釋字第 603 號解釋部分協同部分不同意見書

余雪明大法官　提出

本席對多數意見認為國家蒐集指紋，應符合一定憲法上標準之原則，表示贊同。但認為只須符合「重要公益」目的即可，不必用最嚴格之「重大公益目的」。至其認為戶籍法第八條第二、三項違憲一節，則難苟同。多數意見以窄化立法目的，排除可能構成「重大公益」目的之治安等目的，將政府利益降級，再在利益衡量上將指紋可能之效益即避而不談或輕描淡寫，可能之風險則誇大其詞，並有意忽略指紋比姓名、相片更能精確建立本人同一性之特質，及否定其目的手段間之密切關聯性，而達成其不合比例原則之結論，造成明顯偏頗之印象，令人遺憾。本席以為指紋本身與隱私權無涉，依 1983 年德國聯邦憲法法院戶口普查法一案建立之" 資訊自決權 "，其法意亦不及於指紋。合理從立法史認定戶籍法第八條第二項之立法目的包括「治安之維持」，以及承認指紋比對確認身分可以避免極多之經濟及精神上之損失，以及指紋在同等效力之辨識工具中之不可取代性，當可輕易通過不同標準比例原則之檢驗而合憲。至於戶籍法第八條第三項，因身分證事實上用途廣泛，不予發給可能影響國民之參政權及生活之方便性，應受較嚴格之審查，本席以為可依合憲性解釋之原則，在限縮解釋為政府有發給同等效力之身分證明文件義務後合憲。茲說明其理由如次：

隱私權之概念及發展

隱私權的概念，源自美國侵權行為法，其經判例承認，可得請求救濟之隱私權侵害類型包括：未經同意，為謀財物或其他利益而利用他人之姓名或肖像（right of publicity）；對他人私密或其他利益為不合理並高度令人厭惡之侵入（intrusion of seclusion)；不涉公眾正當知之權利而揭露他人私事，至其極為不快（public disclosure of private facts）；或明知或可得而知之不實陳述使他人蒙羞（false light in the public eye）

（註一）。其後美國最高法院並自美國憲法增補條文第九條（人民保有之其他權利不因憲法列舉若干權利而受影響）等引伸出憲法對若干個人私密領域之直接保障，包括個人對婚姻、生育、避孕、家庭、養育兒女及教育等之自主決定權（註二）。德國隱私權之建立，則源於基本法第一條（人性尊嚴不可侵犯）與第二條第一項（人人有自由發展其人格的權利，但以不侵犯他人之權利，或不違反憲政秩序或道德規範者為限），其內容雖與美國大抵相當，但隱私權憲法化，故其位階較高。加以特殊之歷史背景，在利益權衡上其份量往往高於言論自由，此於美國言論自由在憲法天秤地位較高者不同。人格權雖與人性尊嚴相提並論，但前者之應用以其他憲法條文並無明定者為限（註三）。

由於資訊自動化處理時代之到來，個人資訊被公私機構大規模蒐集、處理與利用不同資訊之整合可以組成不同性質之個人簡介，個人對其正確性及使用幾無從控制，對其自主決定造成心裡壓迫而影響其人格發展之條件，於是從傳統之隱私權發展出資訊隱私權（或資訊自決權）以規範個人資訊之蒐集、儲存利用與移轉（註四）。就其消極面向而言，資訊隱私權可以阻止或限制某些敏感個人資訊之收集或利用。就其積極面而言，可以增進個人自主決定生活之選擇或參與政治制度或社會政策之決定而免於心理壓力之能力。在以服務為導向之資訊社會下，公私機構對個人資訊之自動化處理亦無從避免，縱屬可能影響個人自主決定之敏感資訊（註五），如顯示種族來源、政治意見、宗教或哲學之信念、工會之參與以及涉及健康及性生活、犯罪或被指為犯罪之個人資訊，亦非當然不得蒐集、處理、利用或公開，只是增加限制條件或加強保護而已。如私人醫學資訊對醫生、醫院員工、保險公司及公共健康相關機構之公開，為現代醫學實務之所必要，縱因此影響外界對病人之觀感亦不得不然。又如國家固不得未經同意收集個人政治、哲學、宗教信念之資訊，但相關團體因為正當活動對其成員資訊之處理，在適當保障下，自非法所不許。

美國模式

各國對資訊隱私權之保護，美國與歐洲聯盟採用不同之模式。美國除上述自憲法增補條文第九條等所引出之憲法直接對個人私密領域之保障外，復自人權宣言引伸出私密結社自由以及憲法增補條文第一條引伸出表意結社自由，以禁止政府取得敏感性之社員資訊（如為增進少數民族利益之社團）；自憲法增補條文第四條（禁止不合理之搜索與扣押）發展出〝合理隱私預期〞之概念，作為行使隱私權之門檻，保障個人不受政府對其私人事務之監督與入侵。此種片段與局部之保障，留下廣大之立法形成空間。美國對於個人資訊之收集與運用之限制，就聯邦、州與不同之領域，有極多不同之專法規定，其中較具一般性之聯邦法則有 1974 年之隱私權法與資訊自由法，前者規範部分政府機構對個人資訊之收集與使用，後者則為第三人對政府控制資訊請求提供之相關規定（註六）。

1977 年美國最高法院 Whalen v. Roe 一案（註七），為美國隱私權之重要判例。該案涉及紐約州之法律規定為防止濫用，醫生所開處方如涉及某些危險藥品（如鴉片及其製品，古柯鹼、沙酮等）應集中電腦建檔，其內容應包括醫師、藥局、藥名及份量，以及病人之姓名、地址及年齡。建檔後原始處方保留一定年限後即予以銷毀。法律並禁止病人的姓名外洩。最高法院認為該法為州警察權合理之行使。至於原告主張該法侵犯其憲法保障之隱私權領域，法院指出，除受憲法增補條文第四條保障之個人不受政府對其私人事務之監督與入侵以外，個人尚有兩種不同之隱私利益：其一為避免個人事務之公開（non-disclosure interest or informational seclusion），其二為對若干重要決定之自主決定之利益（主要指對婚姻、家庭、生育、子女教養等）。對於原告主張資料之可能外洩影響其名譽，致部分醫生或病人不敢對此等藥品為使用或處分，因而影響健康一節，法院認為決定權仍在醫師及病人，事實上仍有每月上萬之處方，故此種潛在之影響尚不構成違憲，

亦無任何證據認為有關安全之規定不被適當執行。雖然法院指出為公共目的收集及使用資訊其附隨之義務為避免資訊之不當外洩。

1974 年通過之隱私權法規定政府專業行政機構對個人資訊之儲存限於有相關（relevant) 及必要（necessary）（註八）者；儘量向本人（subject individual）收集資料（註九），紀錄應力求正確與完整（註十）；建立適當之行政與技術保安措施以確保紀錄之安全（註十一）；並對紀錄公開之條件作詳細之規定（註十二）。該法雖原則禁止未經紀錄涉及之個人書面請求或同意之公開，但有十二項豁免之規定（註十三）。其中包括對所有聯邦執法機關之揭露，其次為對政府有關部門及國會之揭露。而應用最廣之豁免則為：例行性之使用（routine use）（註十四）。但此種應用應與其原始收集之目的「相容」（compatibility），對涉及之本人有事實上之通知（actual notice），及對擬議之例行性使用在聯邦公報（federal register）上公開。不過實務上應用寬鬆（註十五）。法院在該法之權限為許當事人獲悉其紀錄，修正其錯誤及在一定條件下獲得損害賠償（註十六）。

資訊比對（Data matching）是對兩個以上紀錄做電子比較以發現在一個以上資料庫記載之個人。在 1988 年通過之電腦比對及隱私保護法（Computer matchingand Privacy Protection Act）修改隱私權法對比對增加額外之程序限制，如須提供（source agency）與收受機構（recipient agency）須先訂書面協議，比對前應做成本效益分析。且各機構應先設立「資訊確保處」（Data Integrity Board）。在比對後如對個人擬採不利措施（adverse action），機構之官員應先作獨立之查證（independent verification）；或如資訊限於給付（benefits）之指明與金額，對提供之資訊正確性有高度信心，機構應通知本人事實之認定，並予本人對其正確性提出異議機會（註十七）。

資訊自由法為提高政府之透明度容許一般公眾對政府控制之資訊請求公開，與隱私權有互補性。資訊自由法有九項豁免公開之規定，

相關政府機構可據以拒絕公開（註十八）。兩法之間的關係如下：如資訊自由法規定應公開者，隱私權法不得禁止之；如資訊自由法不強制公開，而第三者要求個人資訊，政府機構得依隱私權法不予公開；如資訊自由法未規定應公開而本人要求該資訊，隱私權法可命其對本人公開。縱某等資訊不便對其本人公開，仍應分離合理部分予本人。由於資訊自由法重點在政府之活動，純個人資訊不得對第三人公開（註十九）。

在資訊使用之監督方面（Oversight of Data Use）隱私權法建立內部（Internal）及外部（external）之監督機制。各機構應指定職員擔任「隱私權法官員」（Privacy Act Official）評估該機構遵守隱私權法之情形。此外依電腦比對及隱私權保護法各機構之首長應指定高級職員擔任「資訊確保處」（Data IntegrityBoard）之成員檢討機構內部資訊比對之活動。在實務上因為資源不足，相關人員缺乏獨立性，故僅為事務性之查核而已。至機關外之監督則為管理及預算局（Office of management and Budget）及國會之委員會。後者依隱私權法（註二十）收到各機關對紀錄體系建立及修改之擬議通知，實務上僅眾議院之政府運作委員會（House Committee on Government Operation）下之政府資訊小組委員會（sub-Committeeon Government information）對其持續監督。管理及預算局則對資訊使用之政策架構發出指導原則（Guidelines）與通知（circulars），其關切主要是資訊使用之效率，對資訊保護著力不多（註二十一）。

歐盟模式

在歐盟方面，德國聯邦憲法法院之判決中與資訊隱私權較有關係者，有 1969 年之 Microcensus case（註二十二）及 1983 年之 Census Act case（註二十三）。在 Microcensus 案中聯邦普查法原規定定期收集戶口及僱用之統計資料。1960 年之修正並收集居民之旅遊資訊。該案原告拒絕提供資訊被罰一百馬克，而提起憲法訴訟主張私人資訊之強

制揭露違反基本法第一條人性尊嚴之規定。法院指出此規定並未違反基本法第一條或第二條第一項。人性尊嚴在基本法價值體系之頂端，政府不得在第二條第一項容許之範圍外加以限制，以保障每一公民不受侵犯之隱私領域。政府如將「人」視為「物」而對其所有相關資訊清查即違反人性尊嚴。政府必須保留個人隱私之領域為其人格自由發展之空間。但並非所有涉及個人資訊揭露之統計調查均違反個人尊嚴或侵害其私領域之自決權，作為社會之一員由於該等資訊為政府計劃所必要，人人均應回應官方之普查，並答覆有關個人之問題。如官方調查只涉及個人與外界世界之關係，一般而言並不侵害個人隱私。如資訊因其隱名性而喪失個人特質時尤然。此結論前提為隱名性獲充分保障。本案中法律禁止所獲資訊之公開，並規定普查員之保密義務，且無義務向國稅局提供資訊。如無法律明文許可，負責官員亦不得以任何普查資訊向其上級報告。本案問卷雖涉及私領域，但並未強求個人揭露其私生活之隱密細節，亦未容許政府監視不涉外界之個人生活。政府雖可不透過普查而取得旅遊之地點、長度、旅社及交通資訊，但將非常困難。所要求之資訊並未涉及政府不得介入之最私密空間，因此政府自得使用該統計問卷而不違反個人之尊嚴或自決權利。

1983 年之「人口普查法」案更建立了一個新之「資訊自決權」。1983 年 4 月 13 日，聯邦憲法法院以暫時處分停止 1983 年聯邦普查法之執行。同年 12 月 15 日，該院認該法多數條文合憲，但要求國會修改若干條文，以去除可能導致個人資訊之收集、儲存、使用、移轉之濫用。其結果為人口普查因而延展四年。該法規定全國人口統計及社會結構詳盡資料之收集。除人口統計及個人基本資訊之收集外（如姓名、地址、性別、婚姻狀態、宗教信仰等）個人並應填寫詳細之問表答覆所得來源、職業、額外工作、教育背景、工作時間、工作往來之交通方式及其他相關事宜。法條並規定統計資訊移轉於地方政府以從事區域計劃、調查、環境保護與選區之劃分。由於該法涉及對基本權

之立即侵害、該院免除須窮盡法律救濟之要件，在超過一百人申請下，該院暫時停止該法之執行、理由為將該等資訊移轉與若干行政單位涉及隱私及人格權之侵害可能。該院在判決中指出，依基本法第一條及第二條第一項之人格權包括個人決定涉及個人生活之資訊在何時，以及在何限度內得以揭露之權。由於自動化資訊處理之現狀及將來可能之發展，個人之決定權須受到特別保護。處理個人資訊之技術方法幾無限度，而此等資訊可在極短時間內不論距離而尋獲。而不同資料之整合可以組成個人之簡介（personal profile），而個人對其正確性與使用無從控制，資訊取得之可能性及其影響力之增加可對個人造成心理壓力而影響其行為為人格自由發展之條件，個人應受保護以避免個人資料之無限收集、儲存、使用與移轉。但「資訊自決權」並非無限制，人並非個人資訊之絕對主人。人在社會中發展，個人資訊無非社會現實之反映，而不能單獨與個人連結。基本法為解決個人與社會之緊張而鋪陳出一個與社群相關並與社群結合之個人。個人原則上應因「重大之公共利益」（Compelling public interest）而接受對其個人資訊自決權之某些限制。如聯邦統計法第六條第一項所承認，基本法第二條第一項要求立法者明確規定所有官方資訊收集過程之目的及條件使公民能明白資訊收集之種類及原因。立法者並應遵守比例原則，使對基本權之限制在公共目的之必要程度內。考慮資訊處理的可能危險，立法者有義務在組織上及程序上採必要措施保障個人之人格權不受侵害。

基於上述原則，法院肯定人口普查用於社會計劃及「滿足公共任務（fulfillment of public tasks）」之正當性。法院審查資訊收集之性質、儲存及傳輸之方式，及其特定用途後肯定多數條文之合憲性，但認為普查政策應分辨可個人化之資訊及純統計目的之資訊。如自動化處理及其他地方機關分享造成特定個人「人格形象（personality profiles）」之重建與揭露，則人格權可能受到侵害。被認為違憲之條文最重要者為容許地方機關比較若干普查資訊與當地之房屋登記（housing

registery）資料比對。統計資訊與個人化之登記資料可能導致特定個人之曝光而侵害核心之人格權。由於某些資料非實現地方機關目的之必要，該規定並有違明確性原則與比例原則。

1995 年之歐盟個人資訊保護指令(註二十四)，可謂具體落實上述 1983 年德國憲法法院普查法判決之憲法上要求。該指令前言（２）指出資訊處理系統應為人服務，故需尊重基本人權及自由，尤其是隱私權，並有助於經濟及社會之進步、貿易之發展及個人之幸福，指令第六條規定個人資訊之處理應公平、合法；為特定、明確正當目的而收集，其處理亦應與此等目的相容。為歷史統計及科學目的之處理如有充分之保障不視為不相容；與收集及處理之目的足夠，相關而不過當；正確，於必要時，保持其正確（keep up to date）；在考慮收集及處理之目的後採合理步驟使不再正確或完整之資訊更正或消除；能顯示資訊主體而保存之時間應不超過其目的所需。如為歷史、統計或科學用途而將個人資訊保留更長時間時，應有適當之保障規定。控制者（有權決定個人資訊處理目的及方式之人）有義務確保此規定之遵守。第七條規定個人資訊須於合乎下列情形之一時方得處理：(a)資訊主體(即與資訊有關之特定人）之明確同意；(b）為履行契約之必要而資訊主體為契約之一方，或為因資訊主體在訂約前之請求而採之步驟；(c）為履行控制者之法律義務；(d）為保護資訊主體之重大利益；(e）為公共利益處理事務之必要或為控制者或被揭露資訊之第三人行使公權力；(f)為控制者或被揭露資訊之第三人之正當利益之必要，但如為保護資訊主體的基本權之最高利益時不在此限。第八條規定禁止處理敏感資訊之原則及其例外。該條第一項規定之敏感資訊為顯示種族來源、政治意見、宗教或哲學之信念、工會之參與之個人資訊，以及涉及健康、性生活者。第二項規定之例外包括資訊主體之同意，但法律另有規定者不在此限；為控制者行使或履行其在雇佣法規之權利或義務之必要；當資訊主體因實體或法律原因無法表示同意時，而為保護資訊

主體或他人重大利益之必要者；為政治、哲學、宗教、工會團體之正當活動而只涉及其成員或經常接觸之對象，且未經資訊主體同意，不揭露該資訊於第三者；資訊已經資訊主體公開或為對請求權（legal claims）建立行使或抗辯之必要者。第三項規定之例外為預防醫學、醫學診斷、照護之提供、健康服務之管理以及醫護從業人員（health professional）而依法有守密義務者，第四項規定會員國得於第二項以外，基於重要公共利益，以法律或主管機關之規則，增加豁免之規定。第五項規定犯罪，刑事處分或安全措施、行政罰、民事案件之判決等資訊之處理限於官方為之。第六項規定依第四、五項而不適用第一項之情形應通知執委會。第七項規定會員國有權決定國民身分號碼（National Identification Number）或其他一般應用之辨識工具（identifier）處理之條件。

第十三條規定豁免與限制。第一項規定會員國得以法律限制第六條第一項（資訊品質，見前）第十條（自資訊主體收集資訊時應向其提供之資訊），第十一條第一項（自第三人收集資訊者應向資訊主體提供之資訊），第十二條（資訊主體自控制者獲悉資訊之權）及第二十一條（資訊處理之公開）所規定權利義務之範圍，如該限制為保障下列利益所必要者：（a）國家安全（national security）；（b）國防（defense）；（c）公共安全（public security）；（d）對犯罪之防止、調查、發現及追訴或受管理從業人員對倫理之違反；（e）會員國或歐盟之重要經濟或財務利益，包括貨幣、預算或貨幣事項；（f）涉及（c）、（d）、（e）事項行使公權力之監督、檢查或管理功能者；（g）對資訊主體或他人權利及自由之保護。第二項規定在足夠之法律保障下，尤其是當資訊並不用於對特定人採措施或決定，會員國得於無明顯影響資訊主體隱私危險之情形下，於資訊純為科學研究之目的，或只用於必要期間之統計目的時，以法律限制第十二條下之權利。

第十七條第一項關於處理之安全規定如下：會員國應使控制者實施適當之技術及組織之措施以保護個人資訊防免不法或意外之毀損、變更、未經授權之揭露或進入，特別是處理涉及資訊在網路（network）之傳輸為然，以及所有其他不法之處理。考慮到技術現狀及實施成本，此等措施應使安全之層次與其處理風險及被保護資訊之性質相當。

第二十八條規定主管機關、第一項規定會員國應規定一或多個機關（public authorities）負責本指令在其領域實施之監督。該等機關在行使其職權時應有充分之獨立性。第二項規定會員國在起草處理個人資訊保護個人權利與自由之相關行政規章時應諮詢主管機關。第三項規定主管機關應有之權力：包括調查權、干預權如對處理實施前之檢查意見、對資訊之禁止流通（blocking）、消除、對處理之暫時或確定之禁止，對控制者之警告或將該事項提交於國會或其他政治機關處理；當法律規範被違反時提起訴訟（legal proceeding）或移交司法當局處理之權，主管機關之決定得向法院上訴；第四項規定主管機關應接受個人或代表個人協會涉及個人資訊處理權力及自由保護之申訴（claim）並告知其決定。主管機關尤應接受於依第 13 條（豁免及限制）規定資訊處理之合法性加以查證之申訴，並於實施查證時告知申訴人。第 5 項規定主管機關活動之定期報告及其公開。第六項規定各主管機關均有權行使第三項賦予之權力，其他會員國之主管機關亦得請其行使之。各主管機關應彼此合作、交換資訊。第七項規定主管機關之成員對其獲悉之資訊，縱在去職以後，仍有職業上之保密義務。

英國之資訊保護法（Data Protection Act of 1998）為實施上述歐盟指令之國內法適例。該法在附件一（schedule 1）揭示資訊保護之八原則：

一、個人資訊之處理應公平合法，且符合附件二所定條件之一（資訊主體之同意；處理為履行資訊主體為一方之契約或應資訊主體在訂約之前之要求所必要；司法之運作（administration of Justice），

法律授與任何人職能之行使，政府或其部門職能之行使，任何人基於公共利益而行使具公共性質之職能所必要；為資訊控制者，第三人或資訊接收者之正當利益之目的所必要，除非依情形有害於資訊主體之權利、自由或其正當利益，內閣部長得以命令指明本條件滿足或未滿足之情形）如涉及敏感資訊，須再符合附件三所定條件之一（資訊主體之明示同意；為資訊控制者基於僱用依法履行義務或行使權利目的所必要，但內閣部長得以命令（by order）在特定情形下排除其適用或規定該條件在未滿足額外條件前視為未符合；為保護資訊主體或他人之重大利益所必要，而資訊主體無法自行或由他人代為同意，或資訊控制者無法合理預期能自資訊主體取得同意，或在保護他人重大利益之情形下，資訊主體不合理之拒絕同意；為政治、哲學、宗教或工會團體之正當活動所必要，已對資訊主體之權利及自由提供適當之保障，僅涉及團體成員或與其有經常往來者，且未經資訊主體同意不對第三人揭露；為進行法律程序取得法律建議，或建立行使或保衛法律權利之目的所必要;涉及之個人資訊已由資訊主體之故意而公開;為司法之運作，法律授予任何人職能之行使，政府部門任何職能之行使所必要，但內閣部長得以命令排除特定情形之適用或規定該條件在未滿足額外條件前提為未符合；為醫學目的所必要，並為醫護從業人員或與醫護從業人員有同等保密義務之人所執行，醫學目的包括預防醫學、醫學之診斷、研究、醫護服務之提供及其管理；所涉及之敏感資訊為種族來源，其處理之目的在保持或提昇機會平等所必要,且對資訊主體之權利及自由有適當之保障,內閣部長得以命令指定其是否滿足上述條件；依內閣部長以命令指定之條件下處理者）。

二、個人資訊只能以一個或多個特定合法之目的而收集，並不得以與該等目的不相容之方式處理。

三、個人資訊應與其處理之目的足夠，相關而不過分。

四、個人資訊應正確，並於必要時維持其正確。

五、個人資訊為任何目的之處理應不得超過其目的所必要之期間。

六、個人資訊之處理應符合本法對資訊主體權利之規定。

七、應採適當之技術及組織步驟以防止個人資訊之未經授權及不合法之處理，以及其意外之損失或毀損。

八、個人資訊不得移轉歐洲經濟區（European Economic Area）以外之國家或地區，除非該地能對涉及資訊主體權利及自由之個人資訊處理提供足夠之保障。

第六條規定主管機關（Office of Data Protection Commission）及上訴法庭（Data Protection Tribunal），其組織規定於附件五，上訴程序則規定於附件六。

第七條規定資訊主體對資訊控制者要求說明其個人資訊是否被處理，其內容、處理目的、接收人等，及其程序要件（如書面要求、身分證明、涉及第三人時其同意、手續費）等。

第十二條規定個人得以書面通知資訊控制者請其不單以資訊處理之評估而決定其如工作表現、信用情形、可靠性或其行為。此通知不適用於決定是否與資訊主體訂立契約或依法之決定。

第十三條規定因資訊控制者違反本法之受害人之求償權。第十四條規定經資訊主體之請求，法院得命資訊控制者改正、停用、消除或銷毀不正確之資訊。

第十六條至第二十六條規定資訊控制者向主管機關之註冊義務。

第二十七條以下規定豁免之情形。第二十八條規定保障國家安全豁免適用該法之資訊保護原則，第２、３、５編（該法實體部分，第一編為定義等，第六編為主管機關職權等規定）及第五十五條（不得未經資訊控制者之同意，取得或揭露個人資訊）或使第三人揭露個人資訊之規定。由部長簽發證書說明部分或全部豁免該等條文於任何個

人資訊即為決定性之證據，但受影響之人得向上訴法庭上訴。該證書得對個人資訊做一般性之描述並向將來生效。如法院認為該證書之發出無合理之依據得命其失效。如該證書對個人資訊僅作一般描述，任何資訊控制者得向上訴法庭主張其不適用於特定個人資訊，除非上訴法庭認為不適用，該證書應視為適用於該資訊。

第二十九條規定為防止及偵查犯罪，逮捕或追訴違法，計算及收取稅收目的之資訊處理豁免第一原則之適用；為上述目的取得個人資訊以履行法定職責而處理之個人資料豁免適用有關資訊之主體告知之規定；為達成上述目的而需公開資訊者不受有關禁止公開之規定之限制；如資訊控制者為相關主管機關為履行上述目的且該等犯行涉及任何給付之不法請求或公款之不法使用，而須就風險評估系統對資訊主體做分類而為之處理不受第七條之限制。

第三十條規定由內閣部長得以命令對健康、教育及社會工作之個人資訊豁免資訊主體之告知規定。

第三十一條規定下列情形免除資訊主體之告知規定：(a) 為保護公眾防止因不誠實不正當執業，其他嚴重不當行為或相關人士之不適合或無能在提供銀行、保險、投資、其他金融或企業經營（in the management of bodies corporate）造成之財務損失，因破產人（已或未免除債務）之行為造成之財務損失；或依法執行任何業務人員之不誠實、不正當執業、其他嚴重不當行為、不適合或無能所造成之財務損失；(b)-(d) 保護慈善事業免於不當管理，財產被不當使用，收回財產；(e) 保障工作人口之健康、安全與福利；(f) 保護非工作人口免於因工作人口或與其有關之行為之健康或安全之危險。

第三十二條為新聞、文學與藝術之豁免。第三十三條為研究、歷史與統計之豁免。第三十四及三十五條為依法應公開之資訊。第三十六條為家庭及個人資訊處理之豁免。

第三十八條規定內閣部長得以命令豁免資訊主體告知之規定，如其公開為法律所禁止或為保護資訊主體或他人更重大之利益。此規定並適用於禁止公開之規定。

第五篇（第四十至五十條）為執法之規定。第四十條為主管機關對資訊控制者違反資訊保護原則之執法通知。第四十一條為通知之撤銷。第四十二條為利害關係人對主管機關就資訊處理是否適法之評估之請求。第四十三條為主管機關對資訊控制者提供資訊之要求，但有律師與客戶間通訊之豁免。第六篇（第五十一至七十五條）則為主管機關職能及雜項規定。

我國

相較於美歐，我國對隱私權之保護只有一般性及初步之規範。如民國八十八年修正民法第一百九十五條第一項人格權受侵害非財產上損害得請求賠償之情形，由原來之身體、健康、名譽、自由，增加「隱私」等項。本院釋字第二九三號解釋對銀行法第四十八條第二項之規定，即指出其為維護人民之隱私權，但認議會對公營銀行預算之審理，有相當理由認其放款顯有不當，在銀行不透露個別客戶姓名及不公開有關資料下，仍得要求銀行提供有關資料。第五◯九號解釋指出「為兼顧對個人名譽、隱私及公共利益之保護，法律尚非不得對言論自由依其傳播方式為合理之限制。」第五三五號解釋對警察勤務條例有關臨檢之規定，在解釋理由書指出「臨檢實施之手段…不問其名稱為何，均屬對人或物之查驗干預，影響人民行動自由、財產權及隱私權等甚鉅」。第五八五號解釋理由書更明白指出，「隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活秘密空間免於他人侵擾及個人資訊之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第二十二條所保障」，故隱私權受憲法保障，應無疑義。但是如美國只限於部分私密領域（見前）或如德國全部憲法化，由於我國民法、銀行法等已有之規定，以及德國

特殊之背景，應以前說為當。至何部分受憲法直接保障，何部分如美國為立法形成空間，仍有待個案解釋決之，而隱私權之範圍應屬立法權限，不宜在解釋中規定。

民國八十四年制定之「電腦處理個人資料保護法」，就個人資料之蒐集處理之規範，形式上採歐洲之集中管理模式，對公、私資料處理綜合加以規範，就其基本原則（第六條個人資料之蒐集或利用，應尊重當事人之權益，依誠實及信用之方法為之，不得逾越特定目的之必要範圍）當事人之權利（第四條規定不得預先拋棄以特約限制之權利有查詢及請求閱覽、製作複本、請求補充或更正，請求停止處理及利用，請求刪除）及限制（第十一條得不公告個人資料檔案之情形，第十二條當事人請求自己資訊之除外情形）公務機關資訊處理之規範，如須有特定目的，並符合法令職掌必要範圍，或經當事人同意，或對當事人權益無害（第七條），得為跨目的利用之情形（第八條），個人檔案公告（第十條），個人資料之更正或補充（第十三條），處理期間（第十五條），安全維護（第十七條）。非公務機關資料處理之規範（第十八條至第二十六條），損害賠償及救濟（第二十七條為公務機關、第二十八條為非公務機關違法之損害賠償、第二十九條為時效、第三十條為適用法，公務機關適用國家賠償法、第三十一條規定當事人依第四條請求公務機關處理後未處理或及時處理時向其監督機關請求處理，第三十二條為向非公務機關請求處理不果，得向目的事業主管機關請求處理）罰則（第三十三條至四十一條）附則（第四十二條至四十五條，其中第四十二條規定法務部協調聯繫執行相關事項）等均有規定。

與歐盟之個人資訊保護指令與英國之資訊保護法相較，雖然實質規定大體相同，但過於簡化，不比英國資訊保護法之層次分明，如不同之豁免其範圍與要件有所不同，敏感與非敏感資訊亦有不同規定，較嚴重之問題為無獨立資訊保護機關之規定，雖可訴諸法院，但無專

業性保護機關，其效果將大打折扣。此點我國較類似美國（亦無獨立資訊保護機關），有改進之空間。

指紋與資訊隱私權

指紋是人指頭前端皮膚上的紋路，有人各不同之特性，普遍被用為辨識之工具。據英國政府之說明（註二十五），人之辨識有三種基本的要素（three basicelements of identity）：（１）生物特徵之辨識（biometric identity）：為專屬個人之特性，如指紋、聲音、虹膜、面貌、DNA、掌形、散熱（heat radiation）等，其中以指紋最為方便使用；（２）因出生被賦予之辨識（attributed identity）如全名、出生地點或時間、父母姓名及地址等；（３）經歷之辨識（biographical identity）在生命經歷中逐步建立，包括在人生活中發生之事件及人與社會之互動，如出生之登記、學歷、選民登記名冊、給付之申請及納稅紀錄、工作之經歷、婚姻之註冊，財產之抵押及所有權、保險單；與銀行、債權人、公用事業及政府機關之往來等。辨識往往需要不只一種辨識工具。此種個人資訊在一定程度內，但不一定，涉及隱私權。

以建立隱私權概念之美國侵權行為法所承認之四種侵害隱私權之態樣而言，已公開或公眾對之有知之權利（如涉言論自由）之事實，無隱私權之適用，對他人私密之入侵或私事之公開，必須社會公念認為不合理、不法或使合理之人感到極不愉快者。美國依憲法增補條文第九條（相當於我國憲法第二十二條）擴大適用隱私權及於某些個人自主決定之私領域，如婚姻、生育、避孕、養育兒女、家庭等，透過最高法院之判決將其提昇至憲法層次加以保護。依憲法增補條文第四條禁止不合理搜索與扣押對資訊隱私權之保護，限於有真實、合理隱私預期之情形。美國最高法院判決除承認上述私領域自主決定之隱私利益外，尚承認個人事務不公開之隱私利益，但後者只限於特定敏感事項政府有防止資訊不當外洩之義務，並非禁止收集個人資訊（註二十六）。

美國最高法院對隱私權之保護為國會留下廣大之法律形成空間。其 1974 年之隱私權法對部分政府機構之資訊收集與處理使用加以規範，並將指紋列入檔案紀錄之範圍（註二十七），故就該法而言，可視為個人資料之一部分。該法雖就資訊之儲存限於相關及必要，須以行政及技術措施確保資訊之安全，並原則規定未經資訊主體同意不得公開。不過該法有十二項豁免之規定，其應用最廣者為例行性使用，只須與原始收集目的相容即可。其對資訊之比對有若干程序規定，如機關間須訂書面協議，因比對採不利措施須先獨立查證，並予當事人異議之權。在資訊自由法之公開，因重點在政府之活動，故純個人資訊原則上均不予公開。

對指紋蒐集與資訊隱私關係有明確說明者有 1986 年加州最高法院 PERKEY V. Department of Motor Vehicles 一案（註二十八）。加州法律規定申請駕照之申請書須附拇指或手指之指紋。立法說明中指出其為維持可靠之特許制度之必要。州之政策為使汽車監理所所發出之駕照及身分證成為本州之基本身分文件，而州有確保此身分制度正確無誤之重大利益。原告拒絕按指紋而被拒發駕照。原告主張，收集及取得指紋而無限制地作為全州身分證明之用，違反憲法保障之個人隱私權，將提出指紋作為發駕照之條件為不當連結。指紋與政府保障公路安全之利益無關。法院首先認為本案不涉基本權，應採合理原則之標準（rational basis test）審查，防止冒領駕照有利於公路安全為正當之立法目的。而相較於簽名及相片，指紋因為其人各不同及終身不變之特性為最正確之辨識方法，要求於申請時提出為合理。指紋之製作不涉身體之入侵或違反憲法第四增補條文對不合理搜索之禁止規定，本身尚不構成對個人隱私權之侵害或違反人性尊嚴。但指紋為個人資訊之一種，受相關資訊保護法律之限制，不得任意公開。首席大法官 Bird 在協同意見書表達其對指紋被濫用之憂慮，並認指紋可構成潛在之敏感資訊。大法官 Mosk 之不同意見書認同多數意見中申請駕照須附指

紋合憲一點，但不同意其分析及對加州法律明白規定所做不合理解釋，亦對其所謂潛在之濫用（包括汽車監理所或其他政府機構）留待將來之判斷。他認為「指紋」並不構成加州資訊保護法所謂「身體狀況」（Physical condition），後者是指醫學上之問題，非該法所保護之個人資訊。指紋不過是一種額外之身分辨識方法，其收集與散佈不涉違憲。指紋並不顯示個人之歷史、思想、習慣、政治立場或財務狀況。占有個人之指紋並不創造監視之氣氛，或顯示其將用於不當之用途。

另在 Thom v. New York Stock Exchange（註二十九）一案，紐約州法律規定證券業之從業人員須按指紋方得就業。該法之目的在杜絕不法分子進入證券行業以減少證券失竊之事件。紐約南區地方法院認為收集指紋可合理達成上述目的，指紋只是確認有無犯罪之方法。

法院並認為原告主張指紋之隱私權無意義（without substance）認為按指紋是犯罪烙印之時代早已過去，聯邦及州法對不涉刑事而按指紋之情事所在多有，如聯邦政府公務員，紐約州之公務員，某些州之學童或新生兒之母親，而及眾多行業之從業員均採指紋為辨識方法。至原告主張並無機會接近證券，法院認為亦可能有間接之機會，且如此細分，亦不切實際。至於取得之指紋將來可能用於犯罪調查用途，法院認為合法取得之指紋將來用於辨識目的，甚至刑事調查，為立法政策之問題。

其他國家似尚未見強制按捺指紋合憲性與其與隱私權關係之判例（註三十）。不過指紋是個人資訊之一種，本身雖不涉隱私權，但其處理如涉其他敏感資訊（如可以指紋啟動付款系統或取得個人健康資訊），政府如有蒐集及利用即有加強保護之義務。無論是依歐盟個人資訊保護指令第八條或依英國資訊保護法第二條之定義，指紋本身尚非敏感資訊（註三十一）。不過縱屬敏感資訊，亦非當然不得蒐集、處理、利用，只是增加限制條件或加強保護（歐盟指令第八條第二項以下及第十七條第一項，及英國資訊保護法附件三參照）。至於跨目的使用，

原則上雖依蒐集之特定目的（一個或多個），但例外頗多。如美國例外最多，包括對執法或其他政府部門之揭露或例行性可與原目的相容之使用。歐盟指令第十三條亦有豁免規定，包括國家安全、國防、公共安全、對犯罪之防止、調查、發現及追訴等之必要而得豁免相關規定。英國資訊保護法第二十八條就國家安全幾乎豁免所有相關規定，其他則只有部分之豁免（如依第二十八條犯罪偵防目的之豁免第一原則等之適用）。

領身分證須按捺指紋之立法例

聲請人及多數鑑定人均主張強制按捺指紋違憲，但此種為國際人權團體一貫之主張，屬於法律「所應然」而非「實然」之層次。根據內政部（註三十二）、鑑定人孟憲輝教授（註三十三）、徐正戎教授（註三十四）等所提供之資料，設有身分證制度之國家約一百國，規定領取身分證須按捺指紋之國家亦有二十餘國，包括亞洲之新加坡、南韓、泰國，歐洲之西班牙、葡萄牙、義大利等。積極推動生物特徵（含指紋）新式身分證之國家尚有英、法等國。另歐盟亦規劃在 2007 年底實行生物特徵護照、內含指紋晶片（註三十五）。而國際民航組織成員國中約 40 餘國（含歐盟）特將護照附（含指紋）有生物特徵之晶片。故在實證法層次，相當多之國家容許政府強制國民按捺指紋作為取得身分證件之條件。但其立法目的、指紋顯示之方式、取得指紋分散或集中處理，以及其他相關實務，則各不同。

在收集指紋之目的（用途）上：南韓規定於「住民登錄法」強制國民於申辦住民登錄證時按捺指紋，其目的（理由）為（１）因應南北韓分裂之整體安全需求；（２）預防犯罪及協助案件偵查；（３）一般身分確認；新加坡規定於國民登記規則（National Registration Regulation,依附於何法不詳）於對國民及永久居民發證時錄存指紋用於辨識身分及協助刑事偵防；法國身分證為自願申辦，但如申辦須按指紋目的為供辨識，但資料存於警局恐仍有供犯罪偵防之用。在歐盟

地區可替代旅行證件。但 2005 年 4 月政府提出安全身分證法案規劃於 2007 年換發電子晶片身分證強制全民持有晶片包括指紋等生物特徵資料，所有資料並存於中央資料庫中。將取代所有官方證件，目的在打擊恐怖份子，防堵非法移民及對抗偽造文書。西班牙申辦身分證必須按捺指紋，僅存檔供身分辨識之用。其法律依據為 1992 年之「國家安全保護組織法」。申請書按之指紋由警局保管。又該國正試驗晶片社會安全證內容分隔（相關工作人員只能進入相關資料，如雇佣、退休金、健保）加密，本人則可用手指進入查閱資訊。而數位化之晶片國民身分證亦在擬議中，而加強身分證件動機之一為防止非法移民。葡萄牙依 1995 年 2 月 21 日第 5 號法及 1999 年國民身分辨識法，事實上強制持有身分證、按指紋、作身分辨識用。德國依 1950 年 12 月身分證法在必要者加密之情形下，得將手指等生物特徵掃描建檔，但須聯邦另行立法規範。但禁止生物特徵之資料庫。義大利自 1999 年電子晶片身分證特性暨發給辦法施行後，逐步以晶片身分證取代傳統之身分證，為多功能（可取代健保卡及選舉人證）自 2002 年 10 月 13 日起，國民指紋資料必須登錄於晶片中，而內政部有中央資料庫。新制之目的為打擊偽冒之身分證流通。英國 2005 年 6 月向國會中提出有生物特徵（含指紋）之身分證法案及設中央資料庫其立法目的為：（１）防止身分冒用（Identity theft）；（２）防止非法移民及工作；（３）防止濫用政府服務（福利）；（４）防止組織犯罪及恐怖主義（註三十六）。哥斯大黎加領取身分證強制按指紋，並逐步建立資料庫。目的除一般辨識功能外，並可供檢警銀行等單位申請使用。巴西領取身分證須錄存指紋，目的（用途）為提供辨識屍體、犯罪案件調查檔案比對。墨西哥申請投票卡需錄存指紋設全國資料庫。香港晶片身分證有拇指模板，加密防偽可用於加速入境及其他用途。澳門含指紋之晶片身分證，有身分識別功能。

至於指紋顯示之方式，直接顯示於身分證紙本者，有南韓、新加坡、葡萄牙、哥斯大黎加（條碼）、巴西、墨西哥；在身分證之晶片內者有義大利、港、澳、及擬議中之英、法身分證。收集而不顯示於身分證者，有法國、西班牙等。多數國家對收集之指紋均設資料庫，如韓、新、法、哥、巴、墨、義以及擬議中之英、法新制。少數分散於晶片，如港、澳以及歐盟之生物特徵護照只容許一對一之比較，不能如前者之容許電腦比對，效能或較差，相對濫用之機會亦減少。至於如德國禁止資料庫，應屬特例。

參考以上各國之憲法判例與法律規定強制蒐集指紋尚非憲法所不許，但如何控制其蒐集、保管與使用，以確保憲法所保障之個人資訊隱私權，為一大挑戰。上引之歐盟 1995 年個人資訊保護指令以及英國 1998 年資訊保護法之相關規定，應為國際上之最佳實務標準（best practices）。而德國聯邦憲法法院 1983 年人口普查法案（Census Act Case）以及 1986 年美國加州最高法院 Perkey V. Dept of MotorVehicles 一案之論述，可供參考。前者關心在自動化處理下不同資訊之組合可以重建個人之簡介或形象（personal profile），其外洩生成心理壓力影響個人自主決定其實不適用於指紋（參看前引 Perkey 案 Mosk 之不同意見），但其將法律應明確規定官方資訊收集之目的及條件，並遵守比例原則，只能在必要限度內並保障資訊安全提升至憲法上之要求可供參考。後者雖肯定汽車監理處收集指紋，防止偽冒之合憲性，但禁止其外洩。而近年新興國家憲法（或最高法院）亦有對以總統命令建立『國民識別資料電腦化系統』無明確目的將取得資訊之控制，保護無明確規定，或以人口普查建立" 國民資料庫 "對目的使用漫無限制，亦無對個人權利保護，或對資料安全維護缺乏規定，而分別宣告違憲者（註三十七）。故立法者在個人資訊保護應符合一定標準之憲法上義務，應已在國際上確立，但要求不宜過細，以保留適當之立法形成空間。

指紋之功能、用途或蒐集目的為辨識

多數意見透過立法目的之窄化及相關事實之高度選擇性認定，達到戶籍法第八條第二項及第三項違憲之結論，本席十分佩服，只是無法認同。其根本之問題，還是對指紋本質認知之錯誤。指紋只是中性之身分辨識工具，此點與姓名或照片無異，只是更為精確。人可以更改姓名，且同姓同名者甚多（每年大專聯考報章多就此大作文章）。相片因時間之經過而漸失辨識作用，且相貌相似者亦甚多，肉眼不易辨識。指紋則因其人各不同之特性，可以正確辨識。如果因為指紋可以連結某人在某場合做某事而認定為應對其嚴格限制或視為敏感資訊，同理姓名亦應限制其認定之功能，如此作法好像精確或發現真實本身不合正義或違憲。更不能因其所聯結之資訊本身敏感（如某人正從事政治活動）而認為指紋亦成了敏感資訊。應禁止或限制者為該項敏感資訊（從事政治活動）之蒐集，而非指紋或姓名。此點指紋與其他輔助性之辨識資訊，如健康或其他經歷之辨識資訊不同。就醫紀錄之蒐集目的為提供醫療服務甚為明確，如果用以指證某人犯罪自然需要有法律之授權，因其本身為公認之敏感資訊，更涉跨目的之使用。所以上述美國之判例均認為指紋本身不涉隱私權，最多只是個人資訊，政府如蒐集，自然有保護不使外洩之義務，並適用有關個人資訊處理之法律。即如建立「資訊自決權」概念之德國聯邦憲法法院 1983 年之人口普查法判決，其如此決定之主因即是資訊自動化處理結果之可能心理壓力影響個人之自主決定，此點對指紋並不適用。因其蒐集不能顯示個人之歷史、思想、習慣、政治立場或財務狀況，亦不創造監視之氣氛（上述 Perkey 案 Mosk 法官語）。依「法律理由如不存在法律本身亦不存在」（Cessante ratione legis, cessat et ipsa lex）之法諺，所謂資訊自決權，亦無必然適用於指紋之理。

立法目的之認定

如前所述，指紋之基本作用在辨識身分，亦即國家蒐集指紋之目的，本無待在法律上標明，此上述各國規定身分證申請需附指紋之國家，多數只規定為辨識身分之目的，至於用途多用在犯罪偵防，而由警局保管。各國違憲審查實務，對立法目的之認定除求之於立法史外，亦不乏法院代為設想者（美國即為顯例）。我國司法院大法官審理案件法第十三條第一項前段即指示「大法官解釋案件，應參考制憲、修憲及立法資料…」，立法目的可從中發現，自不待言。從立法委員柯建銘等十七人提案修正戶籍法增訂第十條之一（即現行條文第八條）說明一指出指紋用於確認當事人身分保障當事人權益，如迷失民眾或無名屍體身分之確認，作用至為明確。說明二指出國民身分證錄存請領人之指紋，可結合現行警政自動化作業，強化治安防範，保障社會安全…（註三十八）。可見其立法目的除原戶政有關之身分辨識外，尚有維護治安，即犯罪偵防之目的。

雖然其後關係機關在言詞辯論中一方面主張依戶籍法取得之「戶政指紋資料」不得與「犯罪指紋資料」為跨目的之使用，並強調二者之目的不同；另方面又主張指紋對犯罪偵防有補充性之功能，且仍將依「個資法」提供（註三十九）。在說明會等場合則強調其多方面之功能，如冒名頂替、防止雙重身分、移民身分確認、防止經濟詐欺等（註四十）。然憲法法庭本不受當事人主張之拘束，而有合理認定立法目的之義務。基於上述指紋之本質，其目的究為戶政上之辨識，或反恐、公共安全、犯罪偵防，實無法切割。各國作法，或認辨識本身為立法之目的（我國行政院之草案說明亦同）或在法條上列舉多種目的，如南韓在「住民登錄法」強制按捺指紋之目的為（１）因應南北韓分裂之整體安全需求（國家安全）；（２）預防犯罪及協助案件偵查；（３）一般身分確認。英國有生物特徵之身分證法案之立法目的為：（１）防止身分冒用；（２）防止非法移民及工作；（３）防制濫用政府服務（福利）；（４）防止組織犯罪及恐怖主義。參考上述立法資料，如認戶籍

法第八條第二項規定身分證錄存指紋之立法目的為：（１）防止冒認身分，保障當事人權益及與戶政有關之一般身分辨識及（２）協助維持治安，應已符合目的明確及重大公共目的之要求。

審查密度及比例原則操作

上述美國指紋案認為指紋本身不涉隱私權，亦不涉基本權（美國基本權之定義與我國不同）而採低密度之審查（合理性標準）認為合憲，即只要求政府目的正當（防止偽冒、公路安全），手段（蒐集指紋）有助於目的之達成（註四十一）。美國中度審查之標準，以商業性言論之限制為例，需政府利益重要（substantial governmental interest），規範直接有助於提升所稱之政府利益，且規範並不過當。不過，規範不過當並不等同最小侵害之手段，手段與目的之契合（fit）不必完美，但須合理，即其與利益間需有比例之關係，手段雖不必為最小侵害手段，但須切合其所欲達到之目的（narrowly tailored），過關其實是相當困難（註四十二）。至於嚴格審查標準，如一般非不受保護亦非評價較低之言論，則政府利益需重大（compelling state interest），亦無較小侵害之手段可供運用，運作結果政府幾無勝算（註四十三）。德國之三種審查密度，明顯性審查（除非違憲情節明顯可見，應尊重立法機關之判斷）與可支持性審查其實並無二致。至嚴密之內容審查則與美國之嚴格審查（strict scrutiny）並無不同。總之審查密度無非是問題取向，取決於問題所涉憲法規範之性質及嚴重性，無明確之判斷標準（註四十四）。

多數意見首先透過立法目的之窄化，一則主張立法目的應明定，再則認為至多可承認關係機關所主張之加強防偽、防止冒領冒用國民身分證即辨識迷途失智者、路倒病人、精神病患與無名屍體之身分等為重要公益目的，而排除可能被認為重大公益目的之維護治安等，將政府目的降級。在利益權衡或成本效應之分析上對蒐集指紋之成本，以及可能之資訊保護風險，強調其「大量」、「高度」（未見其作絕對或相對之量化），對其可能之效益則以無法評估一語帶過。又以現有資訊

足以辨識而認目的與手段（蒐集指紋)「無密切關連性」。又運用先有蛋或先有雞之辯證法，認按指紋對現存身分不明者無助，對將來之需要，又不能以全民承擔風險，故屬「損益失衡、手段過當」，不符比例原則。多數意見所不願面對者，為冒名入獄對司法公信造成的損失難以量化，多起重大刑案現場採有指紋卻因國內建檔不全（建檔率約四成，且不良率四成）而無法比對，個人可能因證件之遺失或被盜用而遭盜領存款而傾家。經濟詐騙民國九十年造成八十億元之損失，九十三年造成九十四億之損失。近年反詐騙專案平均每月三千至五千件，其中四分之一涉及身分之冒認，其中絕大多數也可因指紋檔比對而避免（註四十五)。而初步建檔成本約八千萬元，在中央政府預算中不到萬分之一，雖然尚須於配套法制完備後增設析鑑設施，其與可能避免之巨大精神與經濟損失相比，十分合算。指紋是相對最精確之身分辨識工具，遠佳於姓名或相片或其他辨識資訊，何以會「無密切關連性」，令人難以理解。多數意見雖說適用中度審查標準，其實比最嚴格之標準還嚴。因指紋之無可取代性已可滿足後者最少侵害手段（因在要求同等有效手段中，已無可取代）之要求。

本席認為以指紋為人別之最佳辨識工具而言，且其不涉隱私權(因其為公開至少是半公開之資訊）本案本應以明顯無理由而不受理（技術上可透過程序上之理由)。退一步言，應比照上述美國之判例，以合理性標準原則審查而合憲。即使退一萬步而言，以中度審查標準（甚至最嚴格）標準審查，考慮立法史中之「治安」等目的，合乎「重大公益」之標準，蒐集指紋可以防免上述種種經濟及精神上之損失。「蒐集指紋」在同等有效手段中無可取代（新版身分證之種種防偽措施，只能防止相片及姓名等紀錄之偽變造，無法取代指紋之人別辨識功能。假定第一次指紋建檔正確時)。尤有進者，多數意見所謂資訊保護之「高度風險」亦不如想像之巨。一則現存之指紋檔案多年尚無外洩情形，足見保護措施尚屬良好（註四十六)。二則依內政部之說明，依戶籍法

第八條第二項規定之錄存，擬使用活體掃瞄指紋機，蒐集加密後透過封閉式專屬網路傳輸至全國資料庫建檔，外人無法透過網路入侵。且指紋電腦資料係以「特徵點」、「影像」兩種模式儲存，前者無法還原，後者受解析度所限，亦不可能完全紀錄所有細緻特徵，複製幾無可能。為防濫用之方法包括只供比對定期稽核，特別是異常查詢之警示與追查，並設錄影或類似之監視系統。至於防火牆、入侵偵測、安全閘道、網路連線授權則是法規完備後開放有關單位查詢時之可能配套安全措施（註四十七）。指紋不但可協助辨認犯罪人、被害人，亦可排除無辜之第三人。兩枚指紋相同之鑑定，不一定意味其為犯罪，必須輔以各種情況證據，由法官作綜合判斷，不是單憑一枚複製指紋即可誣陷（註四十八）。加以現行「電腦處理個人資料保護法」（非本案審查標的）第十七條規定：「公務機關保有個人資料檔案者，應指定依相關法令辦理安全維護事項，防止個人資料被竊取、竄改、與毀損滅失或洩漏。」本席對多數意見，人權團體恐配套措施不全，使損及當事人利益之苦心充分理解與尊重，個資法及相關法令容有改善之空間，但亦不宜過度低估關係機關以最佳技術規範，立法機關隨時代進步而修改法律以保護個人資料之決心及能力。因此本席認為資訊保護風險尚在合理範圍，戶籍法第八條第二項可以通過任何標準之比例原則之考驗。

比較解釋與合憲性解釋

採用比較分析外國類似法制之比較解釋法，在我國繼受外國立法頗多之情形，有一定價值（註四十九）。世界有身分證制度之國家百餘國，其中規定申請身分證需附指紋者亦有二十餘國，已如上述。戶籍法第八條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。依內政部之看法，捺指紋為發身分證之要件，亦為身分證之內涵，國會立法授權按捺指紋與建立國民身分證之目的結合，尚無不當連結之情形（註五十）。但由於我國現行法律投票時須憑身分證領取選票（如總統副總統選舉罷免法第十四條及公職人員選舉罷免法第二十一條），

此項規定雖與其他在身分證強制按捺指紋之國家如義大利、西班牙、葡萄牙、新加坡、韓國等相同（註五十一），但影響國民依憲法第十七條之參政權，依美國最高法院之判例，對投票權之不當限制，應受嚴格審查（註五十二）。加以規定須使用國民身分證情形之法規多達 275 種，多數意見在解釋理由書中亦詳細列舉，無國民身分證將重大影響人民之日常生活。故第三項之情形，與第二項單純蒐集指紋之情形有所不同。本席認為指紋在人別辨識上之重要地位，作為連結本人「同一性」之要素，較之姓名、相片，有過之而無不及，作為身分之內涵，不按指紋不發給身分證，本身並無不妥。但考量在舊版身分證過渡期滿對人民可能造成之不方便，可依合憲性解釋原則即使下位法律為符合上位憲法之意旨之解釋使合憲，或限縮其範圍，或轉換其條文意義使合憲（法國之憲法委員會運用特多（註五十三）），解為在政府應發給拒按指紋者同等效力之身分證明，俾能行使投票權或辦理其他需身分證明事務之條件下合憲。

蒐集處理個人資料之憲法上界限

多數意見較有建設性之貢獻在解釋文第三段對國家大規模蒐集指紋（其實更應適用於個人資料之蒐集）建立憲法上之界限，並迫使立法者改良其立法技術。本席對此原則，雖表贊同，但不論應用在指紋或一般個人資料對其細節上仍有不同意見。本席一貫之看法指紋只是個人資料，既不涉隱私權亦非敏感資料，只能是用一般個人資料之標準限制，規範其蒐集處理。縱依多數意見，亦只是用中度原則審查，而應使用「重要公益」而非「重大公益」之文字，再者「法定目的」云云，如用於將來，本席無意見，但本案之審查，本席認為目的可在立法史中發現。

註一：一般請參考 Prosser and Keeton, Torts, 5th ed., 1984, ch.20.

註二：較重要之判決包括 Whalen v. Roe, 429 US 589 (1977) ;Roe v. Wade, 410US 113 (1973)美國爭議性極大准許墮胎之判例；

Planned Parenthood of Southeastern Pa. V. Casey 505 US 833 (1992) 確認 Roe v. Wade 之核心但做若干修改；Lawrence v. Texas 123 S. ct 1406 (2003) 判決德州禁止同性戀性行為之法律違憲等。

註三：一般請參閱 Donald P. Kommers, The Constitutional Jurisprudence of the Federal Republic of Germany, 2nd ed., 1997 c.7;王澤鑑，人格權保護的發展趨勢（臺灣高等法院 94 年 8 月 19 日）

註四：德國聯邦憲法法院 1983 年之戶口普查法一案 65Bverf GE，對此發展扮演關鍵性之角色。美國最高法院尚未接受此概念，而由國會立法逐步規定。

註五：敏感資訊之定義，見歐盟個人資訊保護指令 (Directive 95/46/EC of the European Parliament and 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) 第八條及英國資訊保護法 (Data Protection Act of 1998)第二條。

註六：關於美國資訊隱私權之具體內容，參看 Paul M. Schwartz and Joel R. Reidenberg, Data Privacy Law, 1996。其對聯邦立法之介紹見該書第五章。（以下簡稱 Schwartz and Reidenberg）

註七：429US 589 (1977)

註八：5 U.S.C. Section 552 a (e)(1)

註九：5 U.S.C. Section 552 a (e)(2)

註十：5 U.S.C. Section 552 a (e)(5)

註十一：同上

註十二：5 U.S.C. Section 552 a(b)

註十三：5 U.S.C. Section 552 a(b)(1)-(12)。

註十四：5 U.S.C. Section 552 a (b)(3)

註十五：Schwartz and Reidenberg. 96-100.

註十六：5 U.S.C. Section 552 a (g)(1)

註十七：5 U.S.C. Section 552 a (p)

註十八：5 U.S.C. Section 552 a (b)(1)-(9)。

註十九：Schwartz and Reidenberg. 108-114.

註二十：5 U.S.C. Section 552 a (o)

註二十一：Schwartz and Reidenberg., 118-128。

註二十二：27 BVerf GE 1

註二十三：65 BVerf GE 1

註二十四：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 。該指令前言有七十二點，已點出資訊處理之基本原則。共三十四條，分為通則、個人資訊合法處理之一般規則（又分資訊品質、正當處理之標準、特種資訊之處理、應向資訊主體提供之資訊、資訊主體獲悉資訊之權利、豁免與限制、資訊主體之異議權、處理之保密與安全、通知等）司法救濟、責任與處罰、個人資訊移轉予第三國、行為規範、主管機關與工作小組、負責等章。

註二十五："Identity Fraud: a Study" (UK) Cabinet Office, July 2002.

註二十六：見 Whalen v. Roe 案，見前。該案容許特定危險藥品處方及相關資訊之收集及處理。另在 Planed Parenthood of Southeastern Penn. V. Casey, 505 US 833 (1992)，認州法規定醫院需對墮胎之醫學程序做成紀錄及報告合憲。

註二十七：顧立雄律師說明會書面資料，頁 3。

註二十八：42 Cal 3rd 185 (1986)。加州最高法院是美國最自由派之法院之一，其大法官絕非不重視人權者，加州是少數在憲法上明文保障隱私權之州。

註二十九：306 F. Supp. 1002 (1969)

註三十：至少在關係機關內政部以及鑑定人未見在說明會及辯論中提出，個人亦尚未在參閱過之資料中發現。

註三十一：歐盟指令第八條之介紹見前英國資訊保護法除指令規定者外，又增加資訊主體犯罪或被指摘犯罪之資訊或對犯罪或被指犯罪之程序，此程序之結果或法院之判決。

註三十二：內政部 94,06, 09 全面換發身分證捺錄指紋說明，pp.59-63；內政部 94,06,30 說明會書面資料，pp.12-16；內政部 94,7,7 致本院函；內政部提供 94/7/11，對美、加、荷、比、芬、丹、法、澳、紐、西、德等國身分認證制度之討論) ；94 年 7 月 27、28 日憲法法庭行政院內政部發言紀錄彙整，頁 2（國際民航組織之護照規格）。

註三十三：7 月 27、28 日憲法法庭鑑定報告書補充資料，附 House of Commons,Canada, A national Identity Card for Canada? Report of the Standing Committee on citizenship and immigration, October 2003,pp. 17-25, 31-46.

註三十四：7 月 27、28 日憲法法庭鑑定報告書，頁 42-58

註三十五：Council Regulation (EC) No. 2252/2004 of 13 December 2004 on Standard for security feature and biometrics in passports and travel documents issued by member states.

註三十六：Home Office Identity Cards briefing, May 2005。

註三十七：分別為菲律賓最高法院 1998 年 Blas F. Ople, Vs. Ruben D Torres elal 案及匈牙利憲法法院 1991 年 No.15AB 案。見黃昭元教授鑑定意見（修正版）頁 36-39

註三十八：立法院議案關係文書第一四九八號（85 年 6 月 29 日印發）內政部 94/6/09 說明，附件二，頁 27。行政院草案第八條說明三則為「指紋之作用可確認當事人之身分，保障當事

人權益，如迷失老人或無名屍體之辨認等…」，二者合併審查。

註三十九：內政部 7 月 27、28 日言詞辯論意旨書，頁 12。

註四十：內政部 94,06,09 全面換發身分證捺錄指紋說明。說明會中孟憲輝教授之書面及說明會發言紀錄，頁 4-6, 13, 26, 28-29。

註四十一：美國合理性（低度）審查標準主要用於經濟及社會立法，其演進請參閱 Kathleen M. Sullivan & Gerald Gunther, Constitutional Law, 605-628. (14ed.2001)(Sullivan & Gunther)

註四十二：Central Hudson Gas v. Public Service Commission 447 US 557 (1980) 及 Board of Trustees State University of New York v. Fox 492 US 469 (1989). 一般請參看 Sullivan & Gunther 1135-1158

註四十三：Ibid, 956, 967-968.

註四十四：吳庚，憲法的解釋與適用，2003 年 9 月修正版，頁 405-411。

註四十五：本案說明會發言紀錄，頁 4-6，13，26，28-29。以外國經驗而言，美國問卷發現 44％民眾有駕照及社會安全卡（美國之主要身分證明）被竊經驗。英國每年因身分證件被偽變造之受害人達五萬人，每年經濟損失十三億英鎊，而恐怖份子約三分之一使用偽變造身分。同上，頁 4-6。

註四十六：本案說明會紀錄，頁 9-10。

註四十七：內政部 94,06,09 全面換發身分證捺錄指紋說明，頁 57-58，61-62。內政部 6 月 30 日說明會書面資料，頁 19-20。

註四十八：孟憲輝教授在說明會之書面，頁 6。

註四十九：吳庚，前引註 44，頁 536-539。

註五十：內政部言詞辯論辯論意旨書，頁 6-8。

註五十一：內政部 94 年 8 月 16 日及 22 日致本院秘書長書函。

註五十二：如 Reynold v. Simss, 377 US 533 (1964)一般參見 Sullivan and Gunther,頁 794-858。

註五十三：吳庚，前引註 44，頁 581-592；陳淳文教授就在本院釋字第五八五號解釋「三一九槍擊事件真相調查特別委員會條例」鑑定報告，頁 1-13；李念祖教授在同一案件之鑑定報告，頁 1-4。