行也發布聲明表示，聯邦銀行的企業網站網址，被不法集團設置類似的網站，企圖以『網路釣魚』手段誘導民眾進入[161]；1 月 10 號亦有新聞報導備司令部在寄發後備軍人召集動員令的時候，讓數十萬後備軍人的個人資料曝光，給予詐騙集團可趁之機[162]；1 月 22 日也傳出購物台離職員工進入東森購物，趁機抄下 22 筆信用卡卡號犯案[163]故難保生物辨識系統資料庫的管理或者資料庫電腦與電腦連結過程，不會產生個人資訊外洩的情事。

---

159 參閱李德財 2005 年 5 月 25 日於 tw.bbs.soc.taiwaneseg 對指紋案的意見，http://groups.google.com.tw/group/tw.bbs.soc.taiwanese/browse_thread/thread/eaa9bfa4bcf43f82/541b22e9217d5dea?lnk=st&q=%E6%9D%8E%E5%BE%B7%E8%B2%A1&rnum=9&hl=zh-TW#541b22e9217d5dea

160 參閱:「刷卡」資料全都露 消基會點名新光三越應立即改善，東森新聞報，2007/01/15，消基會針對百貨公司、超級市場、量販店等 15 家連鎖商家進行刷卡存根聯是否揭露「卡號」調查，結果發現新光三越各家分店中的刷卡存根聯上的卡號一覽無遺，對消費者來說是潛在的危險，應該要立即改善。

161 參閱:網路釣魚猖獗 聯邦官網也被偽冒，卡優新聞網，2007/01/05.所謂網路釣魚，是駭客把網友當魚兒釣，再上網的民眾不注意下竊取其個人敏感資料，如信用卡資料、銀行密碼、遊戲帳號以達到榨取金錢的目的.

162 參閱:避免個人資料外洩，寄發動員令將更換信封，中廣新聞網，2007/01/10.

163 參閱:電視購物藏陷阱!信用卡易遭到刷，TVBS 新聞，2007/01/22。

移民署這回除了向廠商承購指紋、臉型、虹膜三合一電腦的硬體和軟體設備外，另有資訊工業策進會從旁協助進行 RFID 通關研究的工作，移民署指出，建置生物辨識電腦系統的目標是透過自動化臉部生物特徵辨識技術，執行入出境查驗工作，在大陸人士及外籍移住民入境時，採用臉部特徵辨識，而原本依法需按印指紋者，如團聚、居留、定居及遣返者，則維持按指紋做法，雙管齊下可有效查察利用改名、假冒身分、偷渡、非法打工、逾期停留及政治滲透等不法情事。

而縱使目前移民署生物辨識資料庫屬境內管理目的使用，不須與國內外相關單位進行情資交換，但生物特徵辨識乃爲世界各國兼顧安全、便利趨勢，其電子護照需與全球相關單位進行情資交換亦是可預測的趨勢，故將來爲使臉型影像檔案可與島內外相關單位進行情資交換，移民署會將此案數據庫檔案，採取以國際通用的檔案格式建檔儲存，並進行轉檔交換，與移民署現行的境管系統整合[164]。

而以美國的例子來說，CAIS 是在波士頓警察署的生物測定資訊分享系統，用來察覺非法居住在美國的外國人和偷渡客，舉例當一個人被逮捕後，就會被留下十指指紋、臉部照相和身上明顯的特徵(如纹身)儲存在 CAIS 內，同樣的資料會進入 FBI 的 IAFIS 和麻薩諸塞州警察署的自動指紋身分系統(AFIS)，必要的話，也與 ICE(Immigration and Coustoms Enforcement)分享，如果被逮捕者非出生在美國，資料將被送到波士頓的 ICE，它將開始調查，若有嚴重的罪行，會通知國際刑事警察組織[165]。生物辨識資料的

---

[164] 參照:大陸客赴臺通關辨臉伺候 島內媒體、學者痛批，中國台灣網，2007/01/01，
http://big5.chinataiwan.org/web/webportal/W2001019/Uyyping/A410251.html

[165] 參閱 Kristen Batch, Lynette I. Millett, Joseph N.Pato, Editors，〈Summary of a Workshop on the Technology, Policy, and Cultural Dimensions of Biometric systems〉，National Research Council，The National Academies Press，2005

趨勢是與其他資料庫連結共同打擊犯罪，而這被涉及的利害關係又如何?光是 FBI 的 IAFIS，它就包含超了過 4 億 8 千萬筆指紋組，由於這些生物辨識系統都涉及了龐大的資訊儲存、辨識、利用、流通與管理，在任何一個環節皆有高度的不確定性，並且一旦外洩所引發的風險後果更是難以估計，且具不可回復性的結果。

再瞧瞧電子護照面，縱使已經是先進國家大勢所趨，然而其安全性卻令許多專業人士憂心忡忡。美國電腦安全大師級人物施奈爾直言:「一本護照有效期限十年，以爲它的安全性可以確保這麼長一段時間，根本是愚不可及。」英國專家史特君指出，問題關鍵在於電子護照使用的無線射頻辨識（ＲＦＩＤ）技術有其先天的弱點，加上規格又是由國際民航組織（ＩＣＡＯ）統一訂定，更讓駭客或有心人士有機可乘。例如英國政府依循國際民航組織規定，將電子護照的密鑰設爲護照編號－持有人生日－護照有效日期，因此只要這串數字不慎外洩，加上一具讀卡機和一部筆記型電腦，晶片中的資料就岌岌可危。雖然英國內政部表示，電子護照只能在兩公分距離內讀取，而且其中資料就算被盜取也無法竄改，對盜取者並無用處。然而專家指出，隨著電子技術進步，無線射頻辨識晶片的讀取距離也越來越大、防不勝防；有心人士盜取資料之後，可以在原始持有人毫不知情的狀況下，複製一本電子護照，供罪犯甚至恐怖分子使用[166]。

因此，在當前國家和許多企業看好生物特徵辨識系統之際，實有必要審慎評估此項技術系統將帶來的社會風險衝擊面。

三、辨識錯誤及科學不確定性風險

雖然很顯然地每個人的生物特徵都是獨一無二的，但是擁有

[166] 參閱:破解術德專家只花兩周兩百美元，中國時報，2007/01/15

這些特徵與能夠正確辨識出這些特徵卻是兩回事，科學不確定性會造成的判讀錯誤、精準度不足，所以生物統計技術學和系統的科學與技術挑戰是需要減少錯誤與變異性。

目前生物特徵身分識別系統的辨識能力，一般以 FAR 及 FRR 兩個數值來表示，FAR 是 False Acceptance Rate 的縮寫，指的是錯誤接受率，也就是讓不該進入的人進入的錯誤機率；FRR 是 False Rejection Rate，指的是錯誤拒絕率，也就是拒絕正確使用者進入的發生機率[167]，以指紋辨識爲例，FAR 是時十分之一，而 FRR 是萬分之一。

此外生物辨識身分系統有一變異性的範圍，包括身體的變異性(年齡、外傷)和生理的變異性(情緒、新陳代謝的改變)，而這些變異性都是生物測定科技所面臨的挑戰[168]。如指紋來說，可能因使用者暫時性或長久性的傷痕，致使辨識錯誤；或者虹膜讀取辨識上，因人的瞳孔受外界刺激而放大縮小，而影響辨別；又如臉貌體形，因鬚髮、年齡、光線照射、高矮胖瘦的改變，使區別相同個體變得困難。臉部辨識雖然普遍，但使用機器辨識造成誤判的情形往往比查驗員人工辨識高，因爲電腦機器辨識過於嚴苛之故，以德國爲例[169]，德國政府前年底開始發行電子護照，卻多次發生民眾過不了關的情況，德國當局只好發佈民眾在辨識時，應遵守以下規則，包括:面對辨識攝影機時，應維持和護照照片一樣的「中性」表情，不可嘻皮笑臉也不能露出牙齒，額頭盡量不要瀏海，並盡量露出耳朵。國際上一本權威刊物的測試報告中也指出[170]，面孔辨識很輕易的由帶上數位相片面具再挖兩個鼻洞的方

---

[167] 參閱:獨一無二 無可取代-生物辨識系統，網際先鋒，2001 年二月

[34] 參考 Kristen Batch, Lynette I. Millett, Joseph N.Pato, Editors，〈Summary of a Workshop on the Technology, Policy, and Cultural Dimensions of Biometric systems〉

[169] 參閱:晶片護照快易通?爭議多惹民怨，中國時報，2007 年 1 月 15 日。

[170] 參閱:生物指紋辨識科技，盛泓科技股份有限公司，

式闖關成功；語音辨識也是如此，在測試中，無論錄音或模仿本人聲音，都很容易破解。

華盛頓舉辦的專題研討會當中，有些研究者即以 sheep、goat、lamb、wolves 來表示生物統計系統在辨別說話者會出現錯誤的可能情形，說明了實行生物辨識身分系統會面臨的挑戰，這樣的挑戰源自於多樣性,特別是在辨識大量人口中的不同說話者:

1.sheep:代表最大比例的人口,他們行爲可被預測和真實性可被系統辨識。

2.goats:較少數人口，具有不可預測和辨識的特性，常會導致性統偵測錯誤。以致於身分的誤判。

3.lambs:容易被模仿。以致於個人資料輕易被取得、變更，造成隱私權侵害、財產名譽被盜用破壞。

4.wolves:可輕鬆模仿其他動物，wolves 與 lambs 容易跟其他動物混淆，造成配對錯誤。[171]使身分判斷錯誤，影響個人相關權益。

而這些都是科學不確定性的風險面，即使官方不斷傳遞發生錯誤的比對機率小，但要考量的是若出現錯誤比對結果，這比對錯誤的結果所造成的不利益，不僅由政府所負擔，更會外溢到不相干的人民身上，使其需要承擔錯誤比對的風險。

四、人類與非人類因素造成的風險

非科技因素，如人類因素、使用者的訓練，可造成重大衝擊

---

http://www.mold.net.tw/quint/organism.htm

[171] 參考 Kristen Batch, Lynette I. Millett, Joseph N.Pato, Editors，〈Summary of a Workshop on the Technology, Policy, and Cultural Dimensions of Biometric systems〉

在生物測定系統的實施上。如對生物辨識身分制度系統感到太過放心，是安全措施不足風險產生的主因。以 Willison 和 Backhouse，2001 年關於犯罪機會和資訊安全的研究爲例，犯罪機會風險的產生包含犯罪的動機，如不誠實的員工濫用電腦，與欠缺安全的結果，如缺乏適當的監控與防護措施[172]。

其中，Clarke 的犯罪具體機會結構(Crime specific opportunity structure)，結合多種犯罪學理論，如情境犯罪預防理論、理性選擇觀點、環境犯罪學、日常活動理論、生活方式理論，企圖提供機會風險的新觀點，認爲組織內部不誠實的成員是潛在的犯罪者，還探討環境中潛在的犯罪者與便利因素(facilitators)、目標與犧牲者之間的互動[173]。此即表示，生物辨識身分制度系統環境所造成的風險種類繁多，不僅只有非人類因素的資訊安全防護措施是系統的安全罩門，一些人類因素如人員安全管理、人員粗心的操作亦是。

了解機會可抑制內部的歹徒與外部犯罪者的行爲，而這可透過員工教育和覺醒計畫，藉在監視關係中主張員工本份的角色，而犯罪明確機會結構模式是一個概念工具，可提供總體的控制環境，和強調團體中成員之間的關係。

五、引發新的犯罪機會、增加犯罪機會

生物特徵識別身分制度管理的挑戰，將非常依賴應用的要求(the application requirements)、系統規模和安全環境[174]。即使在電

---

[172] 參考 Robin Mansell and Brian S. Collins，〈Risk management in cyberspace〉，p356－362, 2005 有關資訊系統中犯罪機會角色的研究。

[173] 參考 Robin Mansell and Brian S. Collins，〈Risk management in cyberspace〉，p360－362, 2005 有關 Clarke 的犯罪具體機會結構(Crime specific opportunity structure)的論述。

[174] Kristen Batch, Lynette I. Millett, Joseph N.Pato, Editors，〈Summary of a Workshop

子交易方面，過往的認證以及保密方式，如使用個人密碼，也難以確保認證過程的安全性，除了使用者遺忘密碼導致錯誤外，簡單的密碼也可能容易被被猜測破解，因而造成被盜用或入侵的風險，所以光是密碼此項防護隱私的措施，就具有變更性和可竊取性，而使得個人權益遭受侵犯和損害。

雖然外交部認爲我國晶片護照內的個人資料有電子簽章（PKI）加密保護，晶片需在 2-5 公分間的距離才能被讀取，此外多數國家採用，的「基本讀取管制功能」（BAC）編碼，也必須在打開護照本，並以光學字型辨識機（OCR）讀取護照資料頁上的可判讀碼，才能解碼啓動閱讀機與晶片護照連結，若未經這些程序即無法讀取，故個人資料乃經過層層保護關卡。

然而晶片護照雖在技術上有安全措施，但國際上的研究仍出現了許多安全上的顧慮，去年八月一日，在美國拉斯維加斯舉行的「黑帽」(Black Hat)電腦安全會議上，一位來自德國的電腦安全專家盧卡斯.格倫瓦德拿出一份德國政府簽發的電子護照，當場示範從其中取得護照持有人的生物辨識資料，並複製到另一片空白的晶片上，並表示他只花了兩個星期的時間與兩百美元，就研究出這套破解電子護照的方法；其實早在去年一月，荷蘭就傳出有駭客大顯身手，取得他人電子護照持有人的生日、照片、指紋等個人資料，而且宣稱可以在距離查驗護照處時十公尺的地方進行[175]。一群電腦專家最近更用實際行動證明，他們可以破解英國護照的晶片密碼，並順利將病毒植入晶片，造成電腦系統癱瘓[176]。故電子護照、生物特徵辨識資料庫雖是趨勢，但其安全性卻讓人憂心忡忡。

---

on the Technology, Policy, and Cultural Dimensions of Biometric systems〉, p3, 2005

[175] 參閱:破解術，德國專家只花兩周兩百美元，中國時報，2007 年 1 月 15 日

[176] 參閱:晶片護照快易通?爭議多惹民怨，中國時報，2007 年 1 月 15 日。

另外針對各項生物特徵辨識的風險來說，臉部辨識，除了臉上的飾物、鬚髮會影響辨識外，在整型文化愈益盛行的台灣在地，這項辨識技術也遭到嚴厲考驗，也許未來可預見某台灣旅行團帶愛美的團員赴韓國整型[177]、施打玻尿酸、泰國注射賀爾蒙後，全體團員全都入境時全被當成持僞造晶片護照處理了；或者於國內整型完後，發現自己不錦不能出入境，就連在國內所有有裝置生物特徵辨識系統的場所，尤其是設有臉部辨識的場所，都成了拒絕往來戶；此外指紋也可被僞造，要僞造是相當容易的，只需要一些很普遍就可獲得的產品，從膠水到尖端攝影科技，它可以很簡單地複製一個指紋將它運用在一個人的手指上。而預防之道有二種方法，一是訓練個人去監視和控制採及指紋過程，但代價是昂貴的，這要求須受良好訓練和專業的員工；二是無生命探測器的使用，如美國 Lumidigm 是世界上首家擁有無生命探測器運作的公司[178]。

國際上對生物辨識系統主流的意見認爲，爲預防個人權亦遭不法之徒侵害，一些電子交易除了個人密碼外還會佐以個人簽章來增加權益的防護，同理，也可運用在生物辨識身分制度上，因爲生理特徵，如手纹、指紋或聲纹容易被竊取及紀錄，故可將各種生物辨識身分系統交相搭配，以降低隱私權被侵犯的可能性，如指纹輔以虹膜和體型辯識、臉部輔以手掌纹、手掌紋輔以虹膜、簽字識別搭配。

而若透過公權力的介入，執行搜集全民的生物特徵資料及建

---

[177] 台視 2005 年 6 月 21 日新聞報導指出，最近幾年國人流行組團到韓國作整形旅遊，其實台灣的醫療技術在國際間也受到肯定，尤其整形價格便宜，外國人更是趨之若鶩，因此衛生署和觀光局合作，推動保健旅遊計劃，以後醫院將進駐墾丁地區飯店，遊客能一邊度假，一邊享受醫療美容服務。

[178] Roberto TAVANO、Pr. Juliet Lodge、Ronald Huijgens、Kamini Aisola、Marc Flammang,《Biometrics in Europe》, European Biometrics Portal Trend Report 2006,June 2006 3.2.3

檔，就附帶責任必須確保資訊保管的安全，承擔管理風險，防範資料外洩、遭竄改變更，且須考量相關補救措施，如若生物特徵資料流失被盜用，該如何補救?保管不當的法律訴訟，政府如何承擔？人民如何獲得救濟？資料庫系統的安全、保密、傳輸安全措施是否完備齊全?此類新的犯罪機會會將引發何種新原則、責任與義務的需求?

此外正如李德財針對按指紋事件所言:「按捺指紋能夠掃清所有黑幫?這些問題得不到回覆的話，那還提什麼改善治安啊!我們要注意，前科犯指紋資料庫和全民指紋資料庫之間，是有很大落差的。然而，即使法律明確規定警察可以隨時便利地查詢和利用，全民指紋資料能夠比目前已有的前科犯指紋資料庫多帶來多少邊際效益呢？對於『全民』指紋資料庫是否真正能夠達到打擊犯罪等「好處」，我們仍舊抱持保留的態度[179]」。

確定的是，電子護照若需要達到安全控制高度的要求，上需要建置以下功能，經由其他的安全技術降低風險[180]:

1.基本取控制功能(BAC):防止側錄及讀取晶片護照，但護照號碼、有效日期不可洩漏。

2.被動式驗證功能((PA):驗證資料(護照)爲合法核發且晶片內資料未被竄改。

3.主動式驗證功能(AA):防止晶片被複製。

4.強化存取控制功能(EAC):針對個人隱私資料，如指紋，進行加密。

---

[179] 參閱李德財 2005 年 5 月 25 日於 tw.bbs.soc.taiwaneseg 對指紋案的意見，http://groups.google.com.tw/group/tw.bbs.soc.taiwanese/browse_thread/thread/93c4aab22e4a21ae/14c2ea00759c670b?lnk=st&q=%E6%9D%8E%E5%BE%B7%E8%B2%A1&rnum=11&hl=zh-TW#14c2ea00759c670b

[180] 移民署副署長蔡震榮研考會意見書。

只是值得思考的是，爲了降低新護照措施的不安全疑慮，反需要建置更多技術成本來防範與規避它的技術風險性，那這樣的新措施是否真有不得不採行的必要，實有待商榷。

六、全球化與文化背景的社會風險

九一一恐怖攻擊事件後，追查涉案的恐怖份子，都是持僞造身分證件進入美國，恐怖份子可以改名換姓，甚至改造外貌，但是卻不易改變與生俱來的生物特徵[181]，這使得世界各國爲加強人口管理或入境管理，紛紛採取生物辨識技術。2004 年初美國政府率先於入境檢查站大規模採用生物辨識技術，掃描顏面特徵、指紋或其他生理特徵以確定護照或簽證持有人之身分。而歐盟的各主要國家中只有英國積極與美國磋商有關事宜，而其他國家的疑慮，包括了美國將以此建立他國公民的龐大身分資料庫，並干涉了他國的身分登記政策，這已不僅是外交上的難題，更牽涉到各國內政策法制的變動，其中就數據整合和程序分析、生物檢測資訊團結和資料庫整合所引發的社會風險亦不容忽視。

面對生物辨識系統一波波襲來的銳不可擋趨勢，2003 年 6 月歐盟在賽薩洛尼基(Thessaloniki)召開會議，各國一致認爲使用於護照或旅行證件上之生物辨識資料或生物檢測資料標準有謀求一致之必要性[182]，而最後於 2004 年 12 月公布廣泛適用於歐盟國家之 15152/04 規則。香港從 2007 年 2 月開始也要換發電子護照，然而即使目前已有歐美、亞太等三十多個國家使用新型的生物特徵辨識電子護照，，照趨勢走向可推估晶片護照核發國家近一、

[181] 參閱陳瑞廣、刑事局指紋編輯室，好用的生物特徵：指紋身分辨識，刑事雙月刊，May-June2005

[182] 參閱劉億成，歐盟「護照及旅行證件生物辨識、檢測資料標準規則」之簡介，科技法律透析，2005 年 2 月

二年內甚至可能達到 50 餘國，但這也引發生物辨識科技費用高昂，新護照的成本及有效期限大幅縮短將轉嫁給消費者，英國核發新型護照後，其成人護照連漲了三成，引發民眾怨聲不斷[183]。

因此文化的不同也會衝擊系統安全，故又該如何採取合適的考量來管理生物特徵資料庫，多國的全球策略通常反應西方價值與文化，所以可能不易建立在其他的文化中，因此會產生許多社會風險，如 Hofstede 提到的三項社會風險[184]:

1. face saving 面子問題，員工感覺提出操作問題或暴露自己是困窘的
2. Criticism avoidance 避免批評:避免和管理階層衝突和批評
3. Kreng－Jai:不願承認我做不到，誠實或直接的答案是難說出口的。

故當地文化可能會與領導機關的價值與意圖碰撞，如印按指紋，在台灣的文化中常常隱含著犯罪，且接受處觸指紋掃瞄器時的的衛生問題，其所造成不安全也因在社會風險的考量之內。國際間科技的相互操作，必須要有科技的能力，但問題不能單一用科技解決，國與國間機構的信任議題其實是更不容易處理的，即使組織的參與者有發展工業互相操作的目標，仍有達成目標的大量問題，障礙從來不只是單一的科技問題，而是牽涉組織系統的文化政治層面。故對系統較佳的實行方式和全球生物測定系統的使用而言，相互合作和有一套標準是重要的。

---

[183] 參閱：美國將在簽證作業採用生物辨識技術，http://stlc.iii.org.tw/tlnews/net9208.htm，參訪日期:2006.9.30。

[184] 參考 Robin Mansell and Brian S. Collins，〈Risk management in cyberspace〉，p362－365, 2005 有關全球銀行內部控制系統的研究。

七、個人和家族污名化及社會歧視風險

生物測定資訊必須被當成個人資料來考慮，因爲此模板(template)與個人資料連結，若收集的資料(如臉部影像)可提供附加訊息有關種族與宗教的資料，個人資料的敏感性特徵可能被強化；相反的，我們也要評估只是爲了測試目的收集的原始(raw)生物測定資料，此類原始生物特徵資料非連結到個人資訊，但這樣的權益(interest)卻被嚴謹地侷限在執行評估和基準上，如配對速度，兩種系統匹配和非匹配的比例[185]。

另，生物辨識身分制度的實施應考量種族歧視、差別待遇的問題，應用的環境必須無種族歧視的問題，並可順應那些對生物測定科技和過程不熟悉、和不願意合作的人，延伸至台灣本土在地化的情境則應考量個人與家族污名化的問題，特定族群可能在該系統下被貼上污名的標籤；或部份殘障人士可能因爲無法進行生物辨識身分制度而遭受誣陷、差別待遇；使犯罪者、曾遭受司法調查及矯治更加汙名化，迫使這類人口更生保護、回歸社會更加困難，也使得社會階層分化加劇；更甚者個人、家族或族群生物特徵資料的暴露、外洩所造成的相關權利侵害與歧視的差別待遇，最後演變的世代、家族或族群歷史事件[186]，這都是應考量的問題。

然而內政部移民署是台灣率先決定對大陸旅客與大陸配偶採用臉部特徵生物辨識系統的管制機關，即使管制機關主張生物特徵辨識將針對所有外來人是實施，因大陸地區人民申請案以「同名異人、同人異名」僞造身分情況較爲嚴重，故第一階段先從大

[185] Roberto TAVANO、Pr. Juliet Lodge、Ronald Huijgens、Kamini Aisola、Marc Flammang,《Biometrics in Europe》, European Biometrics Portal Trend Report 2006,June 2006 4.1.2

[186] 周桂田、張淳美〈生物特徵、指紋資料庫風險〉科學發展 398 期，2006 年 2 月

陸地區人民實施，再逐步擴及所有外來人士。然而因爲管制機關對民眾的資訊公開、澄清與風險溝通的不足，使得相關人權、利益團體與民眾認爲移民署此舉乃針對單一族群歧視的行爲，因而引起相關權益族群的抗議，如中國時報 2007 年 1 月 3 日報導記載移民署門口聚集著一群抗議的大陸配偶，高喊「要工作、要身分、要人權」，抨擊海關人臉生物辨識對她們是歧視，要求所有權利比照外籍配偶[187]。

此外生物特徵辨識系統雖可用來認證無法認證自己的族群，如嬰兒、殘障人士、老人痴呆者或其他有弱點(vulnerable)的團體，如藥物濫用者、流浪漢，但當這些人口沒有或少有資格能同意給資訊時，從倫理觀點來看這是倍受批評的。再來以生物醫學角度剖析，生物特徵辨識技術雖也可應用在生物醫學的潛在來源或關於個人舉止資訊，但都可能會增加歧視風險和多重的強制測試程序，因爲有些生物測定特徵，如 DNA 可能顯露很多醫學資訊包括潛在的疾病，可能會洩漏一個人有無喝酒喝酒、吸毒、用藥、懷孕、年老與否等，這也是值得重視的一點風險。

肆、風險溝通公共領域的欠缺

生物辨識技術以犯罪防治、偵查爲主體具有功能的高度風險性，積極而言，它可能有防止雙重身分、入出境移民、門禁安全使用者、意外災害罹難者、無名屍、遊民、失智老人、走失兒童身分確認、勤惰管理等用途；消極而言，由於資料庫涉及的個人資料龐大，任何人爲或非人爲的管理出了差錯，影響的也許不只是少數被辨識錯誤的使用者權益，而是直接衝擊到資料外洩的社

[187]〈陸娘反歧視 控訴淪爲幽靈人口〉,中國時報，2007 年 1 月 3 日

會治安、社會倫理、國防安全層面，並且，直至目前爲止，沒有任何科學家驗證出它的真正安全性，即使是晶片護照，也沒有任何一個國家可以保證，晶片護照不會被僞造，以上此種正反面的弔詭性辯論凸顯了高科技發展的侷限與風險。首先是高科技本身安全的爭議性，人們無法再直接以計算、控制來保證；其次是高科技發展不能純粹再由科學家、科技官僚所決定，而是必須與社會整體關聯起來，由社會民主來決策[188]。

台灣一味效法各國生物特徵辨識技術的運用，卻忽略了要移植各國注重科技與社會互動、溝通機制的反省的生物特徵辨識技術公共領域，而公共領域正是風險溝通的場域，風險溝通鑲嵌於各國制度與文化之中，文化的不同會衝擊系統安全，西方國家的價值與文化可能不易建立在其他的文化中，這都是危及生物特徵資料庫的安全徵結，因此也會產生許多社會風險，如在 ICT 資訊與通訊技術中，倫敦的員工當感到模稜兩可時，會使用個人判斷去作出最好的決定；泰國的員工會回辦公室詢問老闆[189]。所以當仰賴電腦通訊設備的生物特徵資料庫普遍地建立，文化的不同會衝擊組織的系統安全。

生物特徵辨識技術使關於電子身分的 E-管理和隱私保障的角色重要性變得明朗，此外還有一項不可忽視的觀點即科技是工具，因爲它的角色與管理相關，所以潛在地會帶來無法預期的問題，包括科技挑戰和隱私爭論。技術官僚與科學群體對科技的風險論述，基本上應該是相當多元與競爭，他們在風險溝通過程中也扮演了相當重要的角色，國家技術官僚對科技的風險認知與態度，往往影響著科技政策重大走向，也進而關係著社會公眾對科技風險的思考，一旦技術官僚對

[188] 參閱周桂田，高科技風險社會，http://bio.idv.tw/data/data2/2000010001.htm
[189] 參閱 Robin Mansell and Brian S. Collins，〈Risk management in cyberspace〉，p362－365, 2005

科技風險未採取開放式的、中立式的態度，公眾對於科技爭議的風險評估結果往往質疑其黑箱作業而毫不信任[190]，但無論如何，藉由人民、政府官員、公民的對話可啓蒙與解決此問題。

除了包括(1)評估生物測定系統內容、目的、政策的重要性；(2)就決策而言，建立決定有效性資料的標準(3)制定謹慎的過程以維持、分享數位紀錄[191]外，生物辨識技術的資訊分享應更廣泛地被討論，雖然科學技術官僚習慣以單方面的科學宣導與教育方式，認爲公眾只要接受正確的引導，就能夠對科技產生正確認識，然而我們往往看到這種缺乏雙向、互動式科技與社會的溝通，或排除公眾參與科技評估並肯認社會多元領域的價值判斷，使得在科技發展與科技政策蒙上黑箱作業之譏，尤其一旦引發風險的爭議性，其正當性則普遍受到質疑。

因此，世界先進工業科技國自 1990 年代中起已注意到這個問題嚴重性，紛紛發展不同的公眾參與或涉入科技評估機制，就風險溝通的實施步驟來說，國外制度公民訴訟、公眾參與程度、公民會議、公聽會、計劃環境影響評估模型到政策評估模型，更納入社會相關代表團體的參與（如法人團體參與評估）等等[192]，如歐盟、IRGC (International Risk Governance Council)及其他國際相關組織或政府單位，分別意識到風險感知、風險溝通與公眾參與的重要性[193]。

---

[190] 周桂田，爭議性之風險溝通-以基因改造工程爲思考點，生物科技與法律研究通訊，第十八期，頁 51

[191] Kristen Batch, Lynette I. Millett, Joseph N.Pato, Editors，〈Summary of a Workshop on the Technology, Policy, and Cultural Dimensions of Biometric systems〉，p3－4，2005

[192] 周桂田，爭議性之風險溝通-以基因改造工程爲思考點，生物科技與法律研究通訊，第十八期

[193] Kuei-Tien Chou，Trust、Risk Communication in Double Risk Society， Presented on 2006 Annual Conference of Taiwanese Sociological Association，November 25 2006，Taipei，Taiwan.

風險溝通是一個相當複雜的過程，最基本的影響溝通機制包括政府、媒體、公眾及社會與政治相關機構等的行動（包括社會運動、政治運動）(Miller & Macintryrt 1999:229)。它不只是告知(informing)、傾聽(listening)、言說(telling)和影響(influence)等單面向的程序 Taig(1999:226)[194]，最重要的是風險資訊的來源與公眾對於風險資訊的信任[195]。換句話說，技術官僚對風險溝通中訊息、管道的釋放與建立方式，將影響公眾對資訊、風險事件、甚至決策者的信任[196]。

公眾對風險的感知與溝通，除了科學風險評估所提供的資料證據之外，風險溝通的結構、機制與其所產生的溝通文化，將也影響公眾對風險的感知與信任。如果欠缺完整的風險溝通結構，而任由片面或封閉性的制度形式所壟斷，將逐漸的演變爲各種社會系統（包和社會、政治、科學與決策）的發展與遲滯[197]。

台灣在地社會長期處於風險的無知，對於風險的認知僅僅停留在科技風險、風險運動的論述，基本上社會和科技在地的溝通與反饋都是不完整的。以數年與生物辨識息息相關的反對個人資

---

[194] Arkin(1989:125)指出，風險溝通經常會被侷限在(一)風險科學的本質(nature of risk science)及(二)公眾風險感知本身。具爭議、複雜風險的科學問題或災難，經常會形成公眾理解(Public understanding of science)的障礙，一方面是風險科學本身的不確定性與複雜度，無法帶給公眾確切的安全感知答案，另一方面是公眾知識與資訊的落差(knowledge information gap)、取得資訊的管道也可能阻礙了公眾社會學習的機會。進一步的說，國家、媒體或社會（公眾）網絡所釋出的風險資訊，相當程度的將影響公眾對風險的主觀感知與客觀的行動認知。

[195] Kuei-Tien Chou，Trust、Risk Communication in Double Risk Society， Presented on 2006 Annual Conference of Taiwanese Sociological Association，November 25 2006，Taipei，Taiwan.

[196] 尤其，許多學者（Frewer 1999；Taig 1999；Slovic 2000a）指出公眾對於爭議性科技的信任相當敏感與脆弱，包括公眾爲對於新的風險資訊過度反應、對於各種解決風險方式的選擇、風險爭議常演變成其他議題、科技帶來的利益可風景能大於風險。

[197] Kuei-Tien Chou, Trust、Risk Communication in Double Risk Society, Presented on 2006 Annual Conference of Taiwanese Sociological Association, November 25 2006, Taipei, Taiwan.

料或換發身分證按捺指紋案當社會運動來看，大部份是菁英專業份子或團體透過專業的異議集中在法案上的鬥爭上，並擅常運用媒體相關風險論述的議題設定，擴大輿論形成政治社會壓力，即使在社會運動的動員與結盟上，也僅透過既有社會運動團體間的串連支持形成壓力，較少直接動員民眾，包括了 1998 年社運團體抗議國民 IC 卡事件的串連、2003 年全民個人資料保護聯盟、及 2005 年以台灣人權協會爲主發動 60 餘起社運團體串連的「我不按指紋，給我身分證」運動[198]。

反觀歐美各國，在引進生物特徵辨識技術之前，扮演生物特徵辨識技術的風險溝通公共領域爲數眾多，如當美國政府宣佈，2006 年十月起，所有美國護照都需要植入可遠端讀取的電腦晶片，而在護照中加入 RFID 晶片在美國引發不小的反對聲浪[199]，因爲反對人士擔心有心人士利用強波天線瞄準持有護照的人或交通工具，就可以從空中截取到個人資訊。美國國務院收到的 2,335 意見調查中，98.5%持反對意見，安全及隱私問題是最主要原因。

但布希政府干犯眾怒，仍然決定未來要在新版護照內嵌入 64KB 晶片，表示希望願意遵守由聯合國下的國際民航組織所制定的「全球相容」標準，其他國家包括英、德也都宣佈了類似計畫。而美國務院也表示已對隱私安全採取措施，國務院指出，護照中的晶片「不得進行『追蹤』，只允許政府獲知使用者已經到達了某個機場，而這早可以利用非電子護照得知，只是電子護照可以更確定遞出護照者是合法的持照人。」爲了平息美國人對身分竊取的疑慮，布希政府表示新護照將會在封面加裝「反側錄

[198] 周桂田，2006，〈遲滯型高科技風險社會下之典範鬥爭:以換發身分證按捺指紋案爲分析〉，《政治與社會哲學評論》，第十七期，頁 154

[199] 美護照明年全面植入 RFID 晶片，CNET 新聞專區：Declan McCullagh and Anne Broache，26/10/2005 ，http://taiwan.cnet.com/news/comms/0,2000062978,20102149,00.htm

(antiskimming)物質」，以「減少」被遠端竊取的風險。但這種防止 RFID 強波天線技術的效果如何則並不清楚，負責評估晶片抵禦電波刺探的美國國家標準和科技機構也無法提供進一步資訊。

隱私權倡議人士，RFIDkills.com 創建人 Bill Scannell，美政府是在人民的護照架一個超迷人電台，然後用水泥覆蓋住，但如果門一打開，你還是收聽得到音樂。「有的確總比沒有好，但我們爲什麼要冒這種險呢？」，」Scannell 說。此外，新美國護照將使用「Basic Access Control」（基本存取控制）技術，這是在晶片內儲存一對加密的密鑰。只要讀取器成功獲得授權，RFID 晶片就會把一切資訊全吐出來。電腦科學家卻批評這種加密技術是有瑕庇的。RSA 實驗室的 Ari Juels 與卡羅來納大學 David Molnar 及 David Wagner 警告這種密鑰不夠安全，表示如果電子護照從頭到尾只適用單一固定密鑰，就可能發生問題。而布希政府也可能面臨來自法律層面的挑戰。隱私權人士在致函國務院指出，這項措施「並不具法定職權，因爲並沒有獲得國會通過。

對照美國生物辨識在美國境內引起的各方領域公眾的熱列回響，顯示台灣生物辨識領域的公共領域卻仍有待開發，而試著從各國相關組織簡述瞭解歐美英各國相關組織對生物辨識身分制度議題關注，有助於捕捉各國此制度措施的動態，以供臺灣作爲借鏡。

一、 美國組織

(一)CSTB (The Computer Science and Telecommunications Board)，http://cstb.org

它乃美國國家研究會議(the National Research Council)的一部分，工能是向聯邦管制機關提供有關電腦和通訊的科技與公共政策議題獨立的建議，成員組成包括工業與學術界。

其任務如下:1 回應管制機關、非利益團體和私人工業 2 監視和促進電腦科學和電信通訊領域的健康 3 引進和指導研究 4 促進電腦和電信通訊科技的研究。

(二)EPIC (The Electronic Privacy Information Center)，http://www.epic.org/epic/jobs.html

電子隱私資訊中心是一個主要網際網路公民自由組織，位於華盛頓特區，致力於保護公眾利益，關於網際網路的未來在決定中促進公眾聲音、公民自由問題和保護隱私、the First Amendment(第一修正案)，和憲法價值。從事公眾利益訴訟，進行公共教育，在國會作證，組織會議，調整基層擁護，出版書，報告，和線上簡報。

(三)The Biometric Consortium，http://www.biometrics.org/

生物統計學協會以研究，發展，測試，評估生物辨識建立的私人鑒定/查證技術申請作爲焦點。生物辨識協會每年秋季會組織一個重要的生物辨識會議。關於過去的會議，目前的政府和標準活動，電子佈告欄服務(You may join the BCBB at http://biometrics.propagation.net)，和其他生物辨識的資源的資訊可以在此網站找到。

會議是開放給普通老百姓，主題適合各式各樣的個人 - 政策開發者和決策者，政府和工業主管人員，資訊產業使用者和開發者， IT 總裁， CTOs 和產品經理，執法官，系統整合者，私人的證明和資訊安全專家，教育家和學生，政府，工業，和學術生涯的研究人員和每個人，涉及利用生物辨識解決私人的鑒定/證明申請，和識別碼偷竊行爲的防止，包括國家安全。

另，Biometrics Catalog，生物辨識目錄是一美國政府資助的生物辨識的技術的資訊，關於包括調查和評估報告，政府文件，

立法機關的文字、新聞文章，會議表演，和廠商/顧問的資料庫，在生物辨識目錄中增加和取得資訊是自由和獲得鼓勵的。

(四)ICAMS (The International Campaign Against Mass Surveillance)，http://www.i-cams.org/About_ICAMS.html

對抗大規模監督的國際運動(ICAMS)乃美國公民自由協會所建立，著重於全球南方，是國家的法規，監視團體和 Statewatch 的國際公民自由上的朋友委員會(the Friends' Committee on National Legislation, the International Civil Liberties Monitoring Group and Statewatch.)。

ICAMS 於 2005 年 4 月 20 日，集合將近一百個來自世界各地的團體的支持，在馬尼拉，渥太華和華盛頓的倫敦被提出。ICAMS 報告，「用於大眾註冊的一項全球基礎設施的出現和監督」，隨著運動的發展發行，在 2005 年 ICAMS 將發展運動還尋求自非政府的團體和公眾的背書。

(五)SANS(SysAdmin、Audit、Network、Security)，http://www.sans.org/vendor/expect.php

SANS 是資訊安全訓練及認證的最大來源。也發展、保持、提供免費與收集關於資訊安全的各方面的研究，它也操作網際網路的預先報警系統 - 網際網路風暴中心。

SANS（SysAdmin，審計，網路，安全）學院正如一個結合研究和教育的組織，於 1989 年在美國華盛頓成立。其計畫現在已達到超過 165,000 個安全專業人士、查帳員、系統管理員、網路管理員、重要的資訊安全官員和 CIOs，一同分享他們所學及面對挑戰的解決方案。在 SANS 中心有許多在政府機構、公司、全世界的大學的安全從業者，每年把數百小時投資到研究和教學來幫助整個資訊安全社群。我們的目標乃是將 SANS 參與者的期望

展覽，提供觀眾的一段簡介，有效地幫助你以加入我們作爲目標。

(六)BIOMETRICS CATALOG，http://www.biometricscatalog.org/default.aspx

生物辨識目錄乃由美國管制機關資助，是可免費使用的關於生物統計學科技公共資訊的資料庫，包含或排斥選用不意味著管制機關批准或不批准，生物辨識目錄目前被它的使用者保存，由使用者來增加它的資訊。

此外，生物辨識 NSTC 附屬委員會發展了一份生物統計學隱私文件。附屬委員會高度建議這文件可被視爲一個參考使用：<Privacy & Biometrics Building a Conceptual Foundation> http://www.biometricscatalog.org/biometrics/privacy.aspx

(七)EFF(the Electronic Frontier Foundation)，http://www.eff.org/about/

從網際網路到 iPod，技術在改變我們的社會和賦予我們，如人、公民、創建者和消費者的權利。當我們的自由在網路世界被襲擊的，電子邊境基礎 (EFF) 是第一防線。EFF 在 1990 年被建立，早先是網際網路上的大多數人的雷達、今日則繼續面臨了保護言論自由，隱私，革新，和消費者的尖端問題。從一開始， EFF 就與影響公眾利益的數位權利而戰。

混合專業律師、政策分析家、活躍分子和科技人員， EFF 爲消費者和普通老百姓勝利努力。EFF 在法庭主要爲自由訴訟奮鬥，即使在那意味著具有美國政府或大公司的訴訟。透過我們的行動中心動員了超過 50,000 個有關的公民， EFF 打敗壞立法。除了建議政策制訂者， EFF 也教育了新聞界和公眾， EFF 也支持增強自由發明的發展。

二、 歐洲組織

(一)EBF(The European Biometrics Forum)，

http://www.eubiometricforum.com/

歐洲辨識學論壇是被歐洲委員會支持的一個獨立歐洲的組織，其抱負乃是建立歐盟成爲傑出生物辨識的世界領袖，透過傳達障礙到採用和市場的分裂。論壇也充當協調推動力、支持和國家體制的增強。

EBF 的成員超過 100 個，包括更寬闊的生物辨識社群，如生物統計學的公司，研究代理，政策制訂者和使用者團體。EBF 如一個資訊中心和網絡，促進這些實體之間的資訊的交換。爲了指明其目標和目標， EBF 在歐洲的生物辨識上區別了四主要社群，政策、公眾、工業和研究。

政策 - EBF 的一個主要的目標乃是是決策者的參考點，表達關注，提供關於生物辨識領域的高品質的資訊。

公眾 – 因爲生物辨識影響每個歐洲的公民的，EBF 的目標乃提高公眾意識，表示關注，促進使用者友好，社會接受，和道德的生物辨識發展

工業 - 生物辨識是一個快速成長的工業，EBF 目標是支持歐盟強和有競爭力的生物辨識市場發展。

研究 - 新興的科技的成長是極爲重要的，例如生物辨識。EBF 致力於促進和增進世界級的研製、執行評估和爲生物辨識技術制訂標準的發展

EBF 新總裁，Max Snijder 說「我決心增強和支持 EBF 在生物辨識社群中作爲中立玩家的角色，覆蓋歐洲的公民，政府，研製中心和工業中的利益」

(二)ECLN(European Civil Liberties Network)，http://www.ecln.org/

ECLN 是在 2005 年 10 月 19 日被發起，是一個長期的計畫，計畫發展一個爲全歐洲公民自由問題工作的團體平台。參與的組織分享共同的目標，試圖建立一個以自由和差異爲依據的歐洲社會，一個以公民自由和私人.政治自由爲基礎的社會，擁有資訊自由、行動自由，和全歐洲的平等權。這個網站如同公民自由團體的佈告欄，透過宣傳會議，研究，運動和展示。一系列的「在公民自由和民主防衛的文章」標記了 ECLN 的成立。這些文章處理了大量的問題:當代的種族歧視和「Islamaphobia，反恐戰爭」和人權，「演講罪行」和放逐，歐盟決策，監督，移民入境和收容所的政治和技術，資訊自由，刑事制度和孩童的權利。

(三)EDRI(Digital Civil Rights in Europe)，http://www.edri.org/

歐洲數位權利是國際非營利協會，成立於 2002 年六月，目前有 21 個隱私和市民權利組織是 EDRI 的成員，他們來自於歐洲 14 個城市。歐洲數位權利的成員聯結共同爲資訊社會的市民權防衛，這也使得歐洲組織的合作需求增加中，如同需要來自於歐盟的更多關於網際網路、著作權、隱私的管制一樣。歐洲數位權利的議題包括隱私、數位權利、網路言論自由、安全、e-投票等。

(四)CHALLENGE: Liberty & Security(The Changing Landscape of European Liberty and Security)，http://www.libertysecurity.org/

此網站都是是由歐盟等贊助的一連串關於歐洲自由與安全的討論文章，文章檔案包括:反恐怖主義鬥爭和內部的安全/ Lutte antiterroriste et securite interieure 收容所外購/ Externalization de l'asile 邊界，放大和鄰近地區/ Frontieres， elargissement，voisinage 重要的基礎設施保護/Protection de 基礎設施評論文章

三、 英國組織

(一)PI(Privacy International)，http://www.privacyinternational.org/

國際隱私國際是人權團體，成立於 1990 年，是監督政府與公司隱私侵略的看門狗(watchdog)。位於英格蘭的倫敦，在華盛頓特區裡也有一間辦公室，從竊聽問題到國家安全、身分證，視訊的監督，資料匹配，醫藥的隱私，到資訊自由問題。從事全世界的調查活動。

(二)IBS (The International Biometric Society)

http://www.tibs.org/about.html

IBS 被英國和愛爾蘭區域旁的國際生物辨識社會所組織。IBS 是在生物科技中促進統計、精確的理論、方法發展和申請的一個國際社會，包括農業，生物醫學的科學和公共衛生，生態學，環境科學，林學，和聯合的學科。社會的成員包括統計人員，數學家，生物的科學家，且歡迎致力於推展資訊收集和詮釋生物科學方面的跨學科的努力。

IBS 出版兩份雜誌，《Biometrics》，此報告與社會任務、美國統計協會一起交流。《*JABES*》(the *Journal of Agricultural, Biological, and Environmental Statistics* .)農業，生物，和環境統計學的雜誌。

《Biometrics》：生物辨識有每季的出售和電子形式。其總目標是透過文章描繪新的生物辨識技術的發展和應用以促進生物科學的統計方法理論和技術的使用。

在雜誌上的文章包括普通的通訊(regular communications)，焦點在新方法的發展，和展現他們的應用在生物科學的特殊問題上；顧問論壇文章，是說明現有的方法應用在以前沒有使用過的新地區或提供指導和澄清上這樣的方法的使用；其它還有讀者反應、以及寫給編輯的信，在雜誌上提供意見及建議。

(三)AsylumSupport.info，http://www.asylumsupport.info/about.htm

AsylumSupport.info 著重於關懷人們尋求收容所的所有事情，連結線上數百筆資源，關於收容所和難民，衝突，國家資料，案子、放逐，滯留，辨別力，資助，性別，政府，人權，交易的人類，法律，媒體，遷移，政策和研究的一個網站。

「透過這個網站，資料變得可接近，這完全爲了促進批評，評論，報告，新聞，教學、獎學金和或收容所支持的系統研究目的。網站特點是這些公平用處和目的材料只爲非營利教育目的。「身爲一個私人的網站，我不保證文字、圖表或任何忠告，見解，文宣或其他資訊的可靠性。在這樣的忠告，見解，文宣或其他資訊上的任何依賴將是自行負責的。」我來自利物浦，在西北英格蘭的一個城市，Frank Corrigan。

四、 跨國際組織

(一) Privacy.Org，http://www.privacy.org/index.html

Privacy.Org 是每日新聞，資訊，和提倡隱私的地點。這個網頁是電子隱私資訊中心（EPIC）和隱私國際(PI)的合作計畫。

Privacy 來源包括國際、消費者、小孩、政府 - FTC、政府 - 歐盟、政府 - 經濟合作發展組織、研究、出版物、EPIC 線上指引、工具、搜尋網、Technorati：隱私部落格、搜尋法規。

(二)OECD(Organisation for Economic Co-operation and Development)，

http://www.oecd.org/home/0,2987,en_2649_201185_1_1_1_1_1,00.html

經濟合作與發展組織有 30 個成員國分享對民主政府和市場經濟的承諾。與 70 個其它國家、NGOs 和民間社團有活躍關係，它與全球有伸手可及的距離。它的出版物和它的統計是最著名的，它的工作覆蓋經濟和社會問題，從鉅觀經濟學、貿易、教育、發展和科學與創新。

經濟合作與發展組織是在促進在公共服務和公司行動上的傑出治理角色。它以部分的監視來確保管制單位對重要經濟領域的回應，它幫助政府決策人員採取戰略取向。它是知名的爲它的個別國家調查和回顧。

經濟合作發展組織生產國際性同意的工具、決定和建議在促進遊戲的規則上，即多邊的協議對單獨的國家在全球化的經濟中在取得進步是必要的.。分享成長的利益也是重要的，例如顯露的經濟，持續的發展，領土的經濟和援助。

對話，共識，同儕審查和壓力是經濟合作發展組織的核心。其管制主體－會議，是由成員國家的代表組成。它提供了在經濟合作發展組織委員會的工作上的指導和決定年度預算。

生物科技方面，經濟合作發展組織持續超過 25 年一直在進行與生物科技相關的主題。這些包括科學，工業產品，健康和農業申請。在生物科技的安全議題中也有一個強而有勢的報告。

(三)on the identity trail，http://idtrail.org/content/view/12/34/

「在身分痕跡上」此計劃的中心目標乃是發展跨學科的對話，使政策制訂者和更廣闊公眾產生價值。我們的專案將整合北美洲和歐洲的研究學科和領域。

網頁上記載，在我們的小組上的二十三名參與者決定要在政策和技術的結果上有一種正面的影響力。他們包括了哲學家，倫理學家，女權主義者，認知的科學家，律師，譯解密碼者，設計，政策分析家，政府政策制訂者，隱私專家，商業領袖，績優公司，和成功的起步公司。我們的研究合夥人包括公眾，私人和非營利的機構領域。

計劃由三支流組成：1.身分的本質和價值，匿名和證明；2.匿名的憲法和法律方面的樣子；3.確定、匿名和驗證的技術

在這裡是我們的一些特別的目標，以網際網路的簡短架構可以設計來在考慮到保護隱私的安全證明。 David Chaum 將在安全電子投票系統上繼續工作，目標使公民透過電子投票，還有透過我們的民主政體的機構進行隱私捍衛要求。Stefan Brands 也將發展保護隱私的密碼編譯的技術，具包括電子健康記錄管理的各種的申請的技術。匿名選舉和隱私敏感的健康記錄是在其公民的隱私權之中是尊敬的一個社會的一個重要的方面。運行隱私權含有容量控制個人資料，經常要求公民存取關於自己和政府的資訊。Ken Anderson, Pippa Lawson, Mary O'Donoghue, Stephanie Perrin and Marc Rotenberg 都在共同努力爲公民、隱私提倡和管制機構生產這些實用的工具。法律保護負擔隱私經常起源於隱私和匿名。根據回應網路犯罪和恐怖主義的威脅，戴弗妮吉伯特和 Ian Kerr 的全球法律改革努力將在憲法中在關於「隱私」標準和其使用「的合理的期望」的一個研究中合作。Kerr 也爲法律將檢查隱私暗示在私人領域中的改革，對自動數碼權利管理著重於有版權的改革和行動。史蒂夫·曼，在監督上建立一部記錄片，將檢查監督的法律和道德的暗示，和關於其他監督行動記錄的資訊隱蔽的途徑。

伍、結語

大多數人皆認爲，人類應善用科技以創造文明新面貌，並避免科技的副作用，而這樣的論述凸顯出高科技社會發展的辯証與矛盾，辯正面在於人們如何「看待」並「善用」科技?在何種社會意識形態下運用科技?如何避開而不爲科技所宰制?德國社會學家貝克(Ulrich Beck)指出人們必須揚棄工業主義時代對科技之控制性、計算性與災難預見性等「善用科技、征服自然」的思維，應肯認高科技風險不可控制性、不可計算與不可預測性，而對於科

技與社會的關係，應基於社會公民的理性批判能力，以溝通、商議來決定科技與社會目的發展之動態平衡[200]。

生物辨識身分制度所引發的社會風險具有多樣化、難預測的特性，不能一味倒向唯科學化、實證主義的生產的邏輯。這套生產的邏輯是以線性因果的思維認爲生物辨識的科技系統爲可控制性(可確實保密、儲存)、可彌補性(爲了治安犧牲一點人權也是值得)、與可回復性(即使資料外洩名譽仍可回復)[201]。然而，由於生物辨識系統涉及龐大的資訊儲存、辨識、利用、流通與管理，在任何一個環節皆有高度的不確定性，並且一旦外洩所引發的風險後果是目前難估計，因此，建議需謹慎評估，並以其他方式來取代運用，並進行替代性的風險評估(alternative assessment)，而非僅以本生物辨識科技系統爲唯一的風險評估標的，以免產生政策上一去不返的滑坡效應，換言之，科學風險評估與政府與人民間的風險溝通，皆不可偏廢。

然而，而台灣在地民眾常無知的忽視生物辨識身分制度將構成風險的潛在嚴重性與不可欲的後果，如隱私權被侵犯、政治上形成警察國家、國家至上的風險、社會上階級汙名化、倫理的風險，以及資訊管理上被冒用、被洩露的風險。究其原因，乃一般民眾對於風險之認知，容易受到資訊流通、媒體報導之影響，形成瀑布效應(cascade effect)，或是對大災難特別有恐懼感，或僅基於過去之經驗或情感式的影響，以及直覺式的損益分析[202]，這種直覺式的損益分析，對於是否應該對某種風險加以管制，有時只看到利益面，而低估危險面，故在媒體造成的知溝(knowledge gap)

---

[200] 參閱周桂田，高科技風險社會，
http://home.pchome.com.tw/education/light917/data/data2/2000010001.htm

[201] 周桂田，2006，〈遲滯型高科技風險社會下之典範鬥爭:以換發身分證按捺指紋案爲分析〉，《政治與社會哲學評論》，第十七期，頁 128

[202] 參閱:許耀明，預防原則與科學證據之前提:風險治理，
http://www.iias.sinica.edu.tw/951216/951216_1_4.pdf

差距下，公眾對於治安風險的未來性較清晰，反對於生物辨識技術的風險較爲模糊，因而在利益與風險分析上傾向於利益面考量，這同時意味著公眾並沒有充分、良好的告知或學習判斷，對於隱私權、資料外洩、科技風險仍處於有待自我啓蒙的社會階段中。

尤其，民眾的風險感知也跟科學技術官僚散佈的資料證據息息相關，因爲經由二手傳播之非經驗所形成的公眾風險意識，事實上也必須從科學風險評估或決策者傳遞的資料訊息引證。而我國的技術官僚，長期以來習慣由上往下、威權式的、線性因果的實證確定性來推動各種科學計畫[203]，以簡單化約、工具性的現代化、單面利益論述建構生物辨識系統的好處，而這些端倪也反映在移民署通關辨識與外交部的晶片護照上。

其實現行爭議性科技所衝擊的領域已逾越了既有的社會、法律、倫理的界限，傳統自然科學風險評估方式雖能夠提供一定的解決功能，但對於爭議性科技所引起在不同社會領域的衝擊與不確定性並無法提供答案，而這個部分所要進行開放式的社會風險評估，關鍵正在於公眾對於爭議性科技風險的理解與認知[204]。不同的風險感知和溝通可成爲強化分析階段的來源，但不是一次就讓政策決定，應要調停不同的感知進入單一政策中，以便處理安全和偶發事件。新科技總是改變社會環境，帶來和引進新風險，而一連串的研究建議以漸進的努力去順應科技的利益與緩和科技帶來的缺點，安全管理者必須抓到科技、政策和行爲三位一體的概念[205]。

---

[203] 周桂田，2006，〈遲滯型高科技風險社會下之典範鬥爭:以換發身分證按捺指紋案爲分析〉，《政治與社會哲學評論》，第十七期

[204] 周桂田，爭議性之風險溝通-以基因改造工程爲思考點，生物科技與法律研究通訊，第十八期

[205] 參考 Robin Mansell and Brian S. Collins，〈Risk management in cyberspace〉，p374,

就以晶片護照、生物辨識系統而言，我們看到，在不同場合中相關管制機構的官員一再追隨與強調主流科學的辨識率效果，以及多少國家已採用的趨勢[206]，在此論點下，單一的科學評估就成爲決策的唯一檢正標準，並難以接受其它科學異議的聲音。換言之，在狹隘性之科學實證性的風險評估哲學下，技術官僚憑藉著獨大的專家政治立場，壟斷性地排除社會、倫理風險，而相對性的認定科學爲唯一評估與溝通的基礎。因此，風險溝通變成單面向的、教育的、扭正社會「情感的或不理性的感知」[207]。

其實國外在試驗實施晶片護照及生物辨識系統相關設施後，出現許多問題，除了新儀器辨識率容易出錯外、仍存有諸多社會、倫理、法律、政治、經濟面向的疑慮，如生物特徵辨識科技費用昂貴，新護照的高成本必定轉嫁消費者，英國政府就因核新型生物護照後[208]，因維護科技設備成本居高不下，迫使英國成人護照連漲三成，飆上每本護照新台幣四千元，引發民眾怨聲不斷。故外交部、移民署的晶片護照與生物辨識通關辨識技術設施，在資金運用與攸關民眾權益的護照成本上，應需儘量斟酌沿用舊有設備、避免將高成本轉嫁給消費者，引發民怨。

此外若以高科技需要高思維相應之風險社會公民理性溝通、批判能力之觀點，來檢視台灣民眾對生物辨識技術、晶片護照反應，不得不指出我國全球在地化風險該加油的地方，包括主管官署的不負責任，置民眾於資訊無知的狀態；但相對的我國公民社

2005

[206] 參閱:移民署:陸客僞造身分入境較嚴重，中國時報，2007 年 1 月 2 日.入出境管理局副局長吳學燕指出，預計於七月在國境上採用的生物辨識系統，辨識率可達九 成七。

[207] Kuei-Tien Chou, “Risk Perception, Risk Communication and Policy Making of GMOs”, Theme: Biotechnology, Family and Community, The Fourth International Conference of Biotechnology, Graduate Institute of Philosophy, National Taiwan University.

[208] 參閱晶片護照快易通?爭議多惹民怨，中國時報，2007 年 1 月 15 日

會仍相當脆弱，對應於此種全球性的高科技風險社會並無法建立監督、溝通並理性批判政府的行動，而這也是台灣欲發展人文高科技島的一項重要警訊與隱憂,更是我們值得共同努力的地方[209]。

各國經常以立法來延宕科技風險的可能性，但在美國的生物辨識技術發展霸權與競爭放任之下，所有的社會風險的門檻紛紛失守。外交部、移民署等晶片護照與生物辨識機器的購買，類此涉及人民重大權利、義務的事項，政府應慎思明辨、決策應保守而謹慎，實不宜在未經國會充分討論、生物辨識科技法源尚在未定之天、及有公民審議程序、聽證程序、公民諮詢與公民會議等公共討論,經過多次且多元廣泛的風險溝通後,達到社會共識時，就動輒撒下龐大資金，讓備受爭議的新制上路，這樣的決策未免過於草率，欠缺謀定而後動的智慧，萬一生物辨識技術有違憲的爭議，在立法程序無法過關，那麼購置的設備豈不是浪費公帑？故從本旨研究建議，不應該在反恐的大論述底下，就冒然實施生物辨識技術、晶片護照等政策,否則將產生風險不可回復的後果。

[209] 參閱周桂田，高科技風險社會，
http://home.pchome.com.tw/education/light917/data/data2/2000010001.htm

第九章　結論與建議：生物特徵身分辨識技術未來應用於我國之規範與政策建議

本章主要內容為結論與建議。本章主要目的在於總結前面各章的內容，分析生物特徵身分辨識技術應用在我國時，應該特別予以留意和處理的規範與政策問題。這些規範和政策問題，隨著外交部準備全面換發具有生物特徵身分辨識機制的晶片護照，並且被列為行政院的重大計劃之一，以及陸委會和移民署等針對外來移民準備採取類似的措施，針對生物特徵身分辨識技術的運用，在規範、政策和社會等層面可能引發的效應和影響，進行徹底的討論和辯論，應該已是刻不容緩的社會工程之一。

壹、生物特徵身分辨識科技發展趨勢潛藏的意義

生物特徵身分辨識技術，其精確度究竟有多高，安全性又是如何，同等科技水準的生物特徵身分辨識技術，在遇上不同的社會脈絡和不同的政府資訊安全防護文化時，究竟是否適合特定社會或政府立即採納，做爲身分辨識制度中所仰賴的主要工具，似乎應該是個可以受到質疑和討論的議題。

尤其，當絕大部分的民眾並不清楚政府即將全面核發晶片護照一事的詳細內容，對於何種技術將被運用於晶片護照內也所知不多的情況下，晶片護照內所使用的技術，例如 RFID 及生物特徵身分辨識技術，會使個人的資訊隱私權減損到何種程度，更是一個應該被公開討論、徹底辯論的議題。更重要的是，政府有義務使其公民充分知悉和理解這樣一個有可能會影響其憲法所保障

的公民自由權及內在自由的政府科技使用的發展趨勢。

貳、生物特徵身分辨識科技運用於公部門所涉及的規範問題

台灣一般大眾和所有對科技不熟悉的社會大眾一樣，對於所謂的生物特徵身分辨識科技，多半處於並未深入瞭解的階段，遑論對於利用生物特徵辨識科技做爲工私部門的身分辨識機制此一重大公共政策，在正反資訊和意見都充分提供的前提下，在理解生物特徵身分辨識機制所涉及的各種風險的前提下，做過任何廣泛且深入的討論，形成政策層面的共識。同時，即使生物特徵身分辨識機制是所謂的「重要國際潮流」之一，是和國際民航組織要求進行「國際接軌」的重要手段之一，相關立法措施是否合憲且合宜，政府各部門在安全性保障和隱私保護等各方面的周邊制度，是否適時建立，而且運作良好，也都是必須細究到底的潛在爭議。這些潛在爭議，不應該僅僅止於針對移民相關法令和護照條例等相關規定進行形式上的增補修正，取得形式上的法律授權爲已足，而是應該正視立法蒐集人民生物特徵資訊此種作法的正當性，以及正視其所帶來的規範意涵。

以英國生物辨識議題爲例，雖然不乏立法授權蒐集人民生物特徵資訊甚且製成身分證件的相關討論，然而，其間所涉及的根本辯論，卻始終才是最受矚目的焦點，形式的立法本身，卻不見得是最受關注的重點。

就身分證法案而言，其基於方便驗證個人身分之立法目的，可就十六歲以上並屬於英國國民之人取得生物資料，該資料內容包括面部、指紋、虹膜及其他生物特徵等。其將經由身分證或其他指定證件如護照的發放，取得該人生物資訊。身分證持有人，

負有義務在其規定的範圍之內，對其個人資訊有所更動或本身已知的錯誤必須在法定期間內通知註冊中心，並當持卡人發現身分證被偷、遺失、遭竄改、毀損的情形時，必須通知註冊中心或其他法定人員，且該身分證則將被取消。而註冊單位以及發放選定證件部門，可基於確定其將要註冊或已註冊的資訊是否正確之目的，交換其所儲存之資訊。國務卿亦可在當事人同意的情況下，提供他人註冊中心的相關資料。另國安及情報機關、警察首長、稅務管理局等單位，在符合該機關目的的情形之下，亦將可取得相關個人資訊。且設立國家身分計劃委員（National Identity Scheme Commissioner），監督身分證計畫及註冊中心就身分證的應用及對登記資訊的提供。

就移民及難民法部分，定爲查明護照或相關證件的真實性，實行該項查核之人可請求被檢查之人提供外部特徵資料，諸如指紋、虹膜、或其他眼睛部位特徵等。而警官、出入境官員、監獄長官等人對抵達英國國境時，無法提出有效的證件之人、或拒絕入境但例外留置之人、或請求政治庇護者等可在相關時間內取其指紋。取得生物資料的方式則爲書面通知後，由該人提供指紋，或由警察機關在無逮捕令的情況下予以逮捕，強制取得該人指紋。且該指紋必須在一定期間內被銷毀。

另就反恐怖主以法及相關刑事立法部份，司法警察對於定罪、起訴、警告或其他有合理理由認爲其涉入犯罪之人，在未經其同意的情況下採取其指紋。亦可對依該法羈押之人經警察督察長以上層級之授權，採取指紋以確定其是否從事恐怖犯罪，或者教唆、幫助或煽動該類犯罪。在採取指紋之前，必須告知該指紋採取之目的，以及採取指紋之處所等。在強制採取指紋的部份，亦應告訴其授權採取情形、依據理由、所涉犯罪等。爲辨認身分所採取的指紋，無論當事人後來被証明有罪或無罪，皆可保存，但其使用之目的必須與預防或調查、偵查犯罪、進行起訴等目的

相關。

雖有上述相關立法，但目前英國就生物辨識的相關討論，多集中於身分證法案部分所牽涉的生物特徵資訊取得問題。首先，侵害隱私權而取得生物資料需符合特定公共利益爲前提，但在身分證法案當中所提出的公共利益諸如防止犯罪、減少不法工作、身分欺詐等公共利益，皆未能被證實可經由身分證之實行而達成。其次，由於蒐集個人生物資料將有侵犯隱私權的問題，故其是否符合歐洲人權公約第八條的要求，在公共利益的要求下以符合比例原則的權衡標準，非過度的干涉個人權利即爲重點。故在此諸如大型資料庫的設立、諸多資料的蒐集等是否違反比例原則，則爲考慮重點。另由於強制取得身分證將爲階段性的實施，則在此是否會違反歐洲人權公約第十四條禁止差別待遇的規定，亦有疑問。第三，就資料庫的管理部分，涉及資料保護的問題，從資料的取得、內容、管理等皆須小心討論實施，尤其在資料的揭露部分，對生物資料此種敏感資料的使用揭露規定，是否已臻完善，目前在現行英國身分證法當中將有許多機關可在模糊的定義下取得資料的情況下，恐尚有進步空間。最後，就生物特徵身分辨識技術而言，由於該技術尚在發展當中，其可能會造成的錯誤該如何解決，其技術該限制在怎樣的程度才不會過度蒐集資料而違反比例原則等，皆爲問題所在。以上英國經驗，或許不無目前準備以形式上的立法來處理規範層面問題的我國，值得借鏡之處。

再就亞洲地區的國家來說，亞洲地區雖然不乏已經開始實施生物特徵身分辨識制度和內建生物特徵身分辨識資訊的晶片護照者，但是，最近出現在菲律賓的一個法院判決，卻對司法權介入國家採行生物特徵身分辨識制度的可能性，多少帶來某些啓示，其後續發展值得我們持續觀察。

菲律賓 A PASIG City 地方法院，在今年年初對該國外交部(DFA, the Department of Foreign Affairs)的晶片護照計畫，發布一項定暫時狀態假處分(preliminary injunction)，命令暫緩該國晶片護照計畫之實施。詳言之，該地方法院法官 Franco Falcon，「撤銷」了 DFA 與(the Bangko Sentral ng Pilipinas,Central Bank of the Philippines)之間的契約，判決之前被 DFA 解除 BOT 契約的 BCA International Corp 勝訴，該 BOT 契約是雙方在在 2001 年 2 月簽訂，亦即該項計畫始於 2001 年，而於 2005 年因爲政府與承包商之間發生契約爭議而暫時中止。

此一爭議進入訴訟程序後，Falcon 法官在訂暫時狀態假處分後，隨即發布了暫時禁制令，暫停護照計畫繼續執行。最近 DFA 抗辯認爲地方法院不得針對國家層級的重大施政計畫，例如晶片護照計畫發布禁制令，然而，菲律賓司法院秘書長 Raul M. Gonzalez 卻發表聲明支持地方法院的決定。

如前所述，德國反國際恐怖主義法關於生物辨識特徵在身分制度的運用之規範目的乃以列舉的方式形成所謂的嚴格的目的拘束〈Zweckbindung〉。而這亦與我國釋字六〇三號解釋，大法官之解釋意旨不謀而合。在釋字六〇三號解釋認爲，資訊隱私權爲不可或缺之基本權，受憲法第二十二條之保障，雖然憲法對隱私權之保障並非絕對，惟當法律對隱私權作出干預與侵犯時，必須符合憲法第二十三條之比例原則。也就是符合目的合憲性、手段適當性、手段必要性以及狹義比例原則。而本號解釋，大法官認爲戶籍法關於按奈指紋，否不予核發身份證之規定，首先目的不明確，就算縱用以達到國民身分證之防僞、防止冒領、冒用、辨識路倒病人、迷途失智者、無名屍體等目的而言，亦屬損益失衡、手段過當，不符比例原則之要求。[210]因此宣告戶籍法第八條二、

[210] 可參釋字六〇三號解釋文：「指紋乃重要之個人資訊，個人對其指紋資訊之自

三項違憲。就以目的合憲性而言，由於指紋涉及個人之隱私權，爲人格發展不可或缺之基本權，且亦涉及到此項隱私的資料如何用、如何管理以及是否會外洩等問題。因此若僅單單以按奈指紋換發身份證可達到辨識、冒用、預防犯罪等目的上，則不符目的之合憲性。因此大法官在此採取最嚴格之審查，而這與德國反恐法關於生物特徵辨識特徵在身份制度的運用之規範目的以列舉的方式形成所謂的嚴格的目的拘束不謀而合，道理即在此。

而在應採取嚴格的目的拘束有共識後，若臺灣未來希望建立一套生物特徵之資料庫，或是爲了防止恐怖份子而採用電子護照時，首先在立法背景以致法律規範目的上，亦應如同德國反恐法之規範目的，採取最嚴格之目的拘束，亦如同美國三重審查之嚴格審查要求目的必須與公益有重大之關係，才能採取侵犯人民隱私權之方式，去建立一套生物資料庫或是利用生物特徵作爲能入出境之方式。再者，釋字六〇三號解釋亦提及個人資料的管理方式。因爲若有正當之目的，惟沒有一套管理方式，將會導致資料被濫用，此亦與人權之保障有所違背。而在德國有所謂之資訊監察官，除了避免生物特徵遭外洩外，亦爲個人之隱私權提供了一套保護方式。而臺灣未來應可參考德國之立法例，成立維護生物特徵之資訊監察官，以防止生物特徵之濫用。

主控制，受資訊隱私權之保障。而國民身分證發給與否，則直接影響人民基本權利之行使。戶籍法第八條第二項規定：依前項請領國民身分證，應捺指紋並錄存。但未滿十四歲請領者，不予捺指紋，俟年滿十四歲時，應補捺指紋並錄存。第三項規定：請領國民身分證，不依前項規定捺指紋者，不予發給。

對於未依規定捺指紋者，拒絕發給國民身分證，形同強制按捺並錄存指紋，以作爲核發國民身分證之要件，其目的爲何，戶籍法未設明文規定，於憲法保障人民資訊隱私權之意旨已有未合。縱用以達到國民身分證之防僞、防止冒領、冒用、辨識路倒病人、迷途失智者、無名屍體等目的而言，亦屬損益失衡、手段過當，不符比例原則之要求。戶籍法第八條第二項、第三項強制人民按捺指紋並予錄存否則不予發給國民身分證之規定，與憲法第二十二條、第二十三條規定之意旨不符，應自本解釋公布之日起不再適用。」

參、生物特徵身分辨識科技運用涉及的風險爭議和社會辯論

如前所述，生物辨識身分制度所引發的社會風險具有多樣化、難預測的特性，不能一味倒向唯科學化、實證主義的生產的邏輯。這套生產的邏輯是以線性因果的思維認爲生物辨識的科技系統爲可控制性(可確實保密、儲存)、可彌補性(爲了治安犧牲一點人權也是值得)、與可回復性(即使資料外洩名譽仍可回復)。然而，由於生物辨識系統涉及龐大的資訊儲存、辨識、利用、流通與管理，在任何一個環節皆有高度的不確定性，並且一旦外洩所引發的風險後果是目前難估計，因此，建議需謹慎評估，並以其他方式來取代運用，並進行替代性的風險評估(alternative assessment)，而非僅以本生物辨識科技系統爲唯一的風險評估標的，以免產生政策上一去不返的滑坡效應，換言之，科學風險評估與政府與人民間的風險溝通，皆不可偏廢。

然而，而台灣在地民眾常無知的忽視生物辨識身分制度將構成風險的潛在嚴重性與不可欲的後果，如隱私權被侵犯、政治上形成警察國家、國家至上的風險、社會上階級汙名化、倫理的風險，以及資訊管理上被冒用、被洩露的風險。究其原因，乃一般民眾對於風險之認知，容易受到資訊流通、媒體報導之影響，形成瀑布效應(cascade effect)，或是對大災難特別有恐懼感，或僅基於過去之經驗或情感式的影響，以及直覺式的損益分析，這種直覺式的損益分析，對於是否應該對某種風險加以管制，有時只看到利益面，而低估危險面，故在媒體造成的知溝(knowledge gap)差距下，公眾對於治安風險的未來性較清晰，反對於生物辨識技術的風險較爲模糊，因而在利益與風險分析上傾向於利益面考量，這同時意味著公眾並沒有充分、良好的告知或學習判斷，對於隱私權、資料外洩、科技風險仍處於有待自我啓蒙的社會階段

中。

尤其，民眾的風險感知也跟科學技術官僚散佈的資料證據息息相關，因爲經由二手傳播之非經驗所形成的公眾風險意識，事實上也必須從科學風險評估或決策者傳遞的資料訊息引證。而我國的技術官僚，長期以來習慣由上往下、威權式的、線性因果的實證確定性來推動各種科學計畫，以簡單化約、工具性的現代化、單面利益論述建構生物辨識系統的好處，而這些端倪也反映在移民署通關辨識與外交部的晶片護照上。

其實現行爭議性科技所衝擊的領域已逾越了既有的社會、法律、倫理的界限，傳統自然科學風險評估方式雖能夠提供一定的解決功能，但對於爭議性科技所引起在不同社會領域的衝擊與不確定性並無法提供答案，而這個部分所要進行開放式的社會風險評估，關鍵正在於公眾對於爭議性科技風險的理解與認知。不同的風險感知和溝通可成爲強化分析階段的來源，但不是一次就讓政策決定，應要調停不同的感知進入單一政策中，以便處理安全和偶發事件。新科技總是改變社會環境，帶來和引進新風險，而一連串的研究建議以漸進的努力去順應科技的利益與緩和科技帶來的缺點，安全管理者必須抓到科技、政策和行爲三位一體的概念。

就以晶片護照、生物辨識系統而言，我們看到，在不同場合中相關管制機構的官員一再追隨與強調主流科學的辨識率效果，以及多少國家已採用的趨勢，在此論點下，單一的科學評估就成爲決策的唯一檢正標準，並難以接受其它科學異議的聲音。換言之，在狹隘性之科學實證性的風險評估哲學下，技術官僚憑藉著獨大的專家政治立場，壟斷性地排除社會、倫理風險，而相對性的認定科學爲唯一評估與溝通的基礎。因此，風險溝通變成單面向的、教育的、扭正社會「情感的或不理性的感知」。

其實國外在試驗實施晶片護照及生物辨識系統相關設施後，出現許多問題，除了新儀器辨識率容易出錯外、仍存有諸多社會、倫理、法律、政治、經濟面向的疑慮，如生物特徵辨識科技費用昂貴，新護照的高成本必定轉嫁消費者，英國政府就因核新型生物護照後，因維護科技設備成本居高不下，迫使英國成人護照連漲三成，飆上每本護照新台幣四千元，引發民眾怨聲不斷。故若外交部、移民署仍然要強制辦理，是把國人當成白老鼠，如今新護照屆時能否趕上法律修正腳步、是否適用國內相關仍是疑問，然而巨額資金業已準備付出。

此外若以高科技需要高思維相應之風險社會公民理性溝通、批判能力之觀點，來檢視台灣民眾對生物辨識技術、晶片護照反應，不得不指出我國全球在地化風險該加油的地方，包括主管官署的不負責任，置民眾於資訊無知的狀態；但相對的我國公民社會仍相當脆弱，對應於此種全球性的高科技風險社會並無法建立監督、溝通並理性批判政府的行動，而這也是台灣欲發展人文高科技島的一項重要警訊與隱憂，更是我們值得共同努力的地方。

各國經常以立法來延宕科技風險的可能性，但在美國的生物辨識技術發展霸權與競爭放任之下，所有的社會風險的門檻紛紛失守。外交部、移民署等晶片護照與生物辨識機器的購買，類此涉及人民重大權利、義務的事項，政府應慎思明辨、決策應保守而謹慎，實不宜在未經國會充分討論、生物辨識科技法源尚在未定之天、及有公民審議程序、聽證程序、公民諮詢與公民會議等公共討論，經過多次且多元廣泛的風險溝通後，達到社會共識時，就動輒撒下龐大資金，讓備受爭議的新制上路，這樣的決策未免過於草率，欠缺謀定而後動的智慧，萬一生物辨識技術有違憲的爭議，在立法程序無法過關，那麼購置的設備豈不是浪費公帑？故從本旨研究建議，不應該在反恐的大論述底下，就冒然實施生物辨識技術、晶片護照等政策，否則將產生風險不可回復的後果。

其次，生物特徵身分辨識科技的應用和晶片護照的出現，無非是國家理性主導一切的近代社會的典型面貌。然而，思考這種監控社會統治體制下的 social sorting（社會性分類）將帶來何種風險，卻是值得目前積極考量採行這些措施做爲政府重大施政計畫的我國政府深入理解的。再以英國爲例，目前英國生物辨識技術的應用，藉著身分證法案的推行，已逐漸展開，未來將於二○○八年對英國境內的外籍人士全面發放身分證件，並隨後於二○○九年英國國民於申請護照時可同時申請身分證件，但到了二○一○年每位申請護照之英國國民皆會強制同時發放身分證件。但在政府不斷保證該計畫爲切合時代潮流且能提升公共安全的同時，諸多反對質疑意見仍然不斷，其對於隱私權及相關人權可能產生的侵害、可能發展爲監控國家的疑慮、甚至在技術上是否能真正實行、是否會造成花費龐大但效用不彰的情況等，皆造成英國社會，甚至政府官員、國會成員對於此項生物技術應用持保留態度。雖然目前英國政府在生物應用上似乎已爲勢所必然，但現實上其反對的呼聲不斷，反對黨甚至明確表示一旦於下次大選勝利即會停止該身分證計畫的推行，目前英國這樣的道路是走向國家安全提升的康莊大道，或者走向監控社會隱私受限的警察國家，恐怕仍是未知之數。

最後，以反恐主導者美國爲例，在 911 恐怖攻擊事件後，爲了讓美國公民確信美國政府正盡力採取所有可能的方法，確保美國人民的安全，國土安全部（Department of Homeland Security，簡稱 DHS）與國務院（State Department）緊密合作，對通過邊境的旅客進行更爲嚴密的查驗。此外，在 911 恐怖攻擊事件後，美國政府蒐集個人資訊的誘因也大爲增加，其中包括生物特徵資訊在內，因爲此等資料有助於追蹤恐怖份子，同時可對航空旅客進行更爲透徹的側寫（profile）。爲了便利旅行及協助邊境執法人員判斷文件的有效性，美國政府要求所有與美國相互享有免簽證入

境的國家（VWP countries），應該發展一套更安全的晶片護照系統，而負責核發美國護照的美國國務院，也基於互惠原則，發行晶片護照。

美國的晶片護照除了涵蓋 1998 年版護照（Passport '98）既有的資訊外，同時包含以數位相片方式展現的生物辨識碼（biometric identifier）。護照的封底還嵌入一個 RFID 晶片。值得我們思考的問題是：發行晶片護照的政策，到底隱含哪些我們應該正視的風險和社會辯論？

晶片護照是一份將由各個外國、各個國外旅館及全世界各個機場所共同分享與檢閱的文件。而晶片護照所使用的 RFID 技術，其實就是一種廣泛運用於各個賣場、倉庫以追蹤商品、貨物流向的技術，此技術也用於賽跑中以追蹤跑者，同時也被運用於追蹤動物或孩童的位置，以避免走失。生物特徵辨識技術最常見的則用於犯罪活動的辨識，例如指紋資料庫。當這些技術基於政府的要求而被用於一套全國性的身分辨識系統時，持有護照的一般公眾，其實恩本失去了選擇他們想要持有何種護照的權利，他們變成只能選擇要或不要持新的晶片護照於美國以外的地域旅行。而晶片護照則很可能會成爲追蹤公民穿越各國機場及跨越各國邊境的工具。這是一種喬治歐維爾式的憂慮：公民將會無時無刻地受到來自於國家的監視與追蹤。

雖然憲法所保障的隱私權、財產權和旅行權等並非絕對的權利，然而，晶片護照的發行及使用，所涉及根本的價值問題很可能在於：我們的社會把守法的公民都視爲潛在的恐怖份子，但卻未盡力地有效保護他們免於受到真正的威脅。同時，在適當安全防護措施尚未到位的情形下就發行晶片護照，很可能會對一般人科技警覺性不高的人，帶來一場科技上的災難。尤其，當護照上的資訊在每次被讀取時，都必須先下載到資料庫內，但政府卻無

法保護外國政府資料庫內的我國公民的資訊時，也無從如歐盟的隱私權保護指令爲跨國的個人資料流動提供一套比較有效的管制架構時，持有晶片護照的人民，能夠受到何種程度的資訊隱私保障，其實是很值得懷疑的。

晶片護照的另一個主要弱點，不在於生物特徵身分辨識科技本身，而是在於可以接近使用晶片護照資訊的人。護照的核發審核者、邊境管制人員、執法單位及私人單位將會有管道接近這些個人資訊。相關的管制及防護措施應該要到位，才能確保護照的核發機關不致於在發照時就出錯，或是將護照發給潛在的恐怖份子，或是忽略了身分冒用者使用有效的文件來蒙混過關。此等弱點並不是新出現的，他們原本就存在，但若邊境管制人員及執法部門在決定一個人的真實身分時，過份仰賴科技，將會抓不到身分冒用者。相關的執法人員應該接受訓練，才能學會不要單純依靠電腦系統來決定文件的是否有效及進行身分辨識。護照的核發審核者在時間的壓力下，仍需要花更多的時間來挑出可能涉及身分僞造的因素，否則護照可能會錯誤地核發。如果要避免安全且有效的文件被發給恐怖份子，例如九一一事件中發給劫機者十九份美國簽證的問題，就必須要求相關執法者不全然仰賴科技來追求準確性，才能解決。

或許，究其實際，晶片護照從一開始就是一種無法避免人民遭受未來的恐怖攻擊的脆弱文件。或許九一一事件爲世人帶來的震撼程度，促使各國政府迅速且不理性地採取各種極端的行動，晶片護照的推出，或許便是在這種歷史潮流下的產物。我們或許應該回到生物特徵身分辨識機制的根本面，思考一下晶片護照是不是根本便是一場巨大而無聲的滑坡效應的開端而已？不久的將來，各種政府是不是會把生物特徵身分辨識技術和 RFID 技術運用於駕照和國民身分證件上呢？在那一天來到之前，我們做過資訊充分而徹底的辯論了嗎？理解了生物特徵身分辨識技術及其相

關配套技術的倫理、規範和社會意涵了嗎？

肆、從生物特徵身分辨識的效益取向談未來規劃原則

國際上目前對生物辨識身分制度的實施輿論不一，參照國外討論生物辨識技術的主流意見，國際上對生物辨識系統有以下幾點建議事項可供借鑑:

一、 應採非侵入性採證方式，直覺式互動:爲改善生物測定使用者對科技不熟悉的缺點，建議使用者互動必須可直覺式的(intuitive)或縮小至點，也就是與裝置少或無互動，比方虹膜辨識可允許虹膜形象在個體行進，通過感應器時被捕捉[211]。

二、 改善生物統計學研究的方式:（一）藉同儕審查程序促進審查政策的和諧;（二）提供獲取大量數據組和不同類型的數據，如多模數據(multimodal data)，來衡量實施的改善，並發掘增加數據的方法，將之使用在生物測定研究;（三）開發挑戰性的問題來指引學術研究,和創造比較和獨立評估的;（四）基線增加管制機關資助和申請研究的文件。(the documentation of government－funded and －proposed research)[212]

三、 教育訓練與心理建設：在機構的控制環境中，安全策略如同發展的基石，而這需透過對員工的教育和覺醒的計畫，否則爲承擔安全所創造的策略工作，最後都只是浪費時間，而

---

[211] Kristen Batch, Lynette I. Millett, Joseph N.Pato, Editors，〈Summary of a Workshop on the Technology, Policy, and Cultural Dimensions of Biometric systems〉，p6－7，2005

[212] 參考 Kristen Batch, Lynette I. Millett, Joseph N.Pato, Editors，〈Summary of a Workshop on the Technology, Policy, and Cultural Dimensions of Biometric systems〉，表 2-1，2005

這可讓民眾對此感到安心，以提昇生物辨識身分制度的進行。訓練對系統操作是有用的，有助了解系統操作，但當系統是以直覺式(intuitive)時，對使用者而言，訓練是不需要的，對使用者訓練可能會造成對科技恐懼厭惡的反效果。此外身分管理與技術對大多數的人們而言能是一項新觀念，因此組織需要進一步地教育和告知民眾，關於身分管理方法的使用將有可能使他們更安全及在日常生活中提供更大的便利[213]。

四、 合作與跨科際的研究：合作與跨科際的研究(cross─disciplinary research)是需要的。如果新的犯罪預防方法被這樣的研究和被這樣的方法補充，如管制單位與學界合作，將使人們有更能意識何時該或不該信任生物辨識技術，而這對新的犯罪預防將能更有幫助[214]。一個嚴格的資料保護規則不只是爲了法律執行的原因，也是呈現現今經濟價值和成爲管制機關與企業 ICT(information and communication technologies)風險降低的基本成分。而預防資料外洩的作爲，包括在資訊安全上雇用一個特別的顧問、增加安全和隱私的訓練、檢閱敏感性資料的路徑與儲存，以上才是一個有效的隱私政策[215]。

以反對憂心風險者立場來看，生物辨識系統目前必須考量的問題還包括:一、錯誤排斥率： 有些人可能會面臨電腦錯誤的將他們阻擋在辦公室之外的困擾。 二、健康考量： 有些人會對生

---

[213] Roberto TAVANO、Pr. Juliet Lodge、Ronald Huijgens、Kamini Aisola、Marc Flammang,《Biometrics in Europe》, European Biometrics Portal Trend Report 2006,June 2006 2.2.5

[214] 參考 Robin Mansell and Brian S. Collins,〈introduction〉,《Trust and crime in information societies》, p.6－7, 2005

[215] Roberto TAVANO、Pr. Juliet Lodge、Ronald Huijgens、Kamini Aisola、Marc Flammang,《Biometrics in Europe》, European Biometrics Portal Trend Report 2006,June 2006 4.5

物特徵的輸入技術或因爲接觸輸入裝置所可能帶來的交叉感染有所排斥。三、入口阻塞： 如果系統設計不良，員工排隊等候進入的情況就可能發生。四、繞道而過： 即使擁有了最安全的身分辨識系統，人員如果可以繞過關卡進入就會失去其效用。旋轉式或氣閘式入口，是必須要與生物辨識的門禁控制系統相鄰的[216]。

以上顯示，確實的風險評估與溝通不僅只有科學面，還包含社會、法律、文化等面向，因此對於此種爭議性科技於其所產生不確定性的問題，除了要進行多元領域之自然科學風險評估與溝通之外，也應進行開放性、社會科學式的風險評估。這裏所主張開放性、社會科學式的風險評估，著眼於除了依據傳統自然科學式的風險評估之外，當代許多高度爭議的科技問題，必須增加自然科學領域之外的評估，也就是說，當爭議性的科學發展已經逾越了傳統的解決問題範疇、界限，科學的衝擊除了自身安全的不確定性外，往往也衝擊到了現行法律、倫理、社會的基礎，因此，風險評估的範疇與定義必須開放性的納入有關對這些社會領域的評估，來增進科學發展的正當性[217]。

也就是在開放性風險評估典範下，對於科技爭議與不確定性部份的評估超越了單一領域自然科學式風險評估的限制，而在整體多元的評估過程中進行公共領域的學習、溝通與價值判斷，由社會公眾對科學爭議進行雙向式的理解與溝通判斷[218]，在多元領域與價值的思考、批判下，逐步建構出社會對於不同高科技風險爭議的處理能耐，而發

---

[216] 參閱:生物辨識認證卡解決方案，IDEethod，
http://www.idmethod.com/s_biocard.html，參訪日期 2007/01//27

[217]周桂田，爭議性之風險溝通-以基因改造工程爲思考點，生物科技與法律研究通訊，第十八期，頁 48

[218] 以臺灣目前在法律上仍然無法規範的基因螢光魚，雖然業者已號稱其在觀賞魚市場有相當到了潛力，但若消費者相當充份地得知其可能對於生態有一定程度的衝擊之後，例如不可輕易的將此觀賞基因螢光魚野放到河川之中，透過社會同時對此類科技爭議的理解與學習，反而能夠形成一道預防性的措施。

展出整體風險評估的治理策略[219]。

伍、具體建議

基於本研究以上各章論述和研究所得，本章將提出以下幾點經過歸納以後的具體看法，並且區分「立即可行建議」和「中長期建議」兩者，並分別說明本研究所建議之主辦機關及協辦機關，釐清目前我國政府部門在面對「運用生物特徵辨識身份」此一議題時，應該採行的態度和措施，做爲本研究之具體結論。

首先，在「立即可行建議」方面，我們的結論和建議如下：

一、密切觀察國際民航組織相關規範的發展方向，並釐清其規範內容，避免以「國際趨勢」和「科技正面效益」此等過度簡化的說詞，當做發展生物特徵身份辨識系統和採行晶片護照的藉口。

主辦機關：外交部。

協辦機關：研考會。

二、遵循「行政程序法」和「政府資訊公開法」之相關規定，主動公布政府各相關部會關於採行生物特徵身份辨識措施（包括臉部特徵在內）此一政策之規劃過程、目前確定措施和未來後續發展方向等等相關資訊，以便公眾可以根據充分的資訊，判斷政府

[219] 周桂田，爭議性之風險溝通-以基因改造工程爲思考點，生物科技與法律研究通訊，第十八期，頁 48.

相關措施之內涵爲何，以及其是否合乎成本效益考量，以及是否有侵犯本國人民、外國人和移民之基本人權之虞。並且促成社會大眾對於生物特徵身份辨識措施的廣泛辯論。

主辦機關：外交部、內政部、陸委會。

協辦機關：研考會。

三、重新檢討送立法院審議中之護照條例修正草案、入出國及移民法、兩岸人民關係條例內和生物特徵身份辨識科技有關之規定內容，針對任何生物特徵身份辨識措施（包括臉部特徵在內）之採行，應先確定該等措施具有充分的法律授權，足以嚴密控制行政機關蒐集個人生物特徵資訊之行爲。除形式上之合法性之外，並應審慎評估此等措施和立法內容之合憲性。

主辦機關：外交部、內政部、陸委會。

協辦機關：研考會、法務部。

其次，在「中長期建議」方面，則可以區分成以下幾點：

一、儘速推動通過「個人資料保護法」，以建立個人生物特徵資訊蒐集行爲之最高規範原則。

主辦機關：法務部。

協辦機關：研考會。

二、有鑑於生物特徵之蒐集現象愈加普遍，範圍和種類亦逐漸擴大和增多，針對生物特徵資訊之蒐集，應推動訂定專法，以爲規

範依據。

主辦機關：法務部。

協辦機關：研考會。

三、有鑑於國人對於生物特徵此種個人資訊之敏感性相當陌生，而個人資訊保護相關規定又頗爲簡陋，政府應該避免以科技至上、效率第一的心態看待生物特徵身份辨識資訊的應用，一味向人民宣導甚或強調生物特徵身份辨識系統的重要性和可靠性。相對地，政府應該採取衡平作法，積極推動普及性的「隱私權保護」和「科技風險意識」教育，以利公民社會對於此一重要議題的理解和辯論。

主辦機關：研考會。

協辦機關：法務部、外交部、內政部、陸委會。

附錄一

德國反國際恐怖主義法（Gesetz zur Bekämpfung der internationalen Terrorismus）之介紹

一、第一條至第二十條之內容採取「包裹立法」（Gesetzgebungspaket）之立法形式，其中每一條皆分別代表了對個別不同法律（Gesetz）或法規命令（Verordnung）之修正：第一條是聯邦憲法保護法（Bundesverfassungsschutzgesetz）之修正、第二條是軍事反間諜局（MAD-Gesetz）法之修正、第三條是聯邦情報局法（BND-Gesetz）之修正、第四條是第十條法（Artikel 10-Gesetz）之修正、第五條是安全檢查法（Sicherheitsüberprüfungsgesetz）之修正、第六條是聯邦邊防法（Bundesgrenzschutzgesetz）之修正、第七條是護照法（Passgesetz）之修正、第八條是身份證法（Gesetz über Personalausweise）之修正、第九條是社團法（Vereinsgesetz）之修正、第十條是聯邦刑事局法（Bundeskriminalamtgesetz）之修正、第十一條是外國人法（Ausländergesetz）之修正、第十二條是避難程序法（Asylverfahrensgesetz）之修正、第十三條是外國人集中登記法（Gesetz über das Ausländerzentralregister）之修正、第十四條是外國人法施行細則（Verordnung zur Durchführung des Ausländergesetzes）之修正、第十五條是外國人檔案規則（Ausländerdateienverordnung）、第十六條是外國人集中登記法施行細則（AZRG-Durchführungsverordnung）之修正、第十七

條是聯邦集中登記法（Bundeszentralregistergesetz）之修正、第十八條是第十部社會法典（Zehntes Buch Sozialgesetzbuch）之修正、第十九條是航空交通法（Luftverkehrsgesetz）之修正、第十九條是航空交通安全檢查規則（Luftverkehr-Zuverlässigkeitsüberprüfungsverordnung）之修正、第二十條是一九七五年能源安全法（Energiesicherungsgesetz 1975）及電力分擔規則（Elektrizitätslastverteilungs-Verordnung）、天然氣分擔規則（Gaslastverteilungs-Verordnung）等法規命令之修正。

二、若以比喻的方式來說，此種立法形式彷彿爲網路中之超連結（Hyperlink），於一個網頁上可經點選而連結至其他許多相關網頁，相當便利，與我國若欲爲特定目的修正多數法律時，乃由同一部會或不同部會於同時提出多數修正草案，而立法院儘量於同一立法會期一併審查通過的做法不同。較諸我國之立法形式，此種包裹立法之優點在於，其經通盤協調，能一目瞭然地宣示出國家整體之立法動向及政策目標，且能避免在分散立法時可能產生之規範欠缺、規範矛盾、生效時點前後不同等不當情形。惟「包裹立法」之成功，須以精密之立法技術及深厚之法律素養作爲前提，並非我國在目前條件下可予以速成者。

三、本法第二十一條規定基於本法中各相關條文被修正之法規命令，得依據個案中之授權經由法規命令之形式被修正，以回復統一之命令位階。第二十二條雖規定本法從二○○二年一月一日起生效，卻亦規定其中所修正之部分法律從二○○七年一月十一日起回復爲二○○一年十二月三十一日之規範內容，且於有效期間屆滿前應對新規定加以評估。從上述兩規定可知，本法帶有

濃厚之著眼於特定目的或因應特殊時空環境的「限時法」性質，故不僅在形式上對部分法律預訂其有效期間，且即使在有效施行期間內，亦要求應實質評估修正後之法律或法規命令在因應特殊情勢或需要上之適當與否，以適時作內容上之調整，或回復原來之法秩序。鑒於各該新規定較諸修正前乃高度干預人民之各項基本權利，並非法治國之常態，實爲反恐制暴之目的所不得不然也，上述形式及實質之「限時法」性質，當可稍減本法之嚴峻效果所帶來的負面效應，亦差可謂符合比例原則之誡命。

四、本法具有通盤協調整合之性質，已如前述。其整合之情形可分爲三個面向加以討論：（一）聯邦各機關間之水平整合，例如國防、財政、內政、外交、經濟等各個主管機關間職權之整合；（二）聯邦與各邦間之垂直整合，例如本法第二十條爲一九七五年能源安全法及電力分擔規則、天然氣分擔規則等法規命令之修正部分，即涉及各邦之分配區域；（三）不同位階規範間之整合，此指法律之上位規範與法規命令之下位規範間之整合，以具體落實相關政策，達成反恐之目的。上述三個整合面向顯示出，本法乃一巨細靡遺且涵蓋各個層面之規範整體，雖有多處尚須於個案中予以精緻化，仍提供了一套可供實務操作之基準，而非只是口號性聊備一格之法律，此種儘量明確化相關規定，使人民得以預見，實務亦得據以實踐的做法，亦符合法治國原則及比例原則之要求，避免因規範模糊曖昧而各憑己意恣意適用，使本法成爲一部充滿不安定性、以暴制暴、失去理性的野蠻惡法。

附錄二

Wesentliche bestehende Rechtsgrundlagen zu dieser Thematik lassen sich den folgenden Gesetzen entnehmen:

- **Gesetz zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz TerrorBekämpfG):**

Artikel 7 Änderung des Passgesetzes

Das Passgesetz vom 19. April 1986 (BGBl. I S. 537), zuletzt geändert durch Artikel 1 des Gesetzes vom 1. Mai 2000 (BGBl. I S. 626) sowie durch Artikel 25 des Gesetzes vom 3. Dezember 2001 (BGBl. I S. 3306), wird wie folgt geändert:

1. § 4 wird wie folgt geändert:

a) In Absatz 1 wird nach Satz 3 folgender Satz 4 eingefügt: „Dies gilt nicht, wenn der vorläufige Pass eine Zone für das automatische Lesen enthält.“

b) Nach Absatz 2 werden die folgenden Absätze 3 und 4 eingefügt:

„(3) Der Pass darf neben dem Lichtbild und der Unterschrift weitere biometrische Merkmale von Fingern oder Händen oder Gesicht des Passinhabers enthalten. Das Lichtbild, die Unterschrift und die weiteren biometrischen Merkmale dürfen auch in mit

Sicherheitsverfahren verschlüsselter Form in den Pass eingebracht werden. Auch die in Absatz 1 Satz 2 aufgeführten Angaben über die Person dürfen in mit Sicherheitsverfahren verschlüsselter Form in den Pass eingebracht werden.

(4) Die Arten der biometrischen Merkmale, ihre Einzelheiten und die Einbringung von Merkmalen und Angaben in verschlüsselter Form nach Absatz 3 sowie die Art ihrer Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung werden durch Bundesgesetz geregelt. Eine bundesweite Datei wird nicht eingerichtet.“

c) Die bisherigen Absätze 3 und 4 werden Absätze 5 und 6.

2. § 16 wird wie folgt geändert:

a) Absatz 1 Satz 1 wird gestrichen.

b) Nach Absatz 5 wird folgender Absatz 6 angefügt:

„(6) Im Pass enthaltene verschlüsselte Merkmale und Angaben dürfen nur zur Überprüfung der Echtheit des Dokumentes und zur Identitätsprüfung des Passinhabers ausgelesen und verwendet werden. Auf Verlangen hat die Passbehörde dem Passinhaber Auskunft über den Inhalt der verschlüsselten Merkmale und Angaben zu erteilen.“

Artikel 8 Änderung des Gesetzes über Personalausweise

Das Gesetz über Personalausweise in der Fassung der Bekanntmachung vom 21. April 1986 (BGBl. I S. 548), zuletzt geändert durch Artikel 25a des Gesetzes vom 3. Dezember 2001 (BGBl. I S. 3306), wird wie folgt geändert:

1. § 1 wird wie folgt geändert:

a) Nach Absatz 3 werden die folgenden Absätze 4 und 5 eingefügt:

„(4) Der Personalausweis darf neben dem Lichtbild und der Unterschrift auch weitere biometrische Merkmale von Fingern oder Händen oder Gesicht des Personalausweisinhabers enthalten. Das Lichtbild, die Unterschrift und die weiteren biometrischen Merkmale dürfen auch in mit Sicherheitsverfahren verschlüsselter Form in den Personalausweis eingebracht werden. Auch die in Absatz 2 Satz 2 aufgeführten Angaben über die Person dürfen in mit Sicherheitsverfahren verschlüsselter Form in den Personalausweis eingebracht werden.

(5) Die Arten der biometrischen Merkmale, ihre Einzelheiten und die Einbringung von Merkmalen und Angaben in verschlüsselter Form nach Absatz 4 sowie die Art ihrer Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung werden durch Bundesgesetz geregelt. Eine bundesweite Datei wird nicht eingerichtet.“

b) Die bisherigen Absätze 4 und 5 werden Absätze 6 und 7.

2. § 3 wird wie folgt geändert:

a) Absatz 1 Satz 1 wird aufgehoben.

b) Nach Absatz 4 wird folgender Absatz 5 angefügt:

„(5) Im Personalausweis enthaltene verschlüsselte Merkmale und Angaben dürfen nur zur Überprüfung der Echtheit des Dokumentes und zur Identitätsprüfung des Personalausweisinhabers ausgelesen und verwendet werden. Auf Verlangen hat die Personalausweisbehörde dem Personalausweisinhaber Auskunft über den Inhalt der verschlüsselten Merkmale und Angaben zu erteilen.“

Artikel 12 Änderung des Asylverfahrensgesetzes

Das Asylverfahrensgesetz in der Fassung der Bekanntmachung vom 27. Juli 1993 (BGBl. I S. 1361), zuletzt geändert durch Artikel 4 des Gesetzes vom 20. Dezember 2001 (BGBl. I S. 3987), wird wie folgt geändert:

1. § 16 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) In Satz 1 werden die Wörter „eine unbefristete Aufenthaltsgenehmigung besitzt oder“ gestrichen.

bb) Nach Satz 2 werden folgende Sätze angefügt:

„Zur Bestimmung des Herkunftsstaates oder der Herkunftsregion des Ausländers kann das gesprochene Wort außerhalb der förmlichen Anhörung des Ausländers auf Ton- oder Datenträger aufgezeichnet werden. Diese Erhebung darf nur erfolgen, wenn der Ausländer vorher darüber in Kenntnis gesetzt wurde. Die Sprachaufzeichnungen werden beim Bundesamt aufbewahrt."

b) In Absatz 2 werden die Wörter „erkennungsdienstliche Maßnahmen" durch die Wörter „die Maßnahmen nach Absatz 1" ersetzt.

c) In Absatz 4 Satz 1 wird nach der Angabe „Absatz 1" die Angabe „Satz 1 und 2" eingefügt.

d) Absatz 5 Satz 1 wird wie folgt gefasst:

„Die Verarbeitung und Nutzung der nach Absatz 1 gewonnenen Unterlagen ist auch zulässig zur Feststellung der Identität oder Zuordnung von Beweismitteln für Zwecke des Strafverfahrens oder zur Gefahrenabwehr."

e) Absatz 6 wird wie folgt gefasst:

„(6) Die nach Absatz 1 gewonnenen Unterlagen sind zehn Jahre nach unanfechtbarem Abschluss des Asylverfahrens zu vernichten. Die entsprechenden Daten sind zu löschen."

2. In § 63 wird nach Absatz 4 folgender Absatz 5 angefügt: „(5) Im Übrigen gilt § 56a des Ausländergesetzes entsprechend.“

d) Absatz 5 Satz 1 wird wie folgt gefasst:

„Die Verarbeitung und Nutzung der nach Absatz 1 gewonnenen Unterlagen ist auch zulässig zur Feststellung der Identität oder Zuordnung von Beweismitteln für Zwecke des Strafverfahrens oder zur Gefahrenabwehr.“

e) Absatz 6 wird wie folgt gefasst:

„(6) Die nach Absatz 1 gewonnenen Unterlagen sind zehn Jahre nach unanfechtbarem Abschluss des Asylverfahrens zu vernichten. Die entsprechenden Daten sind zu löschen.“

2. In § 63 wird nach Absatz 4 folgender Absatz 5 angefügt:

„(5) Im Übrigen gilt § 56a des Ausländergesetzes entsprechend.“

. Passgesetz (PassG)

§ 4 Passmuster

(3) Der Pass darf neben dem Lichtbild und der Unterschrift weitere biometrische Merkmale von Fingern oder Händen oder Gesicht des Passinhabers enthalten. Das Lichtbild, die Unterschrift und die weiteren biometrischen Merkmale dürfen auch in mit Sicherheitsverfahren verschlüsselter Form in den Pass eingebracht

werden. Auch die in Absatz 1 Satz 2 aufgeführten Angaben über die Person dürfen in mit Sicherheitsverfahren verschlüsselter Form in den Pass eingebracht werden.

(4) Die Arten der biometrischen Merkmale, ihre Einzelheiten und die Einbringung von Merkmalen und Angaben in verschlüsselter Form nach Absatz 3 sowie die Art ihrer Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung werden durch Bundesgesetz geregelt. Eine bundesweite Datei wird nicht eingerichtet.

- **Personalausweisgesetz (PAuswG)**

§ 1 Ausweispflicht

(4) Der Personalausweis darf neben dem Lichtbild und der Unterschrift auch weitere biometrische Merkmale von Fingern oder Händen oder Gesicht des Personalausweisinhabers enthalten. Das Lichtbild, die Unterschrift und die weiteren biometrischen Merkmale dürfen auch in mit Sicherheitsverfahren verschlüsselter Form in den Personalausweis eingebracht werden. Auch die in Absatz 2 Satz 2 aufgeführten Angaben über die Person dürfen in mit Sicherheitsverfahren verschlüsselter Form in den Personalausweis eingebracht werden.

(5) Die Arten der biometrischen Merkmale, ihre Einzelheiten und die Einbringung von Merkmalen und Angaben in verschlüsselter Form

nach Absatz 4 sowie die Art ihrer Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung werden durch Bundesgesetz geregelt. Eine bundesweite Datei wird nicht eingerichtet.

- **Asylverfahrensgesetz (AsylVfG)**

§ 16 Sicherung der Identität

(1) Die Identität eines Ausländers, der um Asyl nachsucht, ist durch erkennungsdienstliche Maßnahmen zu sichern, es sei denn, daß er noch nicht das 14. Lebensjahr vollendet hat. Nach Satz 1 dürfen nur Lichtbilder und Abdrucke aller zehn Finger aufgenommen werden. Zur Bestimmung des Herkunftsstaates oder der Herkunftsregion des Ausländers kann das gesprochene Wort außerhalb der förmlichen Anhörung des Ausländers auf Ton- oder Datenträger aufgezeichnet werden. Diese Erhebung darf nur erfolgen, wenn der Ausländer vorher darüber in Kenntnis gesetzt wurde. Die Sprachaufzeichnungen werden beim Bundesamt aufbewahrt.

(2) Zuständig für die Maßnahmen nach Absatz 1 sind das Bundesamt und, sofern der Ausländer dort um Asyl nachsucht, auch die in den §§ 18 und 19 bezeichneten Behörden sowie die Aufnahmeeinrichtung, bei der sich der Ausländer meldet.

(3) Das Bundeskriminalamt leistet Amtshilfe bei der Auswertung der nach Absatz 1 gewonnenen Fingerabdruckblätter zum Zwecke der

Identitätssicherung. Es darf hierfür auch von ihm zur Erfüllung seiner Aufgaben aufbewahrte erkennungsdienstliche Unterlagen verwenden. Das Bundeskriminalamt darf den in Absatz 2 bezeichneten Behörden den Grund der Aufbewahrung dieser Unterlagen nicht mitteilen, soweit dies nicht nach anderen Rechtsvorschriften zulässig ist.

(4) Die nach Absatz 1 Satz 1 und 2 gewonnenen Unterlagen werden vom Bundeskriminalamt getrennt von anderen erkennungsdienstlichen Unterlagen aufbewahrt und gesondert gekennzeichnet. Entsprechendes gilt für die Verarbeitung in Dateien.

(4a) Die nach Absatz 1 Satz 1 gewonnenen Daten dürfen zur Feststellung der Identität oder Staatsangehörigkeit des Ausländers an das Bundesverwaltungsamt übermittelt werden, um sie mit den Daten nach § 49b des Aufenthaltsgesetzes abzugleichen. § 89a des Aufenthaltsgesetzes findet entsprechende Anwendung.

(5) Die Verarbeitung und Nutzung der nach Absatz 1 gewonnenen Unterlagen ist auch zulässig zur Feststellung der Identität oder Zuordnung von Beweismitteln für Zwecke des Strafverfahrens oder zur Gefahrenabwehr. Die Unterlagen dürfen ferner für die Identifizierung unbekannter oder vermißter Personen verwendet werden.

(6) Die nach Absatz 1 gewonnenen Unterlagen sind zehn Jahre nach

unanfechtbarem Abschluss des Asylverfahrens zu vernichten. Die entsprechenden Daten sind zu löschen.

- **Aufenthaltsgesetz (AufenthG):**

§ 49 Feststellung und Sicherung der Identität

(1) Jeder Ausländer ist verpflichtet, gegenüber den mit dem Vollzug des Ausländerrechts betrauten Behörden auf Verlangen die erforderlichen Angaben zu seinem Alter, seiner Identität und Staatsangehörigkeit zu machen und die von der Vertretung des Staates, dessen Staatsangehörigkeit er besitzt oder vermutlich besitzt, geforderten und mit dem deutschen Recht in Einklang stehenden Erklärungen im Rahmen der Beschaffung von Heimreisedokumenten abzugeben.

(2) Bestehen Zweifel über die Person, das Lebensalter oder die Staatsangehörigkeit des Ausländers, so sind die zur Feststellung seiner Identität, seines Lebensalters oder seiner Staatsangehörigkeit erforderlichen Maßnahmen zu treffen, wenn

1. dem Ausländer die Einreise erlaubt oder ein Aufenthaltstitel erteilt

werden soll oder

2. es zur Durchführung anderer Maßnahmen nach diesem Gesetz erforderlich ist.

(2a) Die Identität eines Ausländers ist durch erkennungsdienstliche Maßnahmen zu sichern, wenn eine Verteilung gemäß § 15a stattfindet.

(3) Zur Feststellung und Sicherung der Identität sollen die erforderlichen Maßnahmen durchgeführt werden,

1. wenn der Ausländer mit einem gefälschten oder verfälschten Pass oder

Passersatz einreisen will oder eingereist ist;

2. wenn sonstige Anhaltspunkte den Verdacht begründen, dass der Ausländer

nach einer Zurückweisung oder Beendigung des Aufenthalts erneut unerlaubt ins Bundesgebiet einreisen will;

3. bei Ausländern, die vollziehbar ausreisepflichtig sind, sofern die Zurückschiebung oder Abschiebung in Betracht kommt;

4. wenn der Ausländer in einen in § 26a Abs. 2 des Asylverfahrensgesetzes genannten Drittstaat zurückgewiesen oder zurückgeschoben wird;

5. bei der Beantragung eines Visums für einen Aufenthalt von mehr als drei Monaten durch Staatsangehörige von Staaten, bei denen Rückführungsschwierigkeiten bestehen sowie in den nach § 73 Abs. 4 festgelegten Fällen;

6. bei der Gewährung von vorübergehendem Schutz nach § 24 sowie in den Fällen der §§ 23 und 29 Abs. 3;

7. wenn ein Versagungsgrund nach § 5 Abs. 4 festgestellt worden ist.

(4) Maßnahmen im Sinne der Absätze 2 bis 3 sind die Aufnahme von Lichtbildern und Fingerabdrücken sowie die Vornahme von Messungen und ähnlichen Maßnahmen. Diese sind zulässig bei Ausländern, die das 14. Lebensjahr vollendet haben. Zur Feststellung der Identität sind diese Maßnahmen nur zulässig, wenn die Identität in anderer Weise, insbesondere durch Anfragen bei anderen Behörden nicht oder nicht rechtzeitig oder nur unter erheblichen Schwierigkeiten festgestellt werden kann.

(5) Zur Bestimmung des Herkunftsstaates oder der Herkunftsregion des Ausländers kann das gesprochene Wort des Ausländers auf Ton- oder Datenträger aufgezeichnet werden. Diese Erhebung darf nur erfolgen, wenn der Ausländer vorher darüber in Kenntnis gesetzt wurde.

(6) Die Identität eines Ausländers, der das 14. Lebensjahr vollendet hat und in Verbindung mit der unerlaubten Einreise aus einem Drittstaat kommend aufgegriffen und nicht zurückgewiesen wird, ist durch Abnahme der Abdrücke aller zehn Finger zu sichern.

(7) Die Identität eines Ausländers, der das 14. Lebensjahr vollendet hat und sich ohne erforderlichen Aufenthaltstitel im Bundesgebiet aufhält, ist durch Abnahme der Abdrücke aller zehn Finger zu sichern, wenn Anhaltspunkte dafür vorliegen, dass er einen Asylantrag in einem Mitgliedstaat der Europäischen Gemeinschaften gestellt hat.

(8) Der Ausländer hat die Maßnahmen nach den Absätzen 2 bis 7 zu dulden.

Darüber hinaus existieren einige Vorgaben auf europäischer Ebene, allerdings stellen diese keine spezifischen Anforderungen gegenüber dem Gesetzgeber in Bezug auf die Integration biometrischer Daten in Ausweisdokumenten. Außerdem wird von europäischer Seite keine solche Integration gefordert.

附錄三

運用生物特徵辨識身分制度之比較研究專家學者座談會

時間：96 年 4 月三日

地點：研考會七樓簡報室

與會人員：劉靜怡教授、廖福特教授、吳豪人教授、周桂田教授、李茂生教授 謝立功教授、蔡震榮教授、劉宏恩教授 王郁琦教授、姚孟昌教授、葛祥林教授

第一輪發言

王郁琦　教授：

1、對於本報告的許多論點非常贊同。第二章第 27 頁第二段所提到的證件安全性的戰爭是具有吸引力但不必要的戰爭，如果個人擁有多張證件，每一張證件對於駭客或竊盜的人的吸引力將大爲降低，若全部集中在同一張證件中可提供多種用途他人就會有誘因來竊盜其證件，我非常贊成這樣的看法。

2、但資訊隱私的辯論的關鍵在安全和便利之間的對抗，便利和效率仍是許多社會在追求的，美國最高法院 Whalen v. Roe 一案是美國第一個針對資訊隱私的判決，最高法院法官確立了利益衡量（Balancing test）的判斷標準，資訊隱私和言論自由或其它自由不同在於，資訊隱私常需要將許多因素作綜合的判斷，因此需要用多的辯證過程，亦即應將利益、不利益、等等作通盤的討論，

台灣過去行政機關僅談它好的部分，壞的部分就不談，忽略了前置階段的討論；而學者在論證爲何不採取這些措施的時候，也常忽略該措施能帶來便利的部分，因此如何能忠實的呈現兩面的意見，是台灣未來能否進行深層探討的一個關鍵。第八章風險的部分是指出行政機關在推動相關措施，在前置階段時都應該注意。

3、本研究報告前八章點出了許多問題，而行政機關最需要的是一個指引方 guideline，來提供給行政機關操作的準則，如果研究團隊同意 biometric 是一個可以被考慮的技術，僅是有許多安全上、人權上的風險，我們要如何確保其可行。重點不是它是一個趨勢，而是它爲什麼會變成一個趨勢，如何節省行政機關的資源，減少多少錯誤，安全上提高多少防護。

當越來越多國家都採行該措施，我國政府也在考慮時，研究團對應該提供一個 guideline，該 guideline 可以是很嚴格的，譬如移民署欲針對外國旅客採行 Biometric 識別時，它前置的 due process 是什麼，需要回答哪些問題，開始採行時，該注意的問題，是否一定要有 database，如果有，有什麼安全措施。應該要給行政機關一個具體的建議。

4、過去的研究心得

（1）在使用 biometric 時，不必然要建立資料庫，資料庫存在就是風險，可在沒有 database 下，仍然可享受使用 biometric 所帶來的優點，譬如將資料存在卡片上就可達到目的，就不需要建立資料庫。

（2）特定目的外的使用應該禁止。

（3）隨著技術的進步，要降低辨識錯的可能性。

（4）在使用生物辨識資訊時，要公開透明，過去行政機關所造成的誤解，就是因爲沒有很誠懇的跟大眾溝眾

（5）可以採行模組化的方式來儲存，將資訊化成數字，不必然要以肉眼能識別的指紋等等來儲存。

（6）應該要建立適度的監督機制

5、不同意見

p28：「以上種種都顯示出辨識者辨識證件持有人的身分時， 可能出現的問題。因此，開始有機構使用電腦從事辨識者的工作， 藉著比對證件上的生物特徵和持證件者的生物特徵， 取代人爲的辨識。讓機器取代人爲的辨識最大的問題在於，機器缺乏判斷能力。人們可以藉由感覺此人是否誠實（ 雖然會出錯），而進行辨識。但是機器卻是使用同樣的標準對待每一個人。」

這句話也可以有不同的解讀，人所產生的錯誤也是非常的高，機器可以取代。機器也有錯誤的風險，然而，該種風險是可以克服的，我們不必然要設立一種全部仰賴人或全部仰賴機器的制度，機器作第一關的檢查後，第二關由人來作。但實際上當我們要試圖想出 solution 時，得去找出中道（非全部仰賴機器或人）。

6、忠實呈現的論證

198頁：「維護治安利益在大多數公眾感知下認爲大於侵犯隱私權的風險，這種風險的抉擇，相當程度是公眾認爲現行制度保障人民身家安全的不足，寧願犧牲部分個人隱私爲代價的風險個人化選擇，而這樣民眾風險感知不足的遲滯型風險的文化結構，或說是反身現代與簡單現代的典範轉移困境，將不利於一個身處全球化科技競爭、知識與科技複雜風險快速變遷的社會，因爲愈是隱匿、遲滯愈是缺乏反省批判的風險，愈容易被篤信科技安全的確定性、加強犯罪預防的簡單化約、工具性的現代化論述所操弄[16]，而形成國家機器社會，忽視科技系統可能產生的不可控制性、不可彌補性、不可回復性效應。

關鍵的問題是我願易爲我安全犧牲多少隱私，人民對於治安的需求常大於對隱私的考量，透過民主的機制，我們如何面對？即使在憲法層次來講，拿隱私換什麼東西的問題是永遠存在，不應該由政府或學者來指導民眾應該如何選擇，現行制度已經有很多方式可以讓民眾選擇。

6、234 頁

針對大陸旅客採取三合一措施，這是差別待遇的問題，而非是 biometric 可否被支持的一個理由，這是兩個獨立的問題，我對研究團隊的疑問是，若移民署最後是在一兩年內後針對所有旅客全面實施，目前僅因經費人力的問題，所以先針對大陸人士採取，是否可以接受？從目前的研究報告來看，隱含著時機未到，那確切的時機是何時？若政府實行正當法律程序後，是否可以達成？若研究團隊指出明確的規範，對政府有相當的幫助。

劉宏恩 教授：

1、剛剛王教授認爲可能不必然要建立資料庫，但現實上公部門針對犯罪偵防或移民署很難把生物辨識技術和資料庫切開，否則缺乏辨識功能。Biometric 會成爲趨勢是因爲技術和業者走在需求前，因此 push 公部門來使用這種措施，有點像我們 XP 用的好好的，但微軟推出 vista，想辦法告訴你 vista 有多好，技術業者告訴我們我們有這個需求，非我們直接有這些需求，企業去創造了需求，這在風險社會、政府跟業者間的關係、民間和技術業者的關係都有討論的意義。

2、有些國家私部門已經開始運用了這個措施，私部門的運用是否需要作一些討論，現在國家一般人民的損害往往非來自於公部門，這樣技術的運用是否需要管制。荷蘭有些 Pub，讓自願者植

入晶片，可以自由進出，進入 Pub 時就是 VIP。

3、台灣政府部門有時認爲作民調即可，但有時民調是不夠的，因爲針對沒有背景知識受訪者所做的調查沒有意義。非僅是宣導，必須有正反面意見具呈讓民眾有機會聽懂，再作民調，供政府作決策。

葛祥林 教授：

1、在結論應該提出政策建議，必須要提出此制度是針對一般人、高風險團體或特定個人，不同的使用對象會牽涉到禁止或門檻的高低，以德國刑事訴訟法爲例，可否以爲偵察目的大量搜取 DNA，法律是否定，除非有一個具體的犯罪嫌疑，才能去蒐集，目前是以一個性侵案件爲標準，去蒐集特定人口的 DNA。這樣的一個辨識系統資料庫有多大、事前建置或是後建置，這些都需要一些指標，若本報告結論能提出這些指標，未來對法規擬草規範會有相當助益。

2、媒體有相當的宣傳，我們擋不住這樣的趨勢，近日的新聞說歐洲的資料庫已將互通了，假設建構資料庫，需要有哪些安全措施、誰有取得資料的權利、在何種限制的狀況可以取得。

3、幾十年前歐洲已將開始討論仿冒護照的問題，當時德法兩國意見相當分歧，當時德國認爲歐洲護照絕對不能仿冒，因此要防止任何仿冒的漏洞；而法國認爲不知道未來何時會又出現納粹的政權，所以一定需要一個漏洞，可以仿冒護照。這類的意見，我們往往無法從民調中得到，但專家可以預先去思考這個問題，是否要跟著民意走，創制複決一直沒有落實，代表我的政權害怕民意、非專業，我們要審慎評估。

4、必須思考個人生物特徵改變的機率和因應，錯誤的處理程序必

須包含在規範中，特徵並非如歐洲 26 歲的規定就停止改變，人的老化可能就會產生變化，必須留意 biometric 沒有想像中的可靠，如何隨機性修正資料輸入。

5、Biometric 資料庫究竟是事前建置或事後，這是一個重要的指標。是針對一般人或特定犯罪嫌疑人？我們不像美國，是否一定像美國：懷疑任何人是壞蛋，我們要考慮的比美國人多。結論可以將一些未來擬草規範的指標納入，可以幫未來的價值提高。

蔡震榮 教授

請參考書面。

姚孟昌 教授

1、生物特徵的引進，改變了國家與個人的關係。人民願不願易把某些空間交回國家？國家是否能加以管制。要反對這個制度，只要提出幾個論點，只要告訴人民，老大哥永遠在看著你，到時你可能只是個號碼，在這個制度下，人民的感受記憶已經不是那麻重要了，而是你在這個社會上被記錄下來什麼，若以這個論述來看，會將這個制度污名化。

換言之，要推動這個制度，會回到一個憲法的根本爭議－國家能管制人民到什麼程度？個人將自由交出去可以換取某些安全，當國家壟斷你的資訊時，你不知道什麼地方被政府掌控了，這些資訊被掌握在國家手裡，要如何規範國家，不要讓國家變成壞蛋 h。

2、一個根本的問題：爲什麼要採取生物辨識制度？可能牽涉到隱私權、人性尊嚴、資訊自決權的保障，這時存在正當性的疑慮，

如何面對人性尊嚴的挑戰，當一個人恐懼他的資料何時會被提出，恐懼政府掌控一切，政府要如何正當化（安全？社會公益），這是有必要的。生物辨識制度目的爲何？如何說服人民將權利交出來？美日德章節論述較少。英國有詳細的論述 p70（比例原則）。可以提出台灣、美、日和德的釋憲機關如何去承認國家壟斷人民社會生活的合憲性。

3、台灣要如何取得國際間人權法、人權體制的認證，英國已經面對了這些問題，是否要遵守國際人權法的規定。

4、政府在制訂相關法案時，很多是屬於技術層面，立法機關無法介入，而行政機關要如何用既有的行政程序去監督，避免裁量的擴大、如何符合法律保留。德國聯邦憲法院對於類似事情的看法，我發現好像沒有太多東西可以看，是沒有這個問題呢 ？還是方興未艾。

5、政府必須要舉證，生物特徵辨識安全性可靠能達到什麼程度。再者，老百姓爲什麼要花錢來限制自己的權利，如果是爲了抓賊，是否有其它方法。

謝立功 教授

1、通關便利和安全間產生衝突，這是一個很難解決的問題。本研究報告也許可以製作一個優缺點的對照表，哪些國家已經具體的採用，採取何種方式？。

2、生物特徵也許未來也會變，我們未來是否要定期去更新資料，這樣成本是要多少，本研究報告也許可以納入。

3、中南美國家的旅客能不經美國就不經過美國，此時有一個便利快速的通道是大家期待，因此快速通關是推這一套系統較有利的因素。

4、若採取此種生物辨識制度，會不會有眼睛被挖掉或手被踱掉的問題，我們是否有辦法解決這些問題。

5、若要針對大陸客來進行生物辨識，是否有一個更強而有力的說法。

6、如何管理接觸到這些資料的人，管理這些資料有何配套嚴謹程序，研究報告可以提出一些建議。

李茂生　教授：

1、沒有很充分的時間做整體的閱讀，但整體的觀感就是有點囉唆。我的建議是說，重點提到就好，不用一直重複，可能是因爲時間的關係，整合上還需要再加強，要再精簡一下。

2、比較重大的問題是說，可能是因爲主持人是學憲法及人權的，有時候太過於側重人權的部分，而比較沒有注意到這個制度花相關的成本可以得到多少效益的問題。像晶片護照相關的議題，可能是我們擋不住的，如果我們不順著美國帝國主義、英國帝國主義走的話，我們可能會拿不到簽證，或者要三、四個月才能拿到，這樣可能就會構成對我們人民移動自由的傷害。既然美國老大要我們做，英國老二要我們做，如果我們不做，我們就被排除在外了。

3、我認爲，最重要的問題是，我們進去這個體系，到底是爲了我們自己而做，或是爲了外國而做？瞳孔、面貌、指紋到底包含多少隱私必須要去考量一下，不是我們學者在說有多少隱私就有多少隱私。其實我在日本的時候，也被強制按捺指紋，在日本的時候，每隔幾年要換居留證的時候，都被要求當著出入境管理局的官員面按捺指紋。

重點不在於那個指紋有多少隱私，而是按捺指紋的意義。每

次去按捺指紋的時候，你就會看到官員那種鄙視的眼神，並不是說按捺指紋這個單純的行爲對我的隱私有多大的傷害，而是透過這種辨識的方式，所產生的差別待遇的問題，而這個差別待遇是你辨識了這個人以後，其身後一大堆資訊的問題，這身後一大堆的資訊才是隱私的所在，所以不是辨識的工具，例如瞳孔、指紋有什麼隱私，而是透過這一個東西，relational database 連結到其他的資料，例如工作能力、所得等等一大堆的資訊才會產生問題。如果不能弄到後面的這一大堆資訊，而只是建立一套犯罪偵防的系統，例如留個指紋、虹膜做犯罪偵防，這個犯罪偵防系統的效益有多少雖然是一個值得討論的問題，但如果這個系統只能從犯罪現場所遺留的跡證，例如刀子上的指紋，去找出是哪個人留下的，而沒辦法去連結到這個人的其他個人資料，那麼這種從作法，我們是擋不住的。我們要擋的是，從一個 item 或是一個號碼，去找出後面所有相關的資訊，例如一個編號打下去，所有這個編號下面所有政府機關的資料整合起來，都跑出來，這才恐怖，才會侵犯我們的隱私，這才是我們要防範的。所以並不是辨識的那個東西是我們的隱私，而是從這個辨識的東西去找到下面所有的 database 裡面的東西，才是我們的隱私。

4、如果從這點來看的話，我們的晶片護照有什麼意義呢？其實，對我們而言沒什麼意義，就只是爲美國服務而已。美國如果要反恐，基本上它就必須要掌握每個號碼後面的所有資料，不然它如何只找出恐怖份子？可是美國又沒有辦法在對全世界六十億的人去找這些資訊，所以它只能要它的每個附庸國都把資料準備好，而後如果你的人民要來美國，它只要輸入一個號碼，就可以進到你各國的資料檢索裡面，看到這個號碼背後所有的資料，看是不是恐怖份子。問題就是說，花那麼多錢去照恐怖份子，找得了或找不了？當然，恐怖份子的大頭頭本來就掌握住了，所以大頭頭不會去美國綁炸彈自殺，真的會去的，都是看起來不像恐怖份子

的人，死掉才知道是恐怖份子的，也就是說恐怖份子都是潛在性的，已經出現的恐怖份子都是已經死掉的了。所以，用這種方式要抓恐怖份子是絕對抓不住的，所以如果藉口說 911 恐怖攻擊，然後要國際民航組織去做晶片護照搞這種玩意兒，我覺得最後真正的作用應該是將來要用在非法移民、非法打工之類的。就是剛剛我講的，透過一個辨識機制，給你一個歧視，而這個歧視 always 有個 database 在那邊做整理最好，例如將來到美國去，美國就看是不是你這個人，然後就從這個號碼進 database 去看，然後看你有沒有可能非法停留過久等等的，或者說從發簽證的時候，就進資料庫去看。所以，到最後就是我們的國家爲了美國這種的國家，爲了英國這種的國家，去蒐集我們人民的資料，爲了美國、英國的經濟發展與安全去蒐集資料，對我們國家的發展可能沒什麼意義。當然，對我們有沒有用？我們可以跟老共要資料，但老共有沒有可能給我們資料？不可能！所以，搞到最後，我們有很多非法移民，可是我們又沒有辦法非法移民到他國！沒辦法移到美國，但我們又擋不住中國的非法移民。所以，這個做到最後就是有損國格啦！這種有損國格的事情，要做的話，是不是要跟人民講？跟人民講說，我們要做的事，有損人格、國格，還要不要做？人民當然還是會說，還是要做，因爲他想要去大峽谷走天空佈道嘛！那這種隱私算老幾嘛！就給你嘛！所以，到最後在結論上就是一句話，「小國的悲哀！」

共同主持人

陳顯武：

1、謝謝劉教授邀請我參與這個研究計畫。今年的三月二十五日是歐盟五十週年，歐盟提出了幾個 2009 年要達成任務，其中生物晶片的東西可能就會列進去，因爲他有提出幾個原則，第一就是恐

怖主義的對抗，還有組織犯罪、非法移民，認爲是歐盟要克服的問題。從這些方面來看，德國的規定還是屬於比較嚴格的，它必須就它國內的相關法律來進行修改。例如剛剛李教授所講的database，德國也必須在國內法進行修改，不然就沒辦法使用。我們國內對於個人資料的保護，是不是有這麼嚴格，就還需要再探討。

2、另外，我們採用生物特徵來做辨識身份的方法，除了考慮安全性以外，也要考慮相關犯罪時，可能對人身造成傷害的嚴重性，例如若用虹膜是不是有可能造成眼球被挖起來。至於德國相關的修法，我們也都有在密切注意中。我先做這樣的說明。

廖福特 教授：

我負責的主要是英國及歐洲的制度方面，我就做個簡單的介紹。我做這個研究時，我是滿自我限縮的，就是我沒有放太多自己的評斷進去。我自己一貫的立場是，如果我是寫文章的話，我會放比較多個人意見進去，如果是研究報告的話，我就是儘量讓多元的意見能夠呈現，我也假設這是研考會比較想要的。英國部分比較有趣的是，英國也有個按捺指紋的法案，而且草案也通過了，我是很好奇這個法案到最後會不會到倫敦的法院來訴訟，或是到歐洲人權法院去訴訟，未來還值得再觀察並予以補充。

周桂田　教授：

1、謝謝各位教授的意見提供。我是一位學社會學的，跟其他教授比較的法學背景比較不同。就像劉宏恩教授剛剛所提的，技術的演進可能會創造需求，而其中又跟市場的引進有關，跟私人也有關係。不過，我們這篇報告主要是放在國家的部門。

2、同時，也像李教授剛剛所講的，在帝國主義的政治經濟架構下，我們可能也擋不住 biometrics 的趨勢，但我想再向李教授請教的是，如果要擋的是 code 後面所產生的個人身份、財產、種族所產生的偏見，在制度上、規範上要如何去擋？我想這是現在世界各國運用 biometrics 都要面對的問題。

3、另外，謝立功教授也有提到，biometrics 的哪個部分可以用，哪個不能用，並不是說所有的 biometrics 都可以用，相關的問題都應該討論，才能知道要如何去規範 biometrics。我寫的風險這個部分，有一個重要的思考點，就是雖然 biometrics 在國際上是個潮流，有個滑坡效應，但這個技術在我們國內運用的時候，在我們本國制度的接軌到底產生什麼樣的問題。我們做社會學的人，常會看我們國內現行的制度、法令的現狀與其他國家到底有什麼不一樣？以我們國內對於個人隱私保護確實是比較差的情況，若引進國外的這些技術，會不會有什麼更嚴重的問題？這是需要我們 concern 的部分。事實上不同的國家在跟進同一制度的時候，會再不同國家的脈絡產生不同的問題，如果依照過去的經驗，醫院賣病人的資料、警官賣資料及教授賣學生的資料，如果我們建置 biometrics 的資料庫，把相關的資料集中到國家的資料庫之後，將來相關資訊系統的管理及隱私暴露的層面，可能就沒那麼簡單，而不只是規範面的思考而已。這就牽涉到，剛剛很多教授有提到，如果要將新的技術引進到社會，例如我們的護照開始使用晶片，政府應該說服人民，讓我們的人民瞭解到底要效率或安全。一般人思考這個問題，可能會思考效率、安全的問題。但其實這是一個典範不同的問題。如果民眾不瞭解的情況下被詢問，可能就會說願意犧牲一些資訊來獲取安全，但若民眾多瞭解後，他會知道這個技術在制度化的過程中，在 general 的層面，在國際的層面，通常會引發哪些問題。

4、第二個層次的問題是，在我們的社會裡面又特別會產生什麼樣

的問題。在這樣情形下的 deliberation 才能比較深入。這是我在第八章所要強調的，無論我們要不要做 biometrics，政府都應該去說服民眾，而不只是去考慮一個很單純的成本效益分析。

5、第三點是最大的 concern 是說，國際上在發展這個 biometrics，是不是像李茂生教授所說的，是帝國主義的擴張，而沒有辦法脫離一定要跟進的？我覺得這裡可以有一個很大的辯論。現在已經發展出這個技術，但我們是否一定要被迫跟進？如果不跟進的話，又是怎麼樣？

綜合討論

葛祥林　教授：

針對具體這部分，我會建議，要不要就建構資訊保護官的制度？要蒐集資訊可以，但要確保其監督。由這樣一個獨立的機構來監督，除了在規範之上有監督以外，在執法上也可以有監督。這是立即可以來推行的。

劉靜怡　教授：

這個的確是立即可以來執行的。我之前接過研考會的計畫，也曾經這樣建議，但可以想見的是，行政院一定跟你說。做比較研究有個最大的問題是到底要比什麼？國際上哪些是可以拿來跟國內比的？舉例而言，問一個美國的知識份子要不要做晶片護照，例如找一個美國法學院的學生來問，他一定會有很多的問號，有很多的 concerns。但我們在台大法律學院找一個學生問他，他可能就不會有這麼多問號。所以這裡面就凸顯一個很大的麻煩就是，在各個國家不同脈絡發展出來的辯論很難比，除了一個最好比的就是晶片護照以外，都很難相互比較。

李茂生　教授：

其實我們做這個 biometrics 純粹是爲了服務美國。像日本在全國的國道、縣道裝了 N 系統，花了四百多億，他還可以說是爲了對付境內像奧母真理教這種的世界末日型宗教。N 系統是紅外線的，講話、動作都全部錄進來了。有個日本自民黨的新秀跟其不倫戀的愛人，就是被 N 系統拍到，被「星期五雜誌」刊登出來，然後他的政治生命就毀了。但我們台灣境內並沒有向日本這樣的威脅存在，所以做這套系統就真的只是讓國人去美國大峽谷看一看，就看全民覺得是否值得。

劉靜怡　教授：不過，國安系統方面都會跟你說，做這個是要防範來自於中國的威脅。

李茂生　教授：老共其實如果要搞垮我們，只要派一兩隻有狂犬病的狗進來，不用一個月，台灣就毀了，你可以去農委會問問看。而且我們台灣商人走私很多東西來台，只要來個禽流感，一下就毀了。

劉靜怡　教授：所以，其實重要的不是在國境上對人做控制，而是要對所有的貨物做控制。

李茂生　教授：對呀。完全沒錯。

劉靜怡　教授：我也是認爲對人的管制的意義不大。我最近去美國的經驗是，他經過一到程序就是，你很快的經過一個通道，對你進行掃瞄。但是他的篩選方式很笨的，完全是以你持何種護照入境，真是一個笑話。只要是拿美國護照入境的，都不會被要求經過這一道掃瞄，但是你怎麼能知道一個拿美國護照在第三世界住了十年的人，是否會成爲恐怖份子或爲了真理而奉獻呢？我之前去美國，我們這種拿台灣護照的人，就有一個海關的官員，一

路一直跟著你，確定你已經出海關了。我就想，妳們時間還真多耶！就是要成本！但是，是不是有些人覺得這樣做真的比較安全呢？我想，說不定有，說不定這提供了國民一種安全感。

李茂生　教授：如果從刑事政策的觀點來看，在局勢不穩定的時候，爲了要能夠度過，你需要一個很穩定的民心，需要一個國民共同感情的中間體，那就是要找到共同的敵人。那要如何確認共同的敵人，就要從日常生活中去確認。所以這個東西就是平常這樣做做，雖然不能達到真正的安全，但可以找到共同的敵人，可以有安全感就可以度過這情勢，這是刑事政策上的妖魔化。美國這樣做，真的以爲能反恐嗎？我不覺得，我覺得他們沒有那麼笨。他們當然知道他們付出那麼多成本，其效果只是一種安全感。

另一方面，爲什麼恐怖份子要跟美國鬥得這麼凶？這也跟美國在人家境內燒殺擄掠很有關係，今天美國把這些人妖魔化，就可以把過去幹的壞事都一起抹淨。這種是以前納粹也做過。所以，美國現在在座的就是這種事，而我們也被他妖魔了。所以，如果我們擋不住，我們在表面上要與他配合，但我們應該選擇最不會讓人感覺受到屈辱的方式，比較不會有屈辱感的。此外，我們真的深入的資料，只有犯罪人的全部資料，一般人的全部資料不會出來，這事後處理。那如果是預防處理，必須蒐集所有人的資料，國際上透過國際合作，美國直接到我國的資料庫找資料，或是由我國警察到資料庫找相關資料提供給外國，我們要提供什麼。

美國在 80 年代公司和調查局結合起來，互通資料，這是相當恐怖的，我們需要現在給他確定機制，避免濫用。應該要建立一個絕對清楚的法治，在公部門建立一個資訊保護監察機構。

研考會代表

1、本報告的研究目的是（1）我國現況的相關制度（2）比較各國的法治（3）未來政策的應用性。從目前期末報告的初稿看來，（1）的部分較爲缺乏。

2、研考會的立場是希望要有政策的具體可行性

3、各章的比重不依，有些國家偏重法治面，有些偏重正反意見，研考會希望能將各國正反意見中性的呈現出來。

4、有些地方用詞上過於強烈

譬如 p187 頁－尤其是兩國的關係由同一公私進行－包含了價值判斷。研考會認爲除非有更充分的論證，否則在報告中不太適合。

5、期中報告審查意見能納入修正。

主持人回應

1、外交部晶片護照的整體規劃的相關資料很難蒐集，請研考會能協助蒐集資料。

2、爲盡量統整各章，用語方面會加以修改。

附錄四

行政院大陸委員會就本委託研究案期末報告初稿函覆意見

From: *行政院陸委會* <*macst@mac.gov.tw*>
To: <*deven717@hotmail.com*>
CC: <*macst1@mac.gov.tw*>, <*rdec@rdec.moc.gov.tw*>
Subject: *於國境線上建置生物特徵身分辨 識通關系統之相關說明*
Date: *Mon, 16 Apr 2007 17:37:27 +0800*
>發文日期:中華民國 96 年 4 月 16 日
>發文字號:陸法字第 0960006171 號
>
>一、依行政院研究發展考核委員會 96 年 4 月 3 日會研字第 0960007023 號函辦理。
>二、有關政府規劃於國境線上建置生物特徵身分辨識通 關系統之緣由及作法，本會說明如下：
>(一)有關隱私權或資訊自決權之保障， 國民得主張之，惟外國人在我國是否亦得主張？依學者見解認爲其屬人格權範圍，外國人亦得主張之，惟對國民與對外國人保護程度及範圍應有不同，同時國境管制較諸於國 民的一般身分辨識有更高的需要,較具有正當性。蓋因國家對本國國民可藉由生活與居 住的環境空間（例如住居所、受教育或執業場所等）和人際關係（如親屬、朋友等）所 提供之種種資訊，交叉比對出其國民的正確身分，惟一旦前往外國，脫離主要生活環境 和人際關係，他國政府除護照以外，少

有方法確認外國人身分,因此採行指紋或其他生 物特徵之辨識方式,有其必要性及正當性。(參酌釋字第 603 號林子儀大法官協同意見 書)。

>(二)國際民航組織爲便於國際間港埠快速通關,並防止恐怖份子攻擊, 維護國境安全,已訂定採用生物特徵辨識系統(以臉部生物特徵爲主,指紋及虹膜特徵 爲輔)並結合無線射頻識別系統之電子護照標準(即各國對其國民核發之護照內含有電 子晶片,晶片中可錄存當事人之生物特徵,除供國人入出所屬國之國境時,爲身分辨認 及通關便利外,晶片中並存有標準規格之資料,於入出他國時,足供他國爲身分之查驗),供各國參採通行,俾持憑出入本國及他國。此一國際標準規範之目的,在於同時可 加速通關速度及節省查驗人力,有效查核通關者身分及防止冒用或僞、變造護照之情事 。

>(三)目前國際間已有美國、英國、加拿大、日本、新加坡、香港、俄羅斯、 澳大利亞、德國等 25 個歐盟國家,對於入出境人士已採行或規劃採行生物辨識之身分辨 識方式,包含中國大陸亦規劃採行此項辨識標準。此外,目前已有一些國家,考量他國 配合國際民航組織推動電子護照之時程不一(或未必採行),除了針對其所屬國民建制 電子護照外,亦兼顧他國國民之往來,建置足資辨識身分之資料庫(如美國、香港及預 計於今年底實施之日本等)。

>(四)我國針對國民核發電子護照乙事,外交部已 列入護照條例修正草案;而針對外國人來臺採生物特徵之人別辨識方式,內政部於入出 國及移民法草案亦已納入法律規範,該二法案均正在立法院審議中。

>(五)中國 大陸固將參照國際趨勢製發電子護照,惟大陸人民來臺,其主管部門以不發護照爲原則 ,我政府國境上自無足資採爲辨識之用。而現行對大陸人民實施按捺指紋的對象有限, 尚無法有效遏止大陸人民以僞冒身分或持僞、變造證件申請來臺之情事

發生，因此爲順 應國際趨勢，與國際接軌，及因應未來大量大陸人民來臺，於衡酌兩岸交流實際情況， 基於身分辨識及通關便利之考量，政府爰規劃結合現行入出境之證照查驗，僅於國境線 上先行建置臉部生物特徵辨識系統（並未包括指紋及虹膜）。而此作法並不具侵入性， 並較可將入境人別之生物特徵取於無形，免生爭議，其作法爲：

>１、申請人繳 交符合採集臉部生物特徵規格之相片（同國人換發新身分證所繳交之國際標準規格相片 ），以申辦入出境許可證。

>２、入出國及移民署將相片掃瞄建檔儲存於資料庫 。

>３、申請人通關時，經由國境線上之臉部生物特徵辨識通關系統，當場攝影 擷取其臉部影像予以比對，以確認通關者與申請入境資料相片上之本人是否爲同一人。

>(六)此一系統之建置，於兩岸交流日益頻繁之際，對強化國境線上管理及維護 國境安全，防範大陸人民以僞冒身分或持僞、變造證件申請來臺等情事之發生，應有相 當之助益。

>(七)由於本案僅先行規劃建置臉部生物特徵辨識通關系統，並未包 括指紋及虹膜，因此有關今年年初媒體曾報導我國將自今年 6 月起，對所有來臺的大陸 人民採指紋、臉部及虹膜三合一入境身分辨識方式，與事實不符。此外，內政部並已研 擬申請動支 96 年第 2 預備金，規劃於取得該預算經費後擴充設備，以對所有入境之外來 人士實施臉部生物特徵身分辨識，故此項措施並非僅對大陸人士實施，亦非歧視性作法 。

>三、上述本會說明，謹供補充、修正研究報告初稿參考。

>四、檢附 本會人民陳情案件處理情形調查表乙份，請撥冗填答。

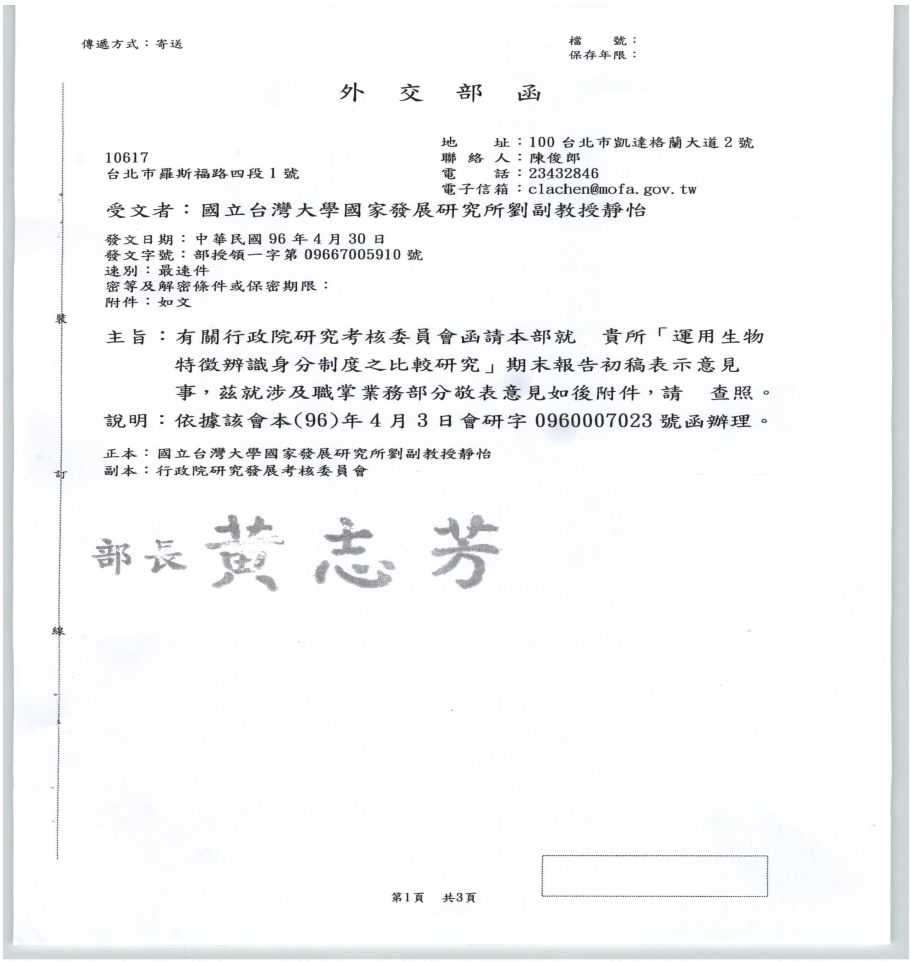
謝謝！

>行政院大陸委員會敬復

運用生物特徵辨識身分制度之比較研究

附錄五

外交部就本委託研究案期末報告初稿函覆意見



傳遞方式：寄送

檔　　號：
保存年限：

外　交　部　函

地　　址：100 台北市凱達格蘭大道 2 號
聯 絡 人：陳俊郎
電　　話：23432846
電子信箱：clachen@mofa.gov.tw

10617
台北市羅斯福路四段 1 號

受文者：國立台灣大學國家發展研究所劉副教授靜怡

發文日期：中華民國 96 年 4 月 30 日
發文字號：部授領一字第 09667005910 號
速別：最速件
密等及解密條件或保密期限：
附件：如文

主旨：有關行政院研究考核委員會函請本部就　貴所「運用生物特徵辨識身分制度之比較研究」期末報告初稿表示意見事，茲就涉及職掌業務部分敬表意見如後附件，請　查照。

說明：依據該會本(96)年 4 月 3 日會研字 0960007023 號函辦理。

正本：國立台灣大學國家發展研究所劉副教授靜怡
副本：行政院研究發展考核委員會

部長 黃志芳

第1頁　共3頁

外交部對於「運用生物特徵辨識身分制度之比較研究」期末報告初稿中涉及職掌業務部分敬表意見如次：

一、我晶片護照不涉爭議性之生物特徵

研究報告： 第一章第參節及第二章第肆節略稱利用生物特徵身分辨識科技係一重大公共政策，相關立法措施應予建立，隱私保護亦應徹底研究。第八章第參節強調生物辨識身分制度風險溝通之重要性。第九章描述本部推動晶片護照發展計劃涉及人民重大權利義務事項，未經國會充分討論，即草率推動。
本部意見： 晶片護照係國際民航組織(ICAO)推動國際共同打擊犯罪策略之一環，我國爰共同參與。本部於計畫推動之初，即基於國情考量，規劃以晶片儲存現行護照既有資料，亦即僅係將現行護照資料數位化儲存，不涉指紋、虹膜等具爭議性之生物特徵；並配合修正護照條例，納入晶片護照條款，作為日後實施之法源依據；同時依計畫進度擬定宣導方案，以簡政便民之服務為宣導主軸，相機公開介紹晶片護照，廣泛向民意機關及民眾說明。綜言之，本部自 92 年起

1

著手晶片護照相關規劃，必要之立法措施、隱私權保護及與立法院溝通及向民眾民宣導等事宜，均已完整納入計畫配套措施中。

二、晶片護照安全性高：

研究報告： 第三節稱晶片護照係使用 RFID（無線射頻）技術，晶片資料易遭盜取。
本部意見： 規劃中之我國晶片護照，並不儲存現行護照以外之資料，民眾顧慮可降至最低，且晶片護照儲存之個人資料須依國際規範以電子簽章(PKI)加密保護，晶片讀取距離僅約 2-5 公分。多數國家選擇採用「基本讀取管制功能」（BAC)編碼，凡讀取晶片資料時須先打開護照本，並以光學字型辨識機(OCR)讀取護照資料頁機器可判讀碼，方可解碼啟動閱讀機與護照晶片之聯結，未經上揭程序即無法讀取，採行防止資料遭盜讀、盜錄之保護設計。另未來晶片護照資料管理系統將沿採內部網路系統，電子簽章(公鑰憑證)以硬體、離線保存，不與外部網際網路聯線，以阻絕駭客入侵。

守分際，報告內容與事實似有出入。

六、儘量沿用既有設備

研究報告：

第八章第肆節及第九章第參節均稱，外交部不應在晶片護照未經國會充分討論，法源未定之前，動輒撥下龐大資金採購相關機器。

因此晶片護照之資訊防護極其嚴密，無法輕易盜取。

三、晶片護照全球適用

研究報告：

第八章第貳節引述廖元豪教授指稱，晶片護照不可能在未發行晶片護照國家使用。

本部意見：

晶片護照核發國家近一、二年內可望達到 50 餘國，幾已涵蓋各主要先進國家。另晶片護照與現行機器可判讀型護照紙本列印規格一致，部分國家即使未規劃發展晶片護照專用通關閘門，仍可經由機器判讀或人工進行查驗，完全不影響通關作業。

四、各國須於 2010 年前發行機器可判讀型護照

研究報告：

第 194 頁：國際民航組織規定世界各國須於 2010 年前發行晶片護照。

本部意見：

國際民航組織係規定世界各國須於 2010 年前發行機器可判

讀型護照，而非晶片護照。

五、晶片護照證實確為可行

研究報告：

第九章第參節指出，政府決定發行晶片護照係把國人當成白老鼠。

本部意見：

全球現已有美、日、紐、澳、星、港及歐盟等 37 國成功發行晶片護照，護照發行前皆經小規模發行及國際共通測試，確屬可行。加拿大、韓國等 10 餘國亦宣稱於一至二年內跟進。本部係經詳細評估後，決定發行晶片護照，並已呈報行政院核定為本部中程個案計畫，規畫及執行過程嚴守分際，報告內容與事實似有出入。

六、儘量沿用既有設備

研究報告：

第八章第肆節及第九章第參節均稱，外交部不應在晶片護照未經國會充分討論，法源未定之前，動輒撒下龐大資金採購相關機器。

本部意見：

基於節省經費考量，本部將在現行設備繼續沿用前提下，採公開招標方式購置製發晶片護照所需之必要設備，主要項目包括個人資料之讀寫、保護、影像處理及辨識、品檢等相關軟硬體設備及新舊軟體應用系統整合等。本部 96 年度該項計畫計編列 5 千 2 百萬元之合理預算。

七、**晶片護照正面效益**

本部意見：

（一）**防止偽、變造：**晶片護照將儲存兩套相同個人之基本資料及照片，一採顯性列印於護照紙本上，以薄型防偽膠膜保護，另一採隱性寫入護照晶片內，以電子簽章加密保護。因後者完成寫入即鎖死無法再行覆寫，縱使護照紙本列印之照片遭變造，在晶片內儲照片影像無法變更下，兩相比對，查驗人員即可目視判別持照人身分真偽，有效杜絕偽變造事例。

（二）**遏止冒名申請、冒領：**本部擬併晶片護照製發設備採購案，導入臉部辨識系統，以強化護照申請人資格審查。本部規劃將申請人繳驗照片掃描成影像檔後，經

5

由系統蒐尋資料庫歷史照片影像，進行1:1或1:多比對臉部特徵，以逐筆查核申請人是否為合法持照人，有無重覆申請(同臉部特徵、不同姓名)或冒領(同姓名、不同臉部特徵)不法情事，透過機器自動、大量、快速、正確處理，輔助櫃台人工查驗經驗及設備之不足，集中心力處理不法申請案件。據悉，澳大利亞於2005年10月發行晶片護照，同時導入臉部辨識系統，強化申請人身分查核，電腦自動就申請人繳驗相片與資料庫700萬筆臉部影像進行比對，成功查獲多起先前單靠人工作業無法有效解決之護照常業犯，其中易容、更名或持假身分證件申請護照均無所遁形。

(三) **便利國人海外通關**：上述主要先進國家已陸續配置晶片護照專用自動查驗通關閘門，未持用晶片護照旅客即無法享有此一快速通關優遇，而須忍受排隊久候查驗之不便。為維護我身為國際資訊大國之形象，並嘉惠每年近800萬出國旅行國人在國外享有快速便捷通關手續，我實有必要儘速發行晶片護照。

(四) 本案研究報告對於晶片護照在防杜文件遭偽變造、不法取得使用、快速通關等方面之正面效益尚可詳加探

討，對於本部晶片護照發展計畫及晶片護照資訊安全防護措施瞭解亦可加強，故部分研究結論不免仍有研究空間。

附錄六

法務部就本委託研究案期末報告初稿函覆意見

本司謹就電腦處理個人資料保護法部分，表示意見如次：

一、 依電腦處理個人資料保護法（以下簡稱個資法）第 3 條第 1 款規定，個人資料係指自然人之姓名、出生年月日、身分證統一編號、特徵、指紋...及其他足資識別該個人之資料，本研究報告所稱之「生物特徵」已足資識別該個人，乃屬個資法所稱之「個人資料」。公務機關對上個人資料之利用，應於法令職掌必要範圍內為之，並與蒐集之特定目的相符（個資法第 8 條規定參照），合先敘明。

二、 另個資法修正草案第 6 條規定（立法院一讀通過條文）:「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。(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，為統計或學術研究而有必要，且該資料須經過處理後或依其揭露方式，無從識別特定當事人者為限。」按個人資料中有部分資料性質較為特殊或具敏感性，如任意蒐集、處理或利用，恐會造成社會不安或對當事人造成難以彌補之傷害。是以，經審酌我國國情與民眾之認知，爰規定有關醫療、基因、性生活、健康檢查及犯罪前科等五類個人資料，其蒐集、處理或利用應較一般個人資料更為嚴格，須符合所列要件，始得為之，以加強保護個人之隱私權益。故如本案所稱之「生物特徵」屬前開 5 類特種資料之一者（如基因），應注意未來上開條文之適用；又縱非前開 5 類特種資料之一，依司法院第 603 號解釋意旨：「...國家基於特定重大公益之目的而有大規模蒐集、錄存人民指紋、並有建立資料庫儲存之必要者，則應以法律明定其蒐集之目的，其蒐集應與重大公益目的之達成，具有密切之必要性與關聯性，並應明文禁止法定目的外之使用。主管機關尤應配合當代科技發展，運用足以確保資訊正

確及安全之方式為之，並對所蒐集之指紋檔案採取組織上與程序上必要之防護措施，以符憲法保障人民資訊隱私權之本旨。」職故，為召慎重，有關蒐集及利用生物特徵之個人資料乙案，仍宜有專法明定蒐集目的、處理及利用方式等事宜為妥。

附錄七

內政部入出國及移民署就本委託研究案期末報告初稿函覆意見

有關「運用生物特徵辨識身分制度之比較研究」期末研究報告初稿

內政部入出國及移民署回應意見一覽表

【原文 1】(p2)

其次，移民署成立之後，亦具體形成無論是短期入境觀光，大陸配偶來臺長期居留，在入境通關之時，均須接受「按捺指紋、拍攝臉型、掃瞄虹膜」的三合一查驗身分政策。並且已經購置生物特徵辨識系統，將在相關授權法令正式通過之後，分配在各個機場海關，做為通關控制之用，可見目前相關政府機關對於生物特徵辨識技術的採用企圖和作法，並未因為釋字 603 號解釋的出現而減緩。

【回應意見 1】

移民署僅採用不具侵犯性的臉部特徵辨識，並未使用「按捺指紋、拍攝臉型、掃瞄虹膜」的三合一查驗。另針對原依法需按捺指紋者如：團聚、居留、定居及遣返者，則維持原按捺指紋做法。

【原文 2】(p5)

除了對本國人民簽發內建儲存個人資料晶片的晶片護照之外，因應外籍移住民和開放大陸觀光客的政策，移民署也準備以生物特

徵做為身分辨識的依據。換言之，在大陸人士或其他外籍移住民入境時，都必須現場按指紋、攝取臉部影像和掃瞄虹膜等，進行比對，若比對率過低，電腦系統將提醒移民官加強查驗證照和其他身分驗證的工作。此種藉助生物特徵身分辨識系統所進行的入出境查驗程序，其目的不外乎提高查察利用改名和假冒身分方式從事偷渡、非法打工、逾期停留及其他不當或不法目的之行為的效率。

【回應意見 2】

世界各國為推行自動通關查驗，由旅客自行使用 RFID 晶片護照進行生物特徵辨識，依國際民航組織（ICAO）規範：生物特徵辨識系統(Biometrics)辨識方式，以臉部特徵為主，指紋及虹膜為輔。移民署僅採用不具侵犯性的臉部特徵辨識，並未使用「按捺指紋、拍攝臉型、掃瞄虹膜」的三合一查驗。另針對原依法需按捺指紋者如：團聚、居留、定居及遣返者，則維持原按捺指紋做法。

【原文 3】(p9)

平心而論，臉部辨識並不是太新的技術，而臉部辨識技術的缺陷也不斷被提出來討論，所以，移民署準備設置的臉部辨識系統，是不是有效的身分辨識方式，或許是應該深入討論的重點之一。電腦辨識以 3D 技術為臉部測點，雖然一般認為誤差率低，但是，此種技術還是會受到環境、裝扮與長相改變等因素影響，則也是不爭的事實。因此，用臉部辨識技術來處理護照真偽查驗的問題，其實可靠性不高，護照防偽如何設計，以及如何確定護照持有人和護照上的個人資料具有同一性，而不是將照片或臉部辨識技術

這種應屬護照查驗中的輔助項目當做重點，或許才是癥結所在。同樣地，臉部辨識技術之外的其他生物特徵身分辨識技術，其精確度究竟有多高，安全性又是如何，究竟是否適合做為身分辨識制度中所仰賴的主要工具，似乎也不盡然是不應該受到質疑的對象。

【回應意見 3】

同回應意見 2。

【原文 4】(p194)

今年 2007 年初中國時報報導，為因應大陸觀光客「大舉入侵」，移民署已購買二十二套生物特徵辨識系統分散於桃園機場、高雄小港機場、金門與馬祖服務站，最快於三月、最慢於七月啟用，全面防堵大陸人滲透國境；移民署署長吳振吉表示使用生物特徵辨識系統是國際上防患未然趨勢，將率先對中國旅客和中國配偶實施臉型辨識；移民署副署長吳學燕進一步指出何以專挑大陸客通關查驗，是因為大陸人民偽造、變造身分入境的情況，比其他外國人來得嚴重，因此率先對大陸人士實施臉型辨識，未來將逐步擴及入境來台的外國人。

【回應意見 4】

臉部特徵生物特徵辨識系統預計於 7 月 1 日上線使用。

【原文 5】(p201)

難保生物辨識系統資料庫的管理或者資料庫電腦與電腦連結過程，不會產生個人資訊外洩的情事。移民署這回除了向廠商承購指紋、臉型、虹膜三合一電腦的硬體和軟體設備外，另有資訊工

業策進會從旁協助進行電腦化的工作，移民署並指出，建置生物辨識電腦系統的目標，主要有二，首先透過自動化臉部生物特徵辨識技術，執行入出境查驗工作，可有效查察利用改名、假冒身分、偷渡、非法打工、逾期停留及政治滲透等不法情事。其次，為使臉型影像檔案可與島內外相關單位進行“情資交換”，移民署將此案數據庫檔案，採取以國際通用的檔案格式建檔儲存，並進行轉檔交換，與“移民署”現行的境管系統整合。

【回應意見 5】

1.移民署並未使用「按捺指紋、拍攝臉型、掃瞄虹膜」的三合一查驗。

2.資訊工業策進會係進行 RFID 自動通關研究案，並非協助進行臉部辨識電腦化的工作。

3. 生物特徵辨識為世界各國兼顧安全、便利之趨勢，並非戕害人權、侵害隱私權之作為。另因電子護照須於全世界通用，故需與全球相關單位進行情資交換，但移民署資料庫屬境內管理，不需與國內外相關單位進行情資交換。

【原文 6】(p209)

然而內政部移民署是台灣率先決定對大陸旅客與大陸配偶採用「按捺指紋、拍攝臉型、掃瞄虹膜」三合一生物特徵辨識系統的管制機關，顯而易見，一開始就犯了對單一族群歧視的行為，因而引起相關權益族群的抗議，如中國時報 2007 年 1 月 3 日報導記載移民署門口聚集著一群抗議的大陸配偶，高喊「要工作、要身分、要人權」，抨擊海關人臉生物辨識對她們是歧視，要求所有權利比照外籍配偶。

【回應意見 6】

移民署並未使用「按捺指紋、拍攝臉型、掃瞄虹膜」的三合一查驗，生物特徵辨識將針對所有外來人士實施，但第一階段係針對過去紀錄較多者、風險高者實施，日後即將擴及所有外來人士。因大陸地區人民申請案以「同名異人、同人異名」偽造身分情況較為嚴重，故先從大陸地區人民實施，再逐步擴及外國人。

【原文 7】(p227)

民眾的風險感知也跟科學技術官僚散佈的資料證據息息相關，因為經由二手傳播之非經驗所形成的公眾風險意識，事實上也必須從科學風險評估或決策者傳遞的資料訊息引證。而我國的技術官僚，長期以來習慣由上往下、威權式的、線性因果的實證確定性來推動各種科學計畫，以簡單化約、工具性的現代化、單面利益論述建構生物辨識系統的好處，而這些端倪也反映在移民署通關辨識與外交部的晶片護照上。

【回應意見 7】

無修正意見。

【原文 8】(p228)

其實國外在試驗實施晶片護照及生物辨識系統相關設施後，出現許多問題，除了新儀器辨識率容易出錯外、仍存有諸多社會、倫理、法律、政治、經濟面向的疑慮，如生物特徵辨識科技費用昂貴，新護照的高成本必定轉嫁消費者，英國政府就因核新型生物護照後，因維護科技設備成本居高不下，迫使英國成人護照連漲三成，飆上每本護照新台幣四千元，引發民眾怨聲不斷。故若外交部、移民署仍然要強制辦理，是把國人當成白老鼠，如今新護照屆時能否趕上法律修正腳步、是否適用國內相關仍是疑問，然

而巨額資金業已準備付出。(p228)

【回應意見 8】

針對外國人來臺採生物特徵之人別辨識方式，內政部於入出國及移民法草案已納入法律，目前正在立法院審議中。中國大陸固將參照國際趨勢核發電子護照，惟大陸人民來臺，其主管部門以不發護照為原則，我政府國境上自無足資採為辨識之用。因此為順應國際趨勢、與國際接軌，及因應未來大量大陸人民來臺，於衡酌兩岸交流實際情況，基於身分辨識及通關便利之考量，大陸委員會爰協請內政部規劃結合現行入出境之證照查驗，僅於國境線上先行建置臉部生物特徵辨識系統，並經行政院同意內政部所提報之計畫案，由內政部移民署推動辦理中。此一系統之建置，於兩岸交流日益頻繁之際，對強化國境線上管理及維護國境安全，防範大陸地區人民以偽冒身分或持偽、變證件申請來臺等情事之發生，應有相當之助益。。

【原文 9】(p228-229)

各國經常以立法來延宕科技風險的可能性，但在美國的生物辨識技術發展霸權與競爭放任之下，所有的社會風險的門檻紛紛失守。外交部、移民署等晶片護照與生物辨識機器的購買，類此涉及人民重大權利、義務的事項，政府應慎思明辨、決策應保守而謹慎，實不宜在未經國會充分討論、生物辨識科技法源尚在未定之天、及有公民審議程序、聽證程序、公民諮詢與公民會議等公共討論，經過多次且多元廣泛的風險溝通後，達到社會共識時，就動輒撒下龐大資金，讓備受爭議的新制上路，這樣的決策未免過於草率，欠缺謀定而後動的智慧，萬一生物辨識技術有違憲的爭議，在立法程序無法過關，那麼購置的設備豈不是浪費公帑？故從本旨研究建議，不應該在反恐的大論述底下，就冒然實施生

物辨識技術、晶片護照等政策，否則將產生風險不可回復的後果。

【回應意見 9】

無修正意見。

【原文 10】(p232)

本章主要目的在於總結前面各章的內容，分析生物特徵身分辨識技術應用在我國時，應該特別予以留意和處理的規範與政策問題。這些規範和政策問題，隨著外交部準備全面換發具有生物特徵身分辨識機制的晶片護照，並且被列為行政院的重大計劃之一，以及移民署針對外來移民準備採取類似的措施，針對生物特徵身分辨識技術的運用，在規範、政策和社會等層面可能引發的效應和影響，進行徹底的討論和辯論，應該已是刻不容緩的社會工程之一。

【回應意見 10】

無修正意見。

【原文 11】(p235-236)

尤其，民眾的風險感知也跟科學技術官僚散佈的資料證據息息相關，因為經由二手傳播之非經驗所形成的公眾風險意識，事實上也必須從科學風險評估或決策者傳遞的資料訊息引證。而我國的技術官僚，長期以來習慣由上往下、威權式的、線性因果的實證確定性來推動各種科學計畫，以簡單化約、工具性的現代化、單面利益論述建構生物辨識系統的好處，而這些端倪也反映在移民署通關辨識與外交部的晶片護照上。

【回應意見 11】

無修正意見。

【原文 12】(p236)

故若外交部、移民署仍然要強制辦理，是把國人當成白老鼠，如今新護照屆時能否趕上法律修正腳步、是否適用國內相關仍是疑問，然而巨額資金業已準備付出。

【回應意見 12】

無修正意見。

【原文 13】(p237)

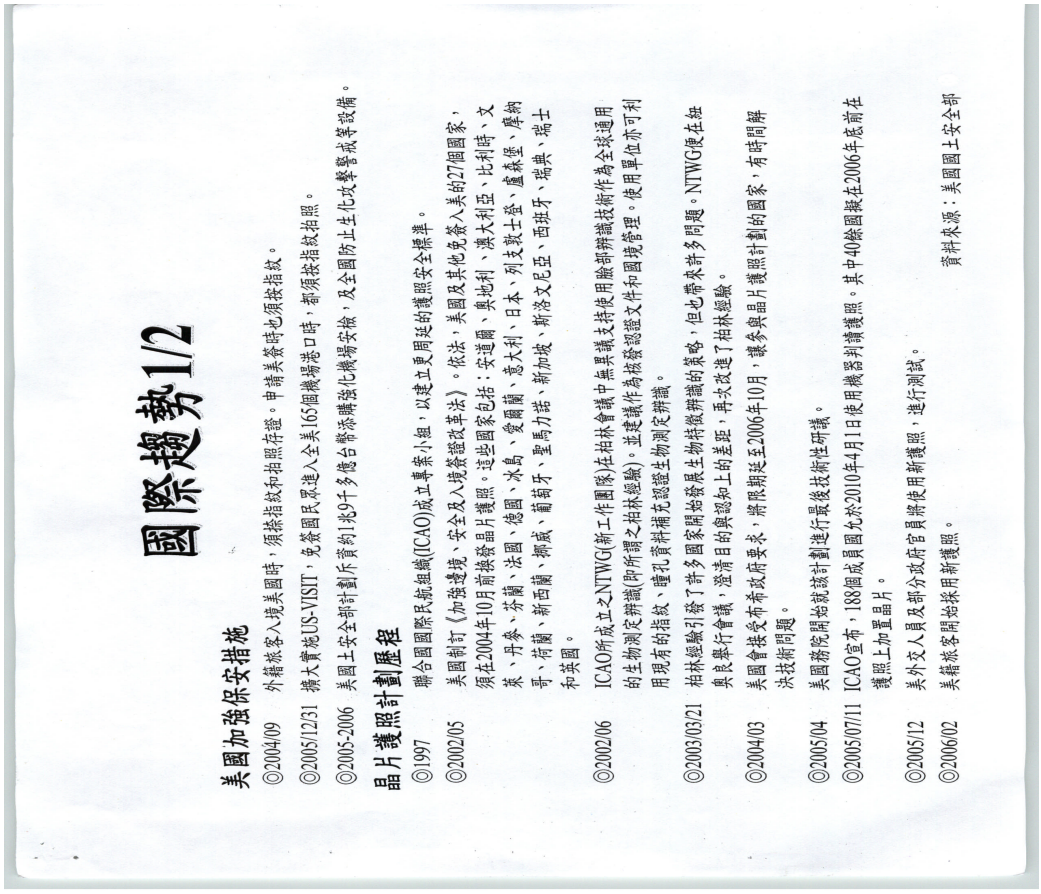
各國經常以立法來延宕科技風險的可能性，但在美國的生物辨識技術發展霸權與競爭放任之下，所有的社會風險的門檻紛紛失守。外交部、移民署等晶片護照與生物辨識機器的購買，類此涉及人民重大權利、義務的事項，政府應慎思明辨、決策應保守而謹慎，實不宜在未經國會充分討論、生物辨識科技法源尚在未定之天、及有公民審議程序、聽證程序、公民諮詢與公民會議等公共討論，經過多次且多元廣泛的風險溝通後，達到社會共識時，就動輒撒下龐大資金，讓備受爭議的新制上路，這樣的決策未免過於草率，欠缺謀定而後動的智慧，萬一生物辨識技術有違憲的爭議，在立法程序無法過關，那麼購置的設備豈不是浪費公帑？故從本旨研究建議，不應該在反恐的大論述底下，就冒然實施生物辨識技術、晶片護照等政策，否則將產生風險不可回復的後果。(p237)

【回應意見 13】

無修正意見。

附錄八

蔡震榮副署長於 4 月 3 日專家學者座談會所提書面資料



國際趨勢1/2

美國加強保安措施

◎2004/09　外籍旅客入境美國時，須採指紋和拍照存證。申請美簽時也須按指紋。

◎2005/12/31　擴大實施US-VISIT，免簽國民眾進入全美165個機場海口時，都須按指紋拍照。

◎2005-2006　美國土安全部計劃斥資約1兆9千多億台幣添購強化機場安檢，及全國防止生化攻擊警戒等設備。

晶片護照計劃歷程

◎1997　聯合國國際民航組織(ICAO)成立專案小組，以建立更周延的護照安全標準。

◎2002/05　美國制訂《加強邊境、安全及入境簽證改革法》。依法，美國及其他免簽入美的27個國家，須在2004年10月前換發晶片護照。這些國家包括：安道爾、奧地利、澳大利亞、比利時、文萊、丹麥、芬蘭、法國、德國、冰島、愛爾蘭、意大利、日本、列支敦士登、盧森堡、摩納哥、荷蘭、新西蘭、挪威、葡萄牙、聖馬力諾、新加坡、斯洛文尼亞、西班牙、瑞典、瑞士和英國。

◎2002/06　ICAO所成立之NTWG(新工作團隊)在柏林會議中無異議支持使用臉部辨識技術作為全球通用的生物測定辨識(即所謂之柏林經驗)。並建議作為核發認證文件和國境管理。使用單位亦可利用現有的指紋、瞳孔實辦補充認證生物測定辨識。

◎2003/03/21　柏林經驗引發了許多國家開始發展生物特徵辨識的策略，但也帶來許多問題。NTWG便在紐奧良舉行會議，澄清目的與認知上的差距，再次改進了柏林經驗。

◎2004/03　美國會接受布希政府要求：滯限期延至2006年10月，讓參與晶片護照計劃的國家，有時間解決技術問題。

◎2005/04　美國務院開始就該計劃進行最後技術性研議。

◎2005/07/11　ICAO宣布，188個成員國允於2010年4月1日使用機器判讀護照。其中40餘國擬在2006年底前在護照上加置晶片。

◎2005/12　美外交人員及部分政府官員將使用新護照，進行測試。

◎2006/02　美籍旅客開始採用新護照。

資料來源：美國國土安全部

國際趨勢2/2

- 比利時已於2004年成為歐洲第一個也是唯一的全面向公民發放電子護照的國家
- 德國內政部宣佈，從2005年11月1日開始，開始推行含有電子晶片加密儲存著護照持有者的數碼照片(生物特徵信息)的電子護照。從2007年3月開始，晶片還將儲存護照持有者的雙手指紋信息。歐盟25國以及美國、日本、俄羅斯、澳大利亞和瑞士將跟進
- 新加坡於2005年宣布，預計十月份啟用符合ICAO標準的生物認證護照，將成為亞洲第一個採用生物認證護照的國家，一方面符合美國的要求，另一方面亦遏止新加坡護照遭到變造濫用，有助國家安全
- 英國自2006年起將換發具有容貌生物辨識(biometrics)功能的護照與身分證(ID card)，到2009年另將併入指紋資料
- 中國大陸目前正與南韓、新加坡等亞洲國家聯手開發了電子護照認證系統，預計將在2008年北京奧運會前全面採用電子護照
- 澳大利亞政府將於今年10月23日起在全國推行使用一種使用RFID晶片儲存了持有者臉型、指紋等生物資訊的新式電子護照。護照內的晶片將以無線傳送的方式將晶片內數據輸入海關官員的電腦顯示屏，並可在瞬間驗證護照的真實性

壹、國際民航組織(ICAO) 電子旅行文件(MRTD)的標準

除了是MRP之外另加下列功能

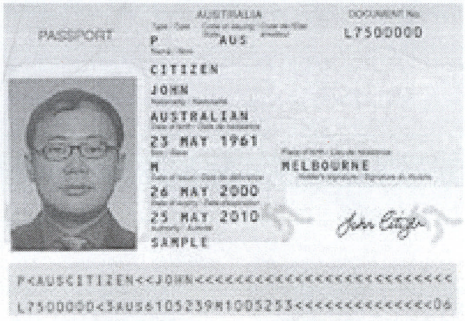
一、使用無線射頻識別系統(RFID)。

二、採用生物辨識系統(Biometrics)。

三、加密採用公開金鑰(PKI)。

12.5 cm

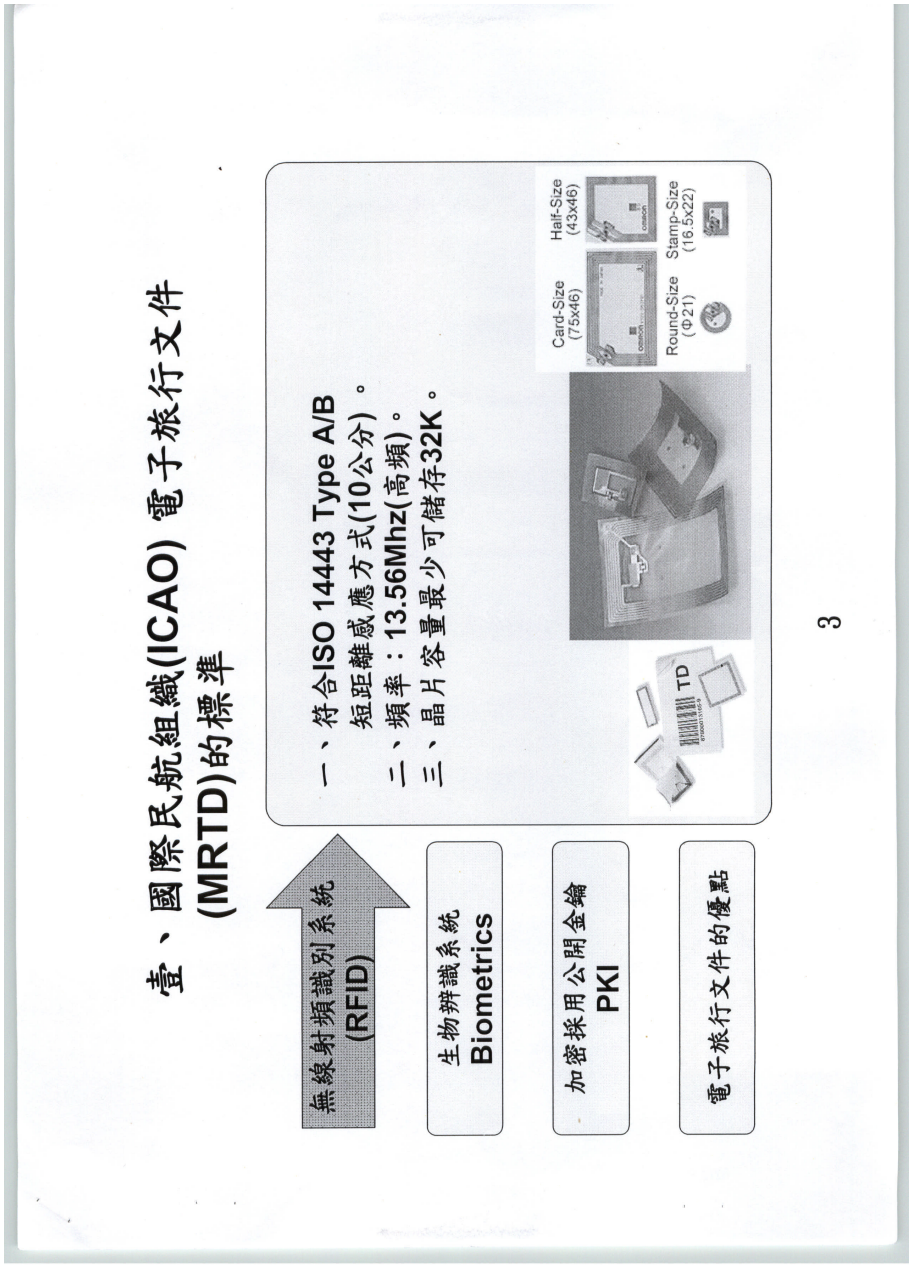
8.8 cm



卡片型態，發照地，英文姓名
護照號碼，國籍，出生日，性別，效期，個人號碼

RFID黏貼方式：
資料頁(首頁)或 文件中間或最後一頁

2


壹、國際民航組織(ICAO) 電子旅行文件(MRTD)的標準
無線射頻識別系統 (RFID)
一、符合ISO 14443 Type A/B
短距離感應方式(10公分)。
二、頻率：13.56Mhz(高頻)。
三、晶片容量最少可儲存32K。
Card-Size (75x46)
Half-Size (43x46)
Round-Size (Φ21)
Stamp-Size (16.5x22)
TD
生物辨識系統 Biometrics
加密採用公開金鑰 PKI
電子旅行文件的優點
3

壹、國際民航組織(ICAO) 電子旅行文件(MRTD)的標準

無線射頻識別系統
(RFID)

生物辨識系統
Biometrics

加密採用公開金鑰
PKI

電子旅行文件的優點

一、生物特徵：臉部(Face)為必要使用，指紋(Fingerprint)、虹膜(Iris)為選用。

二、生物辨識存放於RFID晶片所需容量：

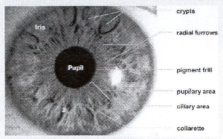
基本資料+臉部=32K

基本資料+臉部+2指指紋=64K

基本資料+臉部+2指指紋+2顆虹膜=128K

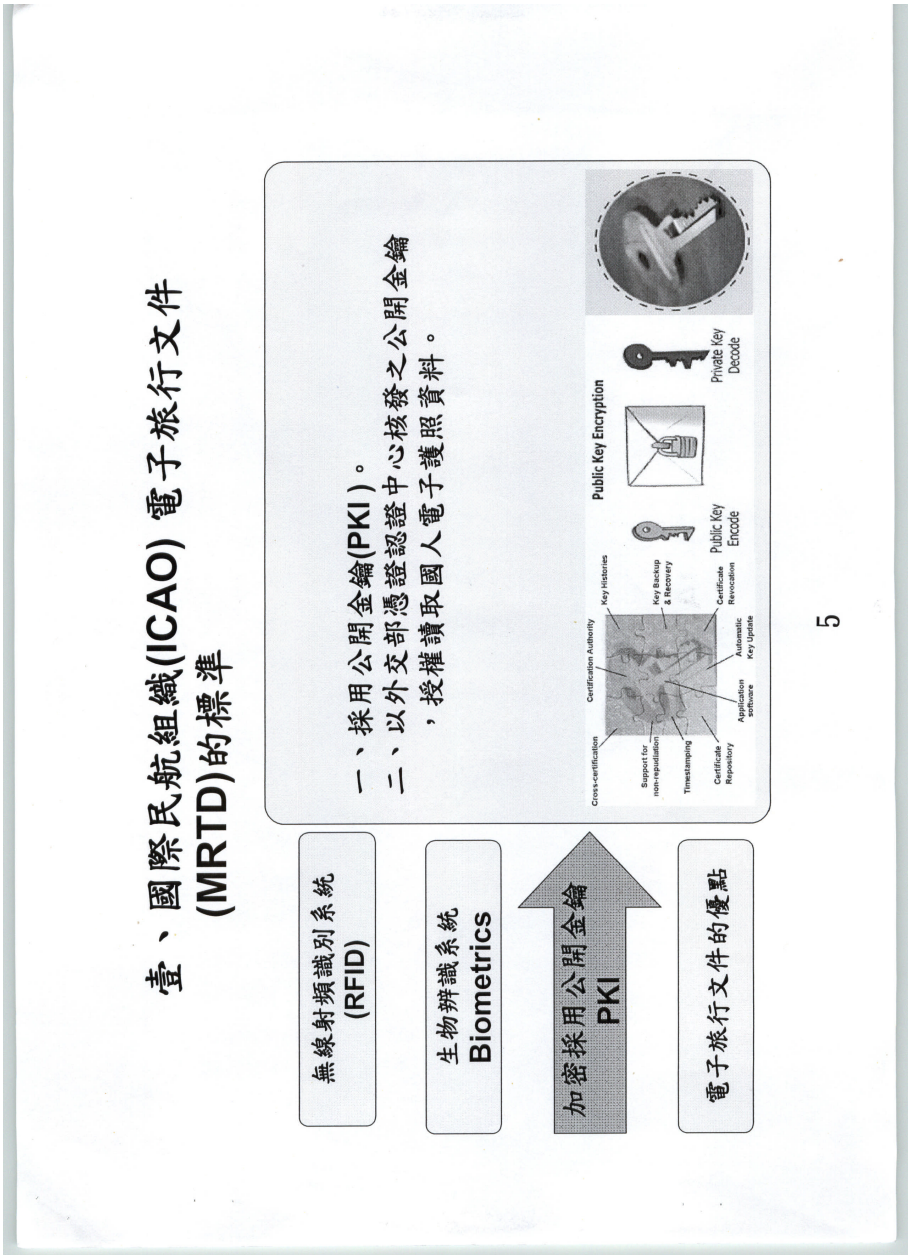
12K

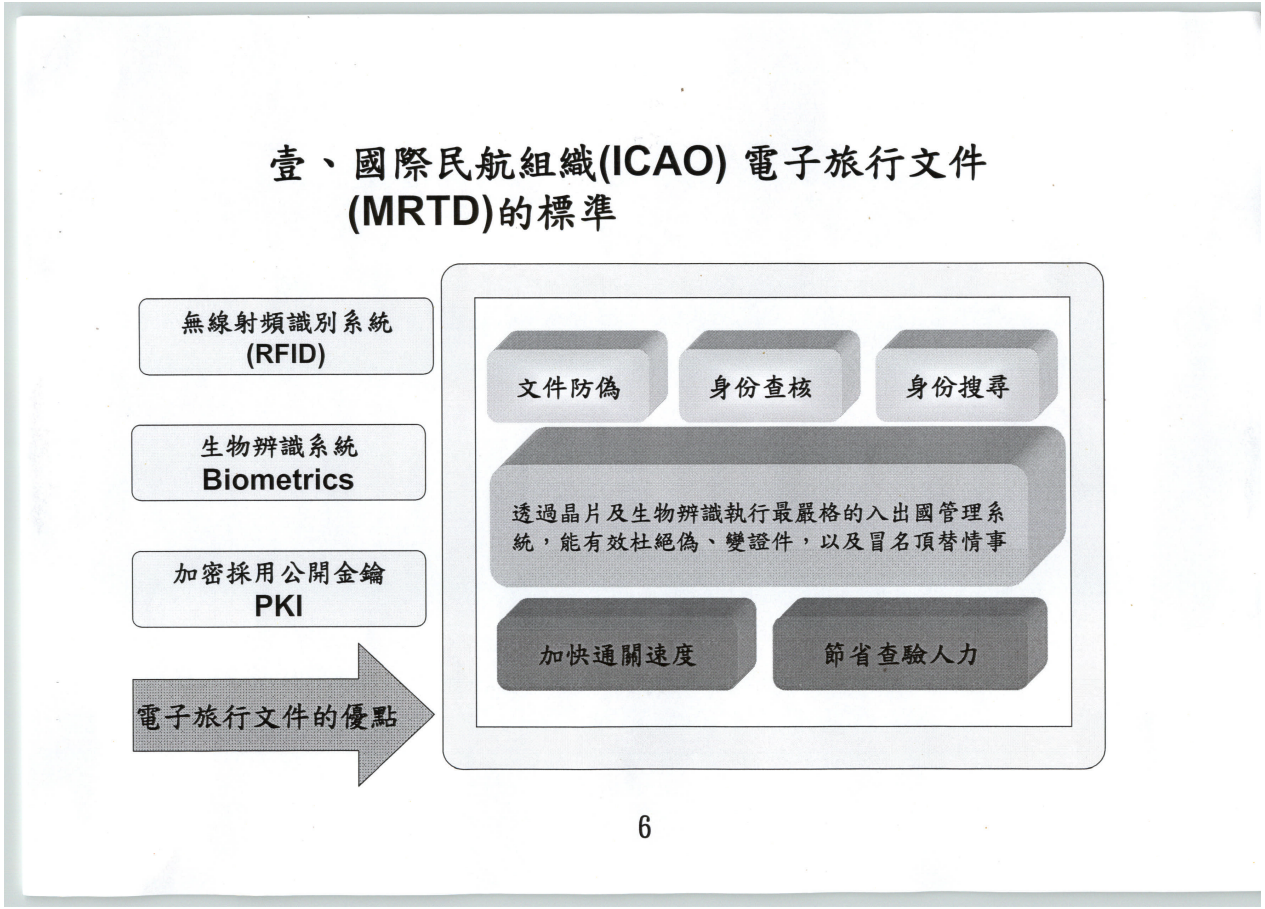
10K

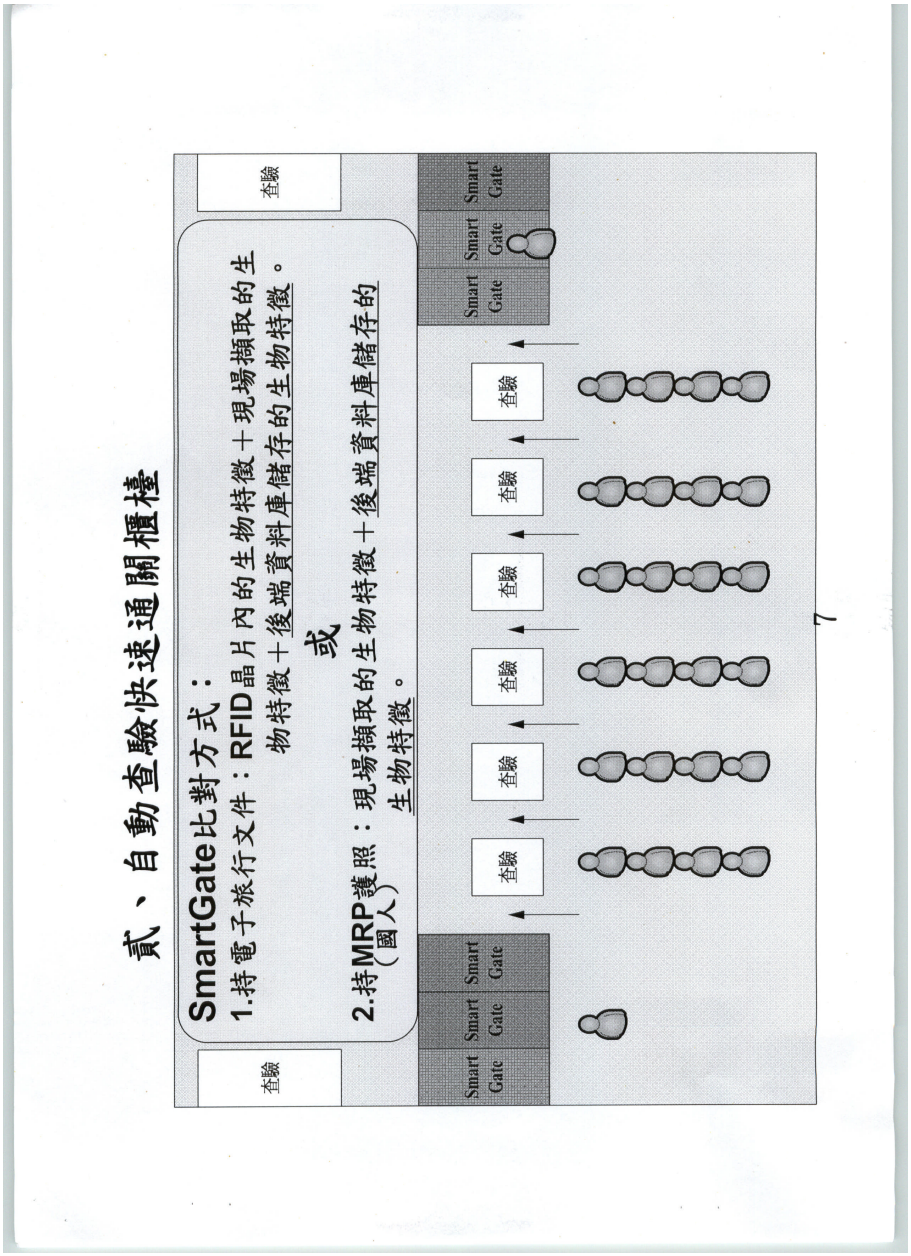


30K

4

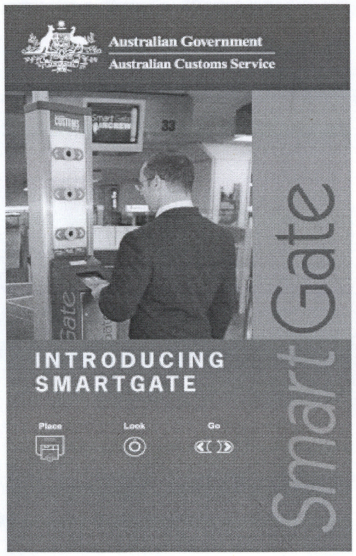

壹、國際民航組織(ICAO) 電子旅行文件(MRTD)的標準
無線射頻識別系統 (RFID)
生物辨識系統 Biometrics
加密採用公開金鑰 PKI
電子旅行文件的優點
一、採用公開金鑰(PKI)。
二、以外交部憑證認證中心核發之公開金鑰，授權讀取國人電子護照資料。
Public Key Encryption
Public Key Encode
Private Key Decode
Certification Authority
Key Histories
Key Backup & Recovery
Certificate Revocation
Automatic Key Update
Cross-certification
Support for non-repudiation
Timestamping
Certificate Repository
Application software
5


壹、國際民航組織(ICAO) 電子旅行文件(MRTD)的標準
無線射頻識別系統
(RFID)
生物辨識系統
Biometrics
加密採用公開金鑰
PKI
電子旅行文件的優點
文件防偽
身份查核
身份搜尋
透過晶片及生物辨識執行最嚴格的入出國管理系統，能有效杜絕偽、變證件，以及冒名頂替情事
加快通關速度
節省查驗人力
6


貳、自動查驗快速通關櫃檯
SmartGate比對方式：
1.持電子旅行文件：RFID晶片內的生物特徵＋現場擷取的生物特徵＋後端資料庫儲存的生物特徵。
或
2.持MRP護照（國人）：現場擷取的生物特徵＋後端資料庫儲存的生物特徵。
查驗
Smart Gate
7

貳、自動查驗快速通關櫃檯

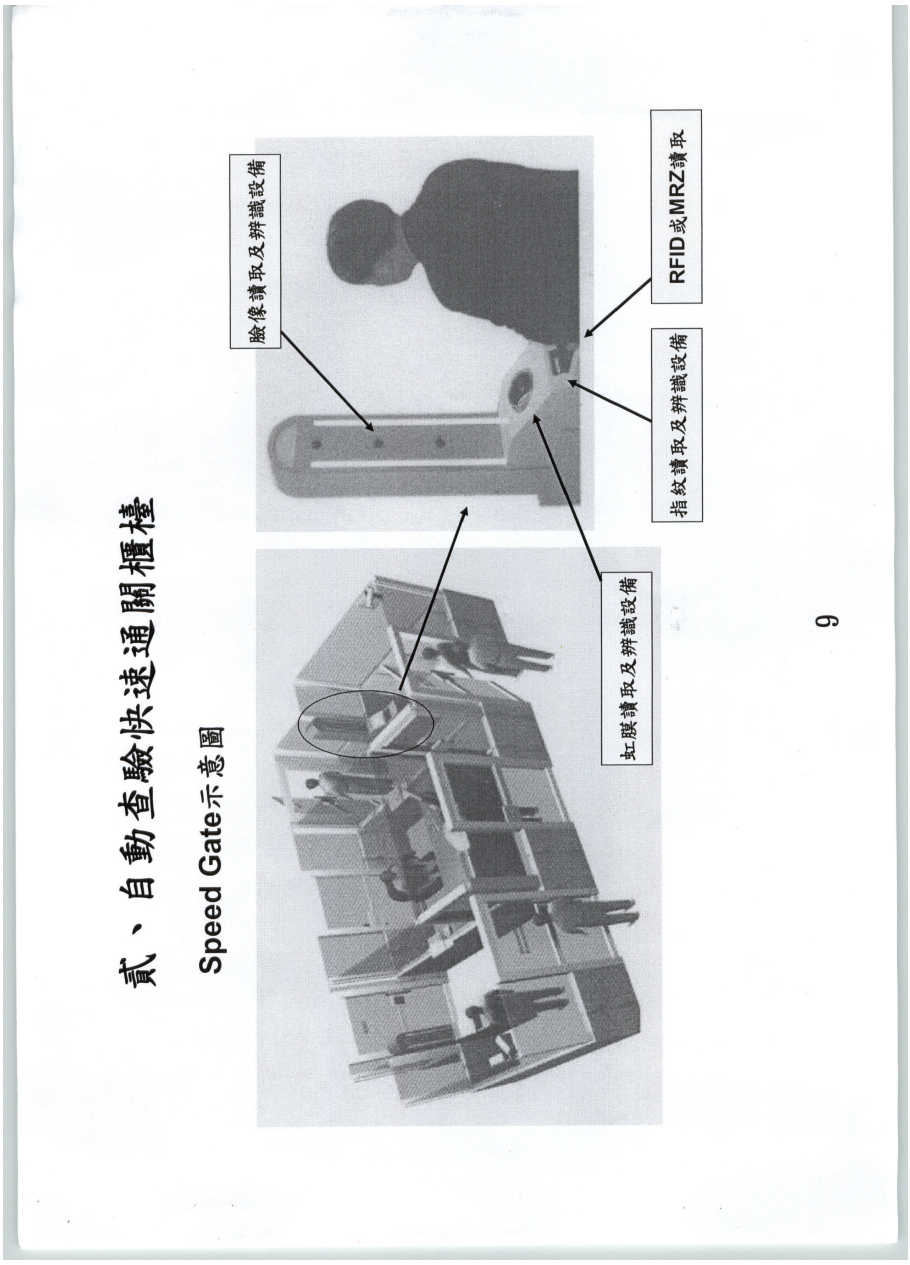
SmartGate示意圖



旅行文件的讀取方式：
一、RFID的感應
二、MRZ的讀取

生物辨識：
一、臉部

8

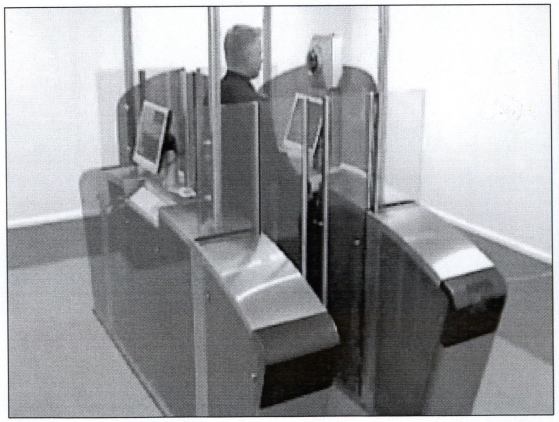

貳、自動查驗快速通關櫃檯
Speed Gate示意圖
臉像讀取及辨識設備
虹膜讀取及辨識設備
指紋讀取及辨識設備
RFID或MRZ讀取
9

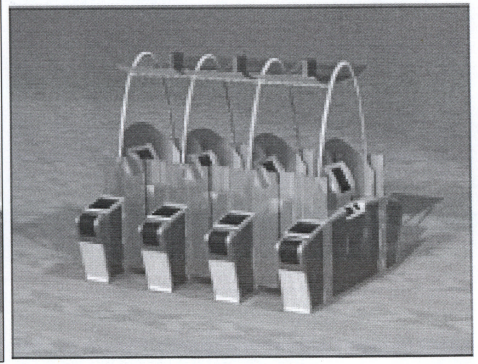
貳、自動查驗快速通關櫃檯

Security Gate示意圖

旅行文件的讀取方式：
一、**RFID**的感應
二、**MRZ**的讀取

生物辨識：
一、虹膜





10

P2：移民署成立之後，亦具體形成無論是短期入境觀光，大陸配偶來台長期居留，再入境通關之時，均須接受「按捺指紋、拍攝臉型、掃描虹膜」的三合一查驗身分政策。
說明：目前依法只針對大陸配偶進行「按捺指紋」查驗身分，並非媒體報導需進行三合一查驗身分。

P5：在大陸人士或其他外籍移住民入境時，都必須現場按指紋、攝取臉部影像和掃瞄虹膜等，進行比對。
說明：現行只針對大陸配偶(不含其他大陸人士或外人)進行指紋比對，並且未進行臉部及虹膜比對。

P9：用臉部辨識技術來處理護照真僞查驗的問題，其實可靠性不高，護照防僞如何設計，以及如何確定護照持有人和護照上的個人資料具有同一性，而不是將照片或臉部辨識技術這種應屬護照查驗中的輔助項目當做重點，或許才是癥結所在。
說明：查驗工作除驗證護照真僞外，同時需驗證旅客身分，照片或臉部辨識技術爲身分查驗重要的一環。

P194：晶片內除了儲存護照上各項基本資料，如護照本人電子檔，還有其各項生物特徵資料，如臉部特徵，未來還可能包括護照本人的指紋及虹膜等
說明：電子護照不存臉部特徵，只存臉部影像

P205：提及護照被複製及任意讀取之情境
說明：電子護照具備以下安全功能，若再安控上要求最高，需建置以下功能，經由其他安全技術降低風險

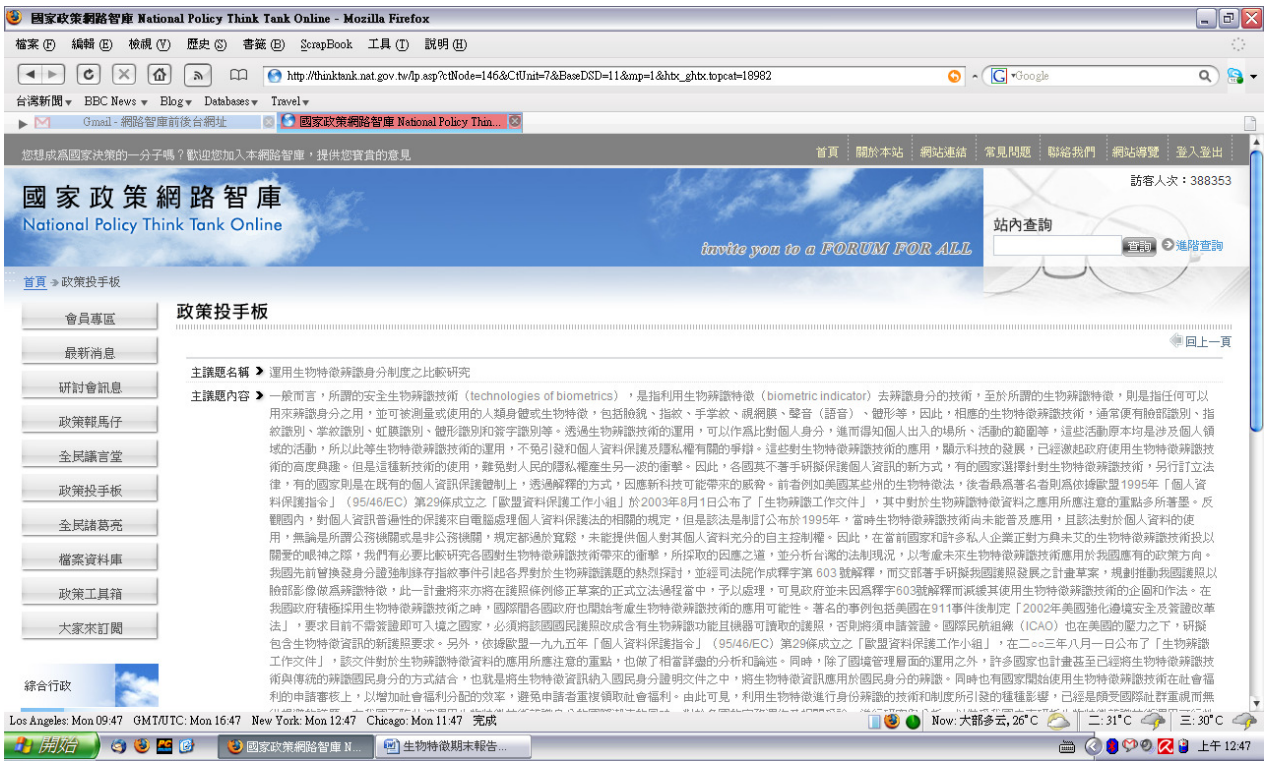
A.基本取控制功能(BAC)
-防止側錄及讀取晶片資料，但護照號碼有效日期、生日不可洩露
B.被動式驗証功能(PA)
-驗証資料(護照)爲合法核發且晶片內資料未被竄放
C.主動式驗証功能(AA)
-防止晶片被複製
D.強化存取控制功能(EAC)
-針對個人隱私資料進行加密處理，如指紋

附錄九

「國家政策網路智庫」運用情形

本研究案於九十六年四月初將本計畫之研究要點上網登載於「國家政策網路智庫」的「政策投手板」項目，供一般大眾閱覽，並得自由參與討論。惟並無任何任何民眾對本研究案提出評論，故本研究計畫報告之內容，仍以本研究團隊的研究所得爲主軸來發展。

運用生物特徵辨識身分制度之比較研究



參考文獻

中文資料

期刊

王郁琦，生物辨識技術對隱私權的影響，收於劉尚志主編，全國科技法律研討會論文集 2005 年，國立交通大學出版，頁 287-317。

李仁淼，再論強制按捺指紋之合憲性，月旦法學教室，2005 年 8 月，頁 8-9。

李建良，「戶籍法第八條捺指紋規定」釋憲案鑑定意見書，臺灣本土法學雜誌 73 期，2005 年 8 月，頁 38-56。

李惠宗，領取國民身份證按捺指紋違憲性之探討－從法學方法論評大法官釋字第六○三號解釋，月旦法學雜誌 126 期，2005 年 11 月，頁 172-186。

李震山，來者猶可追，正視個人資料保護問題－司法院大法官釋字第六○三號解釋評析，臺灣本土法學雜誌 76 期，2005 年 11 月，頁 222-234。

林燦都、傅美惠，按捺指紋措施之合憲性問題探討，法令月刊 56 卷 10 期，頁 12-32。

周桂田、張淳美，〈生物特徵、指紋資料庫風險〉，科學發展 398 期，2006 年 2 月。

周桂田，〈遲滯型高科技風險社會下之典範鬥爭:以換發身分證按捺指紋案爲分析〉，《政治與社會哲學評論》，第十七期。

周桂田，〈在地化風險之實踐與理論缺口 --遲滯型高科技風險社會〉，《台灣社會研究季刊》，2002 年 3 月號。

周桂田，〈知識、科學與不確定性－專家與科技系統的「無知」如何建構風險〉，《政治與社會哲學評論》，第十三期。

周桂田，〈爭議性之風險溝通-以基因改造工程爲思考點〉，《生物科技與法律研究通訊》，第十八期。

范姜真媺，按捺指紋與合憲性審查標準－以日本判例、學說爲主，律師雜誌，2005 年 8 月，頁 54-71。

徐正戎，「戶籍法第八條捺指紋規定」釋憲案鑑定意見書，臺灣本土法學雜誌 75 期，2005 年 10 月，頁 57-81。

詹鎮榮，請領國民身分證，先捺指紋，月旦法學教室，2005 年 7 月，頁 8-9。

顏厥安，戶籍法八條與全民指紋建檔合憲性問題之鑑定意見，臺灣本土法學雜誌 79 期，2006 年 2 月，頁 145-177。

陳瑞廣、刑事局指紋編輯室，〈好用的生物特徵：指紋身分辨識〉，《刑事雙月刊》，2005 年 5-6 月。

熊德仁，論全民指紋制度之合憲性問題，中央警察大學法律學研究所 91 學年度碩士論文。

劉億成，〈歐盟「護照及旅行證件生物辨識、檢測資料標準規則」之簡介〉，《科技法律透析》，2005 年 2 月。

其他

生物指紋辨識科技，盛泓科技股份有限公司，http://www.mold.net.tw/quint/organism.htm

李德財 2005 年 5 月 25 日於 tw.bbs.soc.taiwaneseg 對指紋案的意見，

http://groups.google.com.tw/group/tw.bbs.soc.taiwanese/browse_thread/thread/eaa9bfa4bcf43f82/541b22e9217d5dea?lnk=st&q=%E6%9D%8E%E5%BE%B7%E8%B2%A1&rnum=9&hl=zh-TW#541b22e9217d5dea

李德財 2005 年 5 月 25 日於 tw.bbs.soc.taiwaneseg 對指紋案的意見，http://groups.google.com.tw/group/tw.bbs.soc.taiwanese/browse_thread/thread/93c4aab22e4a21ae/14c2ea00759c670b?lnk=st&q=%E6%9D%8E%E5%BE%B7%E8%B2%A1&rnum=11&hl=zh-TW#14c2ea00759c670b

生物辨識認證卡解決方案，IDMethod，http://www.idmethod.com/s_biocard.html，參訪日期 2007/01//27

美國將在簽證作業採用生物辨識技術，科技法律要聞，http://stlc.iii.org.tw/tlnews/net9208.htm#top，參訪日期:2006.9.30

周桂田，高科技風險社會，http://bio.idv.tw/data/data2/2000010001.htm

周桂田，高科技風險社會，http://bio.idv.tw/data/data2/2000010001.htm

許耀明，預防原則與科學證據之前提：風險治理，http://www.iias.sinica.edu.tw/951216/951216_1_4.pdf

「晶片護照快易通?爭議多惹民怨」，中國時報，2007 年 1 月 15 日。

「電子護照 2010 年上路」，自由時報，94 年 7 月 13 日。

「機場生物辨識，七月啓用」，聯合報，96 年 4 月 19 日。

〈獨一無二 無可取代-生物辨識系統〉，《網際先鋒》，2001 年二月。

英文資料

書籍

ACKERMAN, BRUCE (2006), BEFORE THE NEXT ATTACK: PRESERVING CIVIL LIBERTIES IN AN AGE OF TERRORISM, New Haven: Yale University Press.

ALBRECHT, K. & MCINTYRE, L. (2005), SPYCHIPS: HOW MAJOR CORPORATIONS AND GOVERNMENT PLAN TO TRACK YOUR EVERY MOVE WITH RFID, Nashville: Nelson Current.

BOLLE, R. M. ET AL. (2004), GUIDE TO BIOMETRICS, New York: Springer.

BRIN, D. (1998), THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM?, Massachusetts: Perseus Books.

CHANG, NANCY (2002), SILENCING POLITICAL DISSENT: HOW POST-SEPTEMBER 11 ANTI-TERRORISM MEASURES THREATEN OUR CIVIL LIBERTIES, New York: Seven Stories Press.

COKE, TANYA E. (2003), RACIAL PROFILING POST-9/11: OLD STORIES, NEW DEBATE, IN LOST LIBERTIES: ASHCROFT AND THE ASSAULT ON PERSONAL FREEDOM, New York: The New Press.

DERSHOWITZ, ALAN M. (2002), WHY TERRORISM WORKS: UNDERSTANDING THE THREAT RESPONDING TO THE CHALLENGE, New Haven: Yale University Press.

EATON, JOSEPH W. (1986), CARD-CARRYING AMERICANS, Rowman & Littlefield Pub Inc.

ETZIONI, AMITAI (1999), THE LIMITS OF PRIVACY, Basic Books.

Galison, Peter & Minow, Martha (2005), *Our Privacy, Ourselves in the Age of Technological Intrusions*, *in* RICHARD ASHBY WILSON (ED.), HUMAN RIGHTS IN THE "WAR ON TERROR", Cambridge University Press, 2005.

FRUM, DAVID & PERLE, RICHARD (2003), AN END TO EVIL: HOW TO WIN THE WAR ON TERRORISM, Ballantine Books.

GARFINKEL, S. & ROSENBERG, B. (EDS.). (2006). RFID: APPLICATIONS, SECURITY, AND PRIVACY, Boston: Addison-Wesley.

HARPER, JIM (2005), IDENTITY CRISIS: HOW IDENTIFICATION IS OVERUSED AND MISUNDERSTOOD 1-7 (Cato Institute, 2005).

KEEFE, PATRICK RADDEN (2006), CHATTER: UNCOVERING THE ECHELON SURVEILLANCE NETWORK AND THE SECRET WORLD OF GLOBAL EAVESDROPPING, New York: Random House.

Kytle, Calvin (2004), *Gandhi's Story in South Africa, in* NATIONAL IDENTIFICATION SYSTEMS: ESSAYS IN OPPOSITION 255-63 (Carl Watner ed., 2004).

Moore, Bob (2004), *Population Registers in the Netherlands During World War II, in* NATIONAL IDENTIFICATION SYSTEMS: ESSAYS IN OPPOSITION 120-24 (Carl Watner ed., 2004).

POSNER, RICHARD A.(2006), NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL EMERGENCY, Oxford University Press.

ROSEN, JEFFREY (2004), THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIETY AGE, New York: Random House.

YOO, JOHN (2005), POWERS OF WAR AND PEACE: FOREIGN AFFAIRS AND THE CONSTITUTION AFTER 9/11, University of Chicago Press.

YOO, JOHN (2006), WAR BY OTHER MEANS: AN INSIDER'S ACCOUNT OF THE WAR ON TERROR, New York: Atlantic Monthly Press.

PERRIN, S. (2006), *RFID and Global Privacy Policy*, *in* S. GARFINKEL & B. ROSENBERG(EDS.), RFID: APPLICATIONS, SECURITY, AND PRIVACY, Boston: Addison-Wesley.

SARMA, S. (2006), *A History of the EPC*, *in* S. GARFINKEL & B. ROSENBERG (EDS.), RFID: APPLICATIONS, SECURITY, AND PRIVACY (pp. 37-55). Boston: Addison-Wesley.

SCHNEIDER, BRUCE, APPLIED CRYPTOGRAPHY 4-5 (1996).

SOLOVE, D. J. (2004), THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE, New York: New York University Press.

VOLLMER, BRIANNE CHRISTINE (2005), SURVEY: AN ASSESSMENT OF THE GENERAL PUBLIC'S FAMILIARITY, KNOWLEDGE, AND ATTITUDES TOWARDS RFID, BIOMETRICS, AND THE EPASSPORT, Washington, DC: Georgetown University.

VOLLMER, BRIANNE CHRISTINE (2006), BIOMETRICS, RFID TECHNOLOGY, AND THE EPASSPORT: ARE AMERICANS RISKING PERSONAL SECURITY IN THE FACE OF TERRORISM?, Washington, DC: Georgetown University.

WEINBERG, J. (2006), RFID, Privacy, and Regulation, in S. GARFINKEL & B. ROSENBERG (EDS.), RFID: APPLICATIONS, SECURITY, AND PRIVACY, Boston: Addison-Wesley.

Werth, Nicholas (2004), *The Russian Card: The Propiska, in* NATIONAL IDENTIFICATION SYSTEMS: ESSAYS IN OPPOSITION 116-19 (Carl Watner ed., 2004).

期刊

Crossman, Gareth & Mortimer, Caroline (2005), *ID cards--exposing criminality or invading privacy?*, NEW LAW JOURNAL, 9 December 2005.

Graham-Rowe (2005), Duncan, *Privacy and prejudice: whose ID is it anyway*, NEW SCIENTIST, 17 September 2005.

Ham, Shane, *Winning with Technology*, BLUEPRINT MAGAZINE, Jan. 2002.

Paraskeva, Janet (2004), *Chief Executive's Column: An Identity Crisis*, LAW SOCIETY GAZETTE, 22 April 2004.

Redmond, David (2005), *Licence to live?*, NEW LAW JOURNAL, . 24 June 2005

Rees, Phillip & Hughes, Marcus (2004), *Biometrics and border control*, NEW LAW JOURNAL, 13 August 2004.

Smith, Roger (2004), Rights And Wrongs: Registering Fears, Law Society Gazette, 17 June 2004.

其他

AsylumSupport.info, http://www.asylumsupport.info/about.htm

BIOMETRICS CATALOG, http://www.biometricscatalog.org/default.aspx

The Biometric Consortium, http://www.biometrics.org/

CHALLENGE: Liberty & Security (The Changing Landscape of European Liberty and Security), http://www.libertysecurity.org/

CSTB (The Computer Science and Telecommunications Board), http://cstb.org

EBF (The European Biometrics Forum),

http://www.eubiometricforum.com/

ECLN (European Civil Liberties Network), http://www.ecln.org/

EDRI (Digital Civil Rights in Europe), http://www.edri.org/

EFF (the Electronic Frontier Foundation), http://www.eff.org/about/

EPIC (The Electronic Privacy Information Center), http://www.epic.org/epic/jobs.html

EXPLANATORY NOTES TO IDENTITY CARDS 2006 (2006), *at* http://www.opsi.gov.uk/ACTS/en2006/2006en15.htm

EXPLANATORY NOTES TO IMMIGRATION, ASYLUM AND NATIONALITY ACT 2006 (2006), *at* http://www.opsi.gov.uk/acts/en2006/2006en13.htm

ICAMS （The International Campaign Against Mass Surveillance), http://www.i-cams.org/About_ICAMS.html

IBS (The International Biometric Society), http://www.tibs.org/about.html

JOINT COMMITTEE ON HUMAN RIGHTS, UK HOUSE OF LORDS & HOUSE OF COMMONS (26 January 2005), FIFTH REPORT OF SESSION 2004-05, *at* http://www.publications.parliament.uk/pa/jt200405/jtselect/jtrights/35/3502.htm

JOINT COMMITTEE ON HUMAN RIGHTS, UK HOUSE OF LORDS & HOUSE OF COMMONS (17 October 2005), FIRST REPORT OF SESSION 2005-06, , *at* http://www.publications.parliament.uk/pa/jt200607/jtselect/jtrights/26/2602.htm

Juels, A. et al. (2005), Security and Privacy Issues in E-Passports, Unpublished manuscript, Berkeley.

OECD (Organisation for Economic Co-operation and Development), http://www.oecd.org/home/0,2987,en_2649_201185_1_1_1_1_1,00.html

On the identity trail，http://idtrail.org/content/view/12/34/

PI (Privacy International), http://www.privacyinternational.org/

Privacy International, Mistaken Identity: Exploring the Relationship between National Identity Cards and the Prevention of Terrorism (2004).

Privacy.Org, http://www.privacy.org/index.html

SANS(SysAdmin、Audit、Network、Security), http://www.sans.org/vendor/expect.php

SCIENCE AND TECHNOLOGY COMMITTEE, UK HOUSE OF COMMONS (2006), SIXTH REPORT：IDENTITY CARD TECHNOLOGIES: SCIENTIFIC ADVICE, RISK AND EVIDENCE, *at* http://www.publications.parliament.uk/pa/cm200506/cmselect/cmsctech/1032/103202.htm

日文資料

アンソニー・ギデンス『国民国家と暴力』松尾精文ら訳、而立書房、1999 年。

アムネスティ・インターナショナル日本「国際法の観点から見た入管法改正案(政府案)」難民政策提言シリーズ NO.2 ，2003 年 5 月。

ジル・ドゥルーズ「追伸――管理社会について」『記号と事件』宮林寛訳、河出書房新社、1992 年。

デイヴィッド・ライアン『監視社会』河村一郎訳、青土社、2002年。

デイヴィッド・ライアン『9・11以後の監視――「監視社会」と「自由」』田島泰彦監修、清水知子訳、明石書店、2004年。

小熊英二『単一民族神話の起源――「日本人」の自画像の系譜』新曜社、1995年。

小倉利丸編『監視社会とプライバシー』インパクト出版会、2001年。

日本第164回国会衆議院法務委員会会議録第7号、第8号、第15号、第17号。

日弁連編『プライバシーがなくなる日』明石書店、2003年。

田島泰彦ら編著『住基ネット監視社会』、日本評論社、2003年。

田島泰彦ら編著『表現の自由とプライバシー――憲法・民法・訴訟実務の総合的研究』、日本評論社、2006年。

船越一幸『情報とプライバシーの権利――サイバースペース時代の人格権』北樹出版社、2001年。

藤乘一道「テロの未然防止のための規定の整備」『立法と調査』254号、2006年。

德文資料

Albrecht, Astrid: Biometrische Verfahren im Spannungsfeld zwischen Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, Reihe Frankfurter Studien zum Datenschutz, Baden Baden, 2003 (i.E)

Bäumler, Helmut/ *Breinlinger*, Astrid/ *Schrader*, Hans-Hermann (Hrsg.): Datenschutz von A-Z, Loseblatt, Neuwied, Kriftel, Stand: Juli 2002

Bäumler, Helmut/ *Gundermann*, Lukas/ *Probst*, Thomas: Stand der nationalen und internationalen Diskussion zum Thema Datenschutz bei biometrischen Systemen, Gutachten für den Deutschen Bundestag, vorgelegt dem Büro für Technikfolgenabschätzung beim Deutschen Bundestag, 2001

Breitenstein, Marco: Überblick über biometrische Verfahren, in: *Nolde*, Veronika/ *Leger*, Lothar (Hrsg.), Biometrische Verfahren, Körpermerkmale als Passwort, Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002, S. 35 bis S. 82

Busch, Christoph/ *Daun*, Henning: Frei von Zweifel?, Biometrische Erkennung: Grundlagen, Verfahren, Sicherheit, in: c't 5/2002, S. 156 bis S. 161

Calliess, Christian / *Ruffert*, Matthias (Hrsg.): Kommentar zu EU-Vertrag und EG-Vertrag. 2. Auflage, Neuwied 2002

Dammann, Ulrich / *Simitis*, Spiros: EG-Datenschutzrichtlinie, Kommentar, Baden-Baden 1997

Denninger, Erhard/ *Hoffmann-Riem*, Wolfgang/ *Schneider*, Hans-Peter/ *Stein*, Ekkehart (Hrsg.): Kommentar zum Grundgesetz für die Bundesrepublik Deutschland, Reihe Alternativkommentare, 3. Auflage, Neuwied/Kriftel, Loseblatt, Stand: 2001

Deutsche Vereinigung für Datenschutz (DVD): Stellungnahme „Terrorismusbekämpfungsgesetz und Ausländer" vom 15.11.2001 (abrufbar unter http://www.aktiv.org/DVD/Themen/teaus.html)

Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Biometrische Merkmale in Personalausweisen und Pässen, vom 07.03./08.03.2002, abrufbar unter http://www.datenschutzberlin.de/doc/de/konf/63/bio.htm

Filser, Hubert: Kontrollen im Grenzbereich - Ein neues elektronisches System soll Reisende an Flughäfen automatisch überprüfen -, in: SZ vom 11.03.2003, V2, S. 9

Fingerprint Verification Competion 2002. Ergebnisse abrufbar unter http://bias.csr.unibo.it/fvc2002

Frowein, Jochen Abr. / Peukert, Wolfgang: Europäische Menschenrechtskonvention, 2. Auflage, Kehl, Straßburg, Arlington 1996

Garstka, Hansjürgen: Terrorismusbekämpfung und Datenschutz – Zwei Themen im Konflikt, in: Neue Justiz 2002, S. 524 bis S. 525

Gemeinschaftskommentar zum Ausländerrecht: Loseblatt, Neuwied, Kriftel, Stand: 67. Aktualisierungslieferung, Juli 2002

Gola, Peter / *Schomerus*, Rudolf: BDSG Kommentar, 7. Auflage, München 2002.

Gundermann, Lukas / *Probst*, Thomas: Stichwort *Biometrie*, in: *Roßnagel*, Alexander

(Hrsg.), Handbuch Datenschutzrecht, München 2003.

Huber, Bertold: Die Änderungen des Ausländer- und Asylrechts durch das Terrorismusbekämpfungsgesetz, in: NVwZ 2002, S. 787 bis S. 794

Huber, Bertold (Hrsg.): Handbuch des Ausländer- und Asylrechts,

Loseblatt, München, Stand: 02/2002

Jarass, Hans D./ *Pieroth*, Bodo: Grundgesetz für die Bundesrepublik Deutschland, Kommentar, 6. Auflage, München 2002

Kilian, Wolfgang/ *Heussen*, Benno (Hrsg.) Computerrechts-Handbuch, Informationstechnologie in der Rechts- und Wirtschaftspraxis, München, Loseblatt, Stand: 15. September 2002

Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Auswirkungen des Volkszählungsurteils, in: DÖV 1984, S. 504 bis S. 510

Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Positionspapier zu technischen Aspekten biometrischer Merkmale in Personalausweisen und Pässen (Positionspapier –AKTechnik), abrufbar unter http://www.datenschutz.mvnet.de/beschlue/63biomet.html

Koenig, Christian/ *Lorz*, Ralph Alexander/*Lamprecht*, Rolf: Die Freiheit stirbt an ihrer Verteidigung, in: SZ vom 19./20. Januar 2002, Seite III

Medert, Klaus M./ *Süßmuth*, Werner: Paß- und Personalausweisrecht, Band 1: Personalausweisrecht, Band 2: Paßrecht, 2. Auflage, Köln 1992

Meyer-Ladewig, Jens EMRK-Handkommentar, Baden-Baden 2003.

NIST (National Institute of Standards and Technology) : NIST standards for biometric accuracy, tamper resistance, and interoperability. November 13, 2002; S. 21, abrufbar unter:http://www.itl.nist.gov/iad/894.03/NISTAPP_Nov02.pdf

Nolte, Martin: Die Anti-Terror-Pakete im Lichte des Verfassungsrechts, in: DVBl. 2002, S. 573 bis S. 578

Ohne Verfasser: Biometrik scannt Asylbewerber, in: Computerwoche 4/2003, S. 33

Ohne Verfasser: Eurodac, Aktuelles Lexikon, SZ vom 16.01.2003, S. 2

Ohne Verfasser: EU, Eurodac in Betrieb, in: DANA (Datenschutz Nachrichten), 1/2003, S. 23 bis S. 24

Ohne Verfasser: Bayern, Gesichtskontrolle per Computer, in: DANA (Datenschutz Nachrichten), 4/2002, S. 21

Ohne Verfasser: Rechtsprechung, AG Stuttgart, Beweisverwertungsverbot wegen unzulässigem automatisierten Lichtbildabruf, in: DANA (Datenschutz Nachrichten), 2/2002, S. 41 bis S. 42

Petermann, Thomas/ *Sauter*, Arnold: Biometrische Identifikationssysteme, Sachstandsbericht, TAB Arbeitsbericht Nr. 76, Februar 2002

Petri, Thomas Bernhard: Europol – transnationale polizeiliche Zusammenarbeit

in Europa, Baden- Baden 2001; zugleich Dissertation Frankfurt am Main 2000/2001

Phillips, P.J./ *Grothe*r, P./*Micheals*, R.J./ *Blackburn*, D.M./*Tabassi*, E./*Bone*, J.M: FRVT 2002: Overview and Summary, by P.J. Phillips, P. Grother, R.J Micheals, D.M.

Blackburn, E Tabassi, and J.M. Bone, März 2003

Face Recognition Vendor Test 2002: http://www.frvt.org/FRVT2002

Probst, Thomas: Anonymität und Pseudonymität bei biometrischen Identifikationsverfahren, in: *Bäumler*, Helmut/ *von Mutius*, Albert (Hrsg.): Anonymität im Internet, Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts,Braunschweig/Wiesbaden 2003

Ders. Biometrie aus datenschutzrechtlicher Sicht, in: *Nolde*, Veronika/ *Leger*, Lothar (Hrsg.), Biometrische Verfahren, Körpermerkmale als Passwort, Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002, S. 115 bis S. 128

Roggan, Frederik: Handbuch zum Recht der Inneren Sicherheit, Bonn 2003

Roßnagel, Alexander/ *Pfitzmann*, Andreas/*Garstka*, Hansjürgen: Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern, Berlin 2001

Schneier, Bruce: Angewandte Kryptographie, Bonn 1996

Schulte, Martin (Hrsg.): Handbuch des Technikrechts, Berlin, Heidelberg, New York 2003

Sietmann, Richard: Im Fadenkreuz, Auf dem Weg in eine andere Gesellschaft, in: c't 5/2002, S. 146 bis S. 155

Simitis, Spiros: Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung, in: NJW 1984, S. 398 bis S. 405

Simitis, Spiros (Hrsg.): Kommentar zum Bundesdatenschutzgesetz, 5. Auflage, Baden-Baden, 2003

Tinnefeld, Marie Theres/ *Ehmann*, Eugen: Einführung in das Datenschutzrecht, 3. Auflage, München, Wien 1998

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: Positionspapier zum Antiterrorgesetz der Bundesregierung vom 7. Dezember 2001, abrufbar unter: http://www.datenschutzzentrum.de/material/themen/divers/antiterr.htm

United States General Accounting Office: Technology Assessment : Using Biometrics

for Border Security Report GAO-03-174, November 2002 http://www.gao.gov/new.items/d03546t.pdf

Vogelgesang, Klaus: Grundrecht auf informationelle Selbstbestimmung?, 1. Auflage, Baden-Baden 1987

Weichert, Thilo: AZRG, Kommentar zum Ausländerregistergesetz, 1. Auflage, Neuwied, Kriftel 1998

Ders.: Datenschutz für Ausländer ... nach dem 11.September, in: DuD 2002, S. 423 bis S. 428

Ders.: Automatisches Fingerabdruck-Identifizierungssystem – AFIS, in: DuD 1999,

S. 167 bis S. 167

Ders.: Die Wiederbelebung des Personenkennzeichens – insbesondere am Beispiel der Einführung einer einheitlichen Wirtschaftsnummer, in: RDV 2002, S. 170 bis S. 177

Ders.: Biometrie – Freund oder Feind des Datenschutzes?, in: CR 1997, S. 369 bis S. 375

Woodward, John D.: Biometric Scanning, Law & Policy, Identifying the concerns – drafting the Biometrics Blueprint, University of

Pittsburgh Law Review, 1997

Woodward, John D.: Identifying Law & Policy Concerns, in: Jain, Anil/Bolle, Ruud/Pankati, Sharath, Biometrics, Personal Identification in Networked Society, Norvell 1999, S. 385 bis 405

Ziegler, Peter-Michael: Adlerauge, Europas größte Gesichtserkennungsanlage im Zoo Hannover, in: c't 2003, S. 26 bis S. 28

EG-Verordnung über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten
http://www.bmi.bund.de/cln_028/nn_1084010/Internet/Content/Common/Anlagen/Themen/PaesseUndAusweise/Biometrie__ePass__EU__VO,templateId=raw,property=publicationFile.pdf/Biometrie_ePass_EU_VO.pdf

Passgesetz (PassG)
http://www.bmi.bund.de/cln_028/nn_1084010/Internet/Content/Gesetze/P/PassG.html

Allgemeine Verwaltungsvorschriften zur Durchführung des Passgesetzes (PassVwV)

http://www.bmi.bund.de/cln_028/nn_1084010/Internet/Content/Common/Anlagen/Themen/PaesseUndAusweise/PassVwV,templateId=raw,property=publicationFile.pdf/PassVwV.pdf

Terrorismusbekämpfungsergänzungsgesetz vom 5. Januar 2007 (darunter Artikel 7b Änderung des Passgesetzes) BGBl. 2007 Teil I Nr. 1

http://www.bmi.bund.de/cln_028/nn_1084010/Internet/Content/Common/Anlagen/Themen/PaesseUndAusweise/Artikel__7b__Aenderun

g__des__Passgesetzes,templateId=raw,property=publicationFile.pdf/Artikel_7b_Aenderung_des_Passgesetzes.pdf

Gesetz über Personalausweise (PersAuswG)
http://www.bmi.bund.de/cln_028/nn_1084010/Internet/Content/Gesetze/P/PersAuswG.html

Verordnung zur Bestimmung der Muster der Personalausweise der Bundesrepublik Deutschland (PersAuswMustV)
http://www.bmi.bund.de/cln_028/nn_1084010/Internet/Content/Gesetze/P/PersAuswMustV.html

Bundesministerium des Inneren: Fragen und Antworten zum ePass
http://www.bmi.bund.de/cln_028/nn_1084000/Internet/Content/Themen/PaesseUndAusweise/Einzelseiten/Biometrie__FAQ.html

Chaos Computer Club e.V.: Der neue elektronische Reisepass
http://www.ccc.de/epass/